1. Basic definitions.

Def 1.1 *Binary operation* $*$ on a set A is a mapping $A \times A \to A$. The element which is attached to the pair $(a; b) \in A \times A$ is denoted by $a * b$.

For a given sets X and Y the set of all functions $f : X \to Y$ will be denoted by $\mathcal{F}(X; Y)$; the set of all bijective functions $f \in \mathcal{F}(X; X)$ will be denoted by $\mathcal{S}(X)$. For two functions $f \in \mathcal{F}(X; Y)$, $g \in \mathcal{F}(Y; Z)$ their *composition* $f \circ g$ is defined in a standard way: for $x \in X$ $(f \circ g)(x) = f(g(x))$. Thus composition of functions is a binary operation on $\mathcal{F}(X; X)$; note that composition is also a binary operation on $\mathcal{S}(X)$.

Def 1.2 A binary operation $*$ on a set A is called *commutative* if $\forall\ a, b \in A \quad a * b = b * a$.

$\diamond$ **1.1** 1) Prove that for $|X| > 1$ composition on $\mathcal{F}(X; X)$ is not commutative.
2) Prove that for $|X| > 2$ composition on $\mathcal{S}(X)$ is not commutative.

Def 1.3 A binary operation $*$ on a set A is called *associative* if $\forall\ a, b, c \in A \quad (a * b) * c = a * (b * c)$.

$\diamond$ **1.2** 1) Give an example of a commutative but not associative operation.
2) Give an example of an associative but not commutative operation.
3) Give an example of such an operation $*$ that $(a * a) * a \neq a * (a * a)$ for some $a \in A$.

Def 1.4 An element $\varepsilon \in A$ is called *neutral element* for the operation $*$ on A if $\forall\ a \in A$ $a * \varepsilon = \varepsilon * a = a$.

$\diamond$ **1.3** Prove that a set with a binary operation has at most one neutral element.

$\diamond$ **1.4** Find the neutral element (if it exists) for the following operations:
1) composition of functions on the set $\mathcal{F}(X; X)$;
2) composition of functions on the set $\mathcal{S}(X)$;
3) $\max(a, b)$ on the set of real numbers $\mathbb{R}$;
4) $\max(a, b)$ on the set of nonnegative real numbers $\{x \in \mathbb{R}, \quad x \geq 0\}$;
5) vector product of vectors in 3-dimensional space;
6) (a, b) on the set of natural numbers $\mathbb{N}$ (here (k, l) is the greatest common divisor of k and l);
7) $\mathrm{LCM}(a, b)$ on the set of natural numbers $\mathbb{N}$ (here $\mathrm{LCM}(k, l)$ is the least common multiple of k and l);
8) a^b on the set of nonnegative integers $\{x \in \mathbb{Z}, \quad x \geq 0\}$;
9) $A \cup B$ on $\mathcal{B}(\Omega)$ (here $\mathcal{B}(\Omega)$ is the set of all subsets of a given set Ω);
10) $A \cap B$ on $\mathcal{B}(\Omega)$;
11) symmetric difference of two sets $A \oplus B = (A \setminus B) \cup (B \setminus A)$ on $\mathcal{B}(\Omega)$.

Def 1.5 Let $\varepsilon \in A$ be the neutral element for an operation $*$, $a \in A$. An element $b \in A$ is called *inverse* for a if $a * b = b * a = \varepsilon$. The inverse element is usually denoted by a^{-1}.

Remark For commutative operation sometimes the operation is denoted by plus (+), the neutral element is denoted by 0 and the inverse element is denoted $-a$ (then it is called *opposite* element for a). Note that such additive notations are used only for commutative operations!

$\diamond$ **1.5** 1) Prove that if the operation is associative then any element $a \in A$ has at most one inverse.
2) Prove that if the operation is associative and a^{-1} and b^{-1} exist then $\exists\ (ab)^{-1} = b^{-1}a^{-1}$.

$\diamond$ **1.6** Prove that a mapping $f : X \to X$ has an inverse mapping (under composition) if and only if f is bijective.

