2. Homomorphisms.

Def 2.1 Let G and H be groups. *Homomorphism* is a mapping $f : G \to H$ such that $\forall a, b \in G$ $f(a \cdot b) = f(a) \cdot f(b)$.
The *kernel* of the homomorphism f is $\operatorname{Ker} f = \{g \in G \text{ such that } f(g) = \varepsilon\} \subset G$.
The *image* of the homomorphism f is $\operatorname{Im} f = \{h \in H \text{ such that } h = f(g) \text{ for some } g \in G\} \subset H$.

◇ **2.1** Let $f : G \to H$ be a homomorphism. Prove that
a) $f(\varepsilon) = \varepsilon$; b) $\forall a \in G$ $f(a^{-1}) = f(a)^{-1}$; c) $\forall a \in G$ $\operatorname{ord}(f(a)) \mid \operatorname{ord}(a)$.

◇ **2.2** Let $f : G \to H$ be a homomorphism. Prove that
a) $\operatorname{Ker} f$ is a subgroup in G; b) $\operatorname{Im} f$ is a subgroup in H;
c) Can any given subgroup of G be a kernel of some homomorphism?
d) Can any given subgroup of H be an image of some homomorphism?

◇ **2.3** Let $f : G \to H$ be a homomorphism. Prove that
a) f is injective $\Leftrightarrow$ $\operatorname{Ker} f = \{\varepsilon\}$; b) f is surjective $\Leftrightarrow$ $\operatorname{Im} f = H$;
c) f is isomorphism $\Leftrightarrow$ $\operatorname{Ker} f = \{\varepsilon\}$ and $\operatorname{Im} f = H$.

◇ **2.4** Verify that the following mappings are homomorphisms. Find $\operatorname{Ker} f$ and $\operatorname{Im} f$.
a) $f : \mathbb{R}^* \to \mathbb{R}^*$ where $f(x) = x^2$; b) $f : \mathbb{R}^* \to \mathbb{R}^*$ where $f(x) = x^3$;
c) $f : \mathbb{R}^* \to \mathbb{R}^*$ where $f(x) = |x|$; d) $f : \mathbb{C}^* \to \mathbb{R}^*$ where $f(x) = |x|$;
e) $f : \mathbb{R} \to \mathbb{C}^*$ where $f(x) = \cos x + i \sin x$; f) $f : \mathbb{C} \to \mathbb{C}^*$ where $f(x) = e^x$;
g) $f : \mathbb{Z} \to \mathbb{C}^*$ where $f(x) = (1+i)^x$; h) $f : \mathbb{Z} \to \mathbb{C}^*$ where $f(x) = (\frac{1+i}{\sqrt{2}})^x$.

◇ **2.5** Let G be an abelian group, $m \in \mathbb{N}$. Then the mapping $f : G \to G$, $f(x) = x^m$ is a homomorphism. Is the same statement true for non-abelian G?

◇ **2.6** Classify homomorphisms: a) $f : \mathbb{Z} \to \mathbb{Z}_n$; b) $f : \mathbb{Z}_n \to \mathbb{Z}$; c) $f : \mathbb{Z}_n \to \mathbb{Z}_n$; d) $f : \mathbb{Z}_m \to \mathbb{Z}_n$.

◇ **2.7** a) Let G be a group. We know that $\mathcal{S}(G) = \{$ bijections $\varphi : G \to G\}$ forms a group under composition. Prove the Cayley's theorem: the mapping $f : G \to \mathcal{S}(G)$ defined by the formula $f(a)(x) = ax$ is an injective homomorphism.
b) Prove that the image of the Cayley homomorphism for $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ is the Klein 4-group in $\mathcal{S}_4$.

◇ **2.8** a) Consider a regular hexagon. Let us enumerate it's vertices. Then any isomerty from D_6 defines a permutation in $\mathcal{S}_6$. Prove that this construction defines a homomorphism $f : D_6 \to \mathcal{S}_6$. Find $\operatorname{Ker} f$ and $\operatorname{Im} f$.
b) Let us now enumerate three major diagonals of the hexagon. Prove that we get a homomorphism $f : D_6 \to \mathcal{S}_3$ and find $\operatorname{Ker} f$ and $\operatorname{Im} f$.
c) Next let us enumerate four major diagonals of the octagon. Prove that we get a homomorphism $f : D_8 \to \mathcal{S}_4$ and find $\operatorname{Ker} f$ and $\operatorname{Im} f$.

Def 2.2 An isomorphism $f : G \to G$ is called an *automorphism* of the group G.

◇ **2.9** Prove that the set of all automorphisms of a given group G is a subgroup of $\mathcal{S}(G)$. This subgroup is denoted by $\operatorname{Aut} G$.

◇ **2.10** a)-i) Find $\operatorname{Aut} \mathbb{Z}_n$ for $n = 2, 3, \ldots, 9, 10$. j) Prove that $|\operatorname{Aut} \mathbb{Z}_n| = \varphi(n)$.
*k) Prove that for prime p the group $\operatorname{Aut} \mathbb{Z}_p$ is cyclic.

◇ **2.11** Prove that $\operatorname{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathcal{S}_3$.

◇ **2.12** Consider a regular polytope in the Euclidean 3-space (tetrahedron, cube, octahedron, dodecahedron or icosahedron). For each of them consider the group G of all orientation preserving isometries of the 3-space preserving the given polytope. Find $|G|$ and the orders of all elements of G. Enumerating vertices, edges or faces of the polytope construct homomorphisms from G to permutation groups. For each polytope suggest the best version of enumeration to determine the structure of G.

3. The Lagrange theorem.

Def 3.3 Let H be a subgroup of G, $g \in G$. *Left coset* is the set $gH = \{gh, \quad h \in H\}$; *right coset* is the set $Hg = \{hg, \quad h \in H\}$.

◇ **3.13** Let H be a subgroup of G, $a, b \in G$. Then either $ah = bH$, or $aH \cap bH = \emptyset$.

◇ **3.14** Prove the *Lagrange theorem:* If G is finite group and H is a subgroup of G then the order of H is the divisor of the order of G.

◇ **3.15** a) If $|G| < \infty$, $a \in G$, then $\mathrm{ord}(a)$ is the divisor of the order of G.
b) $a^{|G|} = e$.

◇ **3.16** a) Prove that if $a, p \in \mathbb{Z}$, p — prime, $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$ *(The "Little" Fermat theorem).*
b) Prove that if $a, n \in \mathbb{Z}$, $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{p}$,
where $\varphi(n) = |\mathbb{Z}_n^*| = |\{k \in \mathbb{Z}, \quad 0 < k < n, \quad (k, n) = 1\}|$ — *the Euler function.*

◇ **3.17** Prove that if $|G| = p$ and p is prime then $G \cong \mathbb{Z}_p$.

◇ **3.18** Classify groups of order 4 (up to an isomorphism).

◇ **3.19** Find all non-cyclic subgroups of
a) D_4; b) Q_8; c) D_6; *d) $\mathcal{S}_4$.

Def 3.4 *Left quotient set* = { the set of all left cosets } = G/H.
Right quotient set = { the set of all right cosets } = $H\backslash G$.
(So for $|G| < \infty \quad |G/H| = |H\backslash G| = \frac{|G|}{|H|}$.)

Def 3.5 If the quotient set G/H is finite, the integer $|G/H|$ is called the *index* of the subgroup H (and H is called *a finite index subgroup*).

◇ **3.20** Prove the relative version of the Lagrange theorem: if $G \supset H \supset K$ — subgroups of finite index, then $|G/K| = |G/H| \cdot |H/K|$.