$\diamond$ **1.7** For which of the examples of $\diamond$1.4 each element has its inverse?

$\diamond$ **1.8** Prove that a remainder $\bar{a} \in \mathbb{Z}_n$ is invertible (under multiplication) if an only if a and n are relatively prime (i.e. $(a,n) = 1$).

Def 1.6 *Group* is a set G with an associative binary operation having neutral element ε such that any element of G has its inverse.

For finite groups $|G|$ is called the *order* of the group G.

$\diamond$ **1.9** 1) Prove that $\mathcal{S}(X)$ is a group (under composition).
2) Prove that $\mathbb{Z}_n$ is a group under addition.
3) Prove that $\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n \quad , \quad \bar{a} \text{ is invertible}\}$ is a group (under multiplication).
4) $\mathrm{GL}(n,\mathbb{K})$ is the set of all non-degenerate $n \times n$ matrices over a field $\mathbb{K}$ and $\mathrm{SL}(n,\mathbb{K}) = \{A \in \mathrm{GL}(n,\mathbb{K}) \quad , \quad \det A = 1\}$. Prove that $\mathrm{GL}(n,\mathbb{K})$ and $\mathrm{SL}(n,\mathbb{K})$ are groups (under multiplication of matrices).

The group $\mathcal{S}(X)$ for the standard set $X = \{1,2,\dots,n\}$ is denoted by $\mathcal{S}_n$ and is called *permutation* group.

$\diamond$ **1.10** 1) $|\mathcal{S}_n| = ?$ *2) $\mathrm{GL}(n,\mathbb{F}_p) = ?$ *3) $\mathrm{SL}(n,\mathbb{F}_p) = ?$

Def 1.7 Group G is called *abelian* or *commutative* if its operation is commutative.

Note that for abelian groups additive notations are sometimes used.

$\diamond$ **1.11** Give example of a set G with a commutative binary operation having neutral element ε such that any element of G has its inverse but G is not a group.

$\diamond$ **1.12** 1) Prove that in a group G any equation of the form $ax = b$ and $xa = b$ have a unique solution.
2) Prove that a set G with an associative binary operation is a group if any equation of the form $ax = b$ and of the form $xa = b$ has a unique solution.

$\diamond$ **1.13** Prove that if $\forall\, a \in G \quad a^2 = \varepsilon$ then G is abelian.

Def 1.8 A group G is called *cyclic* if $\exists a \in G$ such that $\forall b \in G \quad b = a^n$ for certain $n \in \mathbb{Z}$. Such a is called the *generator* of G.

$\diamond$ **1.14** 1) Prove that $\mathbb{Z}$ and $\mathbb{Z}_n$ (under addition) are cyclic groups.
2) List all the generators of $\mathbb{Z}$ and $\mathbb{Z}_n$ for $n \leq 10$.
3) Give a necessary and sufficient condition for $\bar{a} \in \mathbb{Z}_n$ to be a generator of $\mathbb{Z}_n$.

$\diamond$ **1.15** 1) Which of the groups $\mathbb{Z}_n^*$ (see $\diamond$1.9.3), $n = 3,4,5,\dots,11,12$ are cyclic?
*2) Prove that for p prime $\mathbb{Z}_p^*$ is cyclic.

$\diamond$ **1.16** 1) Give an example of a finite group which is not cyclic.
2) Give an example of an infinite group which is not cyclic.

Def 1.9 A subset H of a group G is called *subgroup* if H is also is group under the same operation.

Note that this definition implies that $\forall\, a,b \in H \quad ab \in H$, $a^{-1} \in H$ and $\varepsilon \in H$; and these three conditions are sufficient for H to be a subgroup.

$\diamond$ **1.17** Find cyclic subgroups in the following groups:
1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under addition;
2) $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ under multiplication.
3) Which of these groups contain finite cyclic subgroups? Which of these groups contain finite cyclic subgroups of arbitrary order?

⋄ **1.18** 1) Prove that any subgroup of a cyclic group is cyclic.
2) Prove that if G is a cyclic group, $|G| = n$, H is a subgroup of G, $|H| = k$, then $k \mid n$.
3) Prove that if G is a cyclic group, $|G| = n$, $k \mid n$. Then G has exactly one subgroup H of order k.

⋄ **1.19** Let G be a group, $a \in G$. Consider the set $H = \{a^n \quad , \quad n \in \mathbb{Z}\}$. Prove that
1) H is a subgroup of G;
2) H is the minimal subgroup of G containing a (i.e. any subgroup of G, containing a, contains H);
3) H is cyclic group and a is its generator.

Def 1.10 The subgroup H defined in ⋄1.19 is called the *cyclic subgroup generated by* a. We shall denote this subgroup by $\langle a \rangle$. If $\langle a \rangle$ is finite then its order is called *the order of the element* a and denoted by $\operatorname{ord} a$. For $\langle a \rangle$ infinite we put $\operatorname{ord}(a) = \infty$.

⋄ **1.20** Let G be a group, $a, b \in G$. Prove the following statements.
1) $\operatorname{ord}(a) = \operatorname{ord}(b^{-1}ab)$.
2) If $a^m = \varepsilon$ then $\operatorname{ord}(a) \mid m$.
3) If m and $\operatorname{ord}(a)$ are relatively prime then $\operatorname{ord}(a^m) = \operatorname{ord}(a)$.
4) If $m \mid \operatorname{ord}(a)$ then $\operatorname{ord}(a^m) = \frac{\operatorname{ord}(a)}{m}$.
5) $\forall m$ $\operatorname{ord}(a^m) = \frac{\operatorname{ord}(a)}{(\operatorname{ord}(a),m)}$. ($(k,l)$ is the greatest common factor of k and l.)
6) If $ab = ba$ then $\operatorname{ord}(ab) \mid \operatorname{LCM}(\operatorname{ord}(a), \operatorname{ord}(b))$ ($\operatorname{LCM}(k,l)$ is the least common multiple of k and l.)
*7) $\forall k, m, n$ find an example of a group G and elements $a, b \in G$ such that $\operatorname{ord}(a) = k$, $\operatorname{ord}(b) = m$, $\operatorname{ord}(ab) = n$. ($n = \infty$ is also possible!)

Def 1.11 Two groups G and L are called *isomorphic* if there exists a bijection $f : G \to L$ such that $\forall\ a, b \in G \quad f(ab) = f(a)f(b)$. This is denoted by $G \cong L$. The bijection f is called an *isomorphism*.

⋄ **1.21** Let $f : G \to L$ be an isomorphism. Prove that
1)$f(\varepsilon_G) = \varepsilon_L$ and $f(a^{-1}) = f(a)^{-1}$; 2) $\operatorname{ord} a = \operatorname{ord} f(a)$;
3) H is a subgroup of G $\Leftrightarrow$ $f(H)$ is a subgroup of L.

⋄ **1.22** Prove that any cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$.

⋄ **1.23** Consider following groups of order 4: $\mathbb{Z}_4$, $\mathbb{Z}_5^*$, $\mathbb{Z}_8^*$, $\mathcal{B}(\Omega)$ under $\oplus$ for $|\Omega| = 2$ (see ⋄1.4.11). Which of these groups are pairwise isomorphic?

⋄ **1.24** Prove that any cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$.

⋄ **1.25** 1) Prove that any group of order 2 is isomorphic to $\mathbb{Z}_2$.
2) Prove that any group of order 3 is isomorphic to $\mathbb{Z}_3$.
*3) Classify (up to an isomorphism) groups of order 4.

Def 1.12 Consider two groups H and K. Define the operation on the direct product of the sets $H \times K$ by

$$(h; k) \cdot (h'; k') = (hh'; kk').$$

Prove that $H \times K$ is a group under this operation. This group is called the direct product of the groups H and K.

⋄ **1.26** Suppose that a group G contains two subgroups H and K, such that:
1) $H \cap K = \{\varepsilon\}$ (ε is the unit element of the group G);
2) $\forall h \in H$ and $\forall k \in K \quad h \cdot k = k \cdot h$;
3) $\forall g \in G$ may be expressed as $g = h \cdot k$ for some $h \in H$ and $k \in K$.
Then $G \cong H \times K$.

◇ **1.27** Consider the groups $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$, $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$, $\mathbb{R}^*_+ = \{x \in \mathbb{R}, \quad x > 0\}$, $\mathbb{S}^1 = \{z \in \mathbb{C}, \quad |z| = 1\}$, $\{\pm 1\}$ under multiplication.
1) Prove that $\mathbb{R}^* \cong \mathbb{R}^*_+ \times \{\pm 1\}$.
2) Prove that $\mathbb{C}^* \cong \mathbb{R}^*_+ \times \mathbb{S}^1$.

◇ **1.28** (1) For which m and n $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$?

(2) **Theorem.** Any finite group is isomorphic to a direct product of cyclic groups. (We shall prove this theorem later.)

(3) Classify abelian groups of order 8, 12, 16, 24, 36.

(4) Represent all the non-cyclic groups from ◇1.15 as direct products of cyclic groups.

(5) Let G be a finite abelian group. Prove that G is isomorphic to a direct product $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ where $n_i \mid n_{i+1}$ for $i = 1, 2, \ldots, k-1$. Prove that the sequence of integers $n_1, n_2, \ldots, n_k$ is uniquely defined by G.

◇ **1.29** 1) Find the orders of all elements of $\mathcal{S}_3$ and $\mathcal{S}_4$.
2) Find all cyclic subgroups of $\mathcal{S}_3$ and $\mathcal{S}_4$.
*3) Find all subgroups of $\mathcal{S}_3$ and $\mathcal{S}_4$.
*4) Is $\mathcal{S}_3$ or $\mathcal{S}_4$ isomorphic to a direct product of some groups?

◇ **1.30** Consider the Euclidean plane Π. The group $\mathcal{S}(\Pi)$ is very huge but it contains interesting smaller subgroups. Denote by $\mathbb{E}$ the subgroup of $\mathcal{S}(\Pi)$ consisting of the mappings $f \in \mathcal{S}(\Pi)$ which preserve distance between any two points: $\forall\ A, B \in \Pi \quad |AB| = |f(A)f(B)|$. (Here $|AB|$ means the distance between A and B.) The group $\mathbb{E}$ is very important for geometry but it is still too big for the beginners. Fix a regular polygon P_n with n sides and consider all the mappings from $\mathbb{E}$ which preserve the P_n. These mappings form the *dihedral* group D_n.
1) Prove that D_n is a finite group and find its order. Give a geometrical description of all the elements of D_n.
2) Let a be a rotation, let s be a reflection in a line l passing through the center of the rotation a. Prove that $sas = a^{-1}$.
3) Find the orders of all elements of D_n.
4) Find all cyclic subgroups of D_n.
*5) Find all subgroups of D_3 and D_4.
6) Is $D_{2n} \cong D_n \times \mathbb{Z}_2$? (The answer depends on n.)

◇ **1.31** 1) Consider four matrices from $\mathrm{GL}(2, \mathbb{C})$:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Consider the set $Q_8 \subset \mathrm{GL}(2, \mathbb{C})$, $Q_8 = \{\pm E, \pm I, \pm J \pm K\}$. Prove that Q_8 is a subgroup in $\mathrm{GL}(2, \mathbb{C})$.
2) Find the orders of all elements of Q_8.
3) Find all cyclic subgroups of Q_8.
*4) Find all subgroups of Q_8.
5) Is $D_4 \cong Q_8$?
6) Is Q_8 isomorphic to a direct product of some groups?

◇ **1.32** Which of these groups are pairwise isomorphic?
1) S_3, D_3, $\mathrm{GL}(2, \mathbb{F}_2)$; 2) D_8, $D_4 \times \mathbb{Z}_2$, $Q_8 \times \mathbb{Z}_2$;
3) S_4, D_{12}, $D_6 \times \mathbb{Z}_2$, $D_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $D_3 \times \mathbb{Z}_4$, $Q_8 \times \mathbb{Z}_3$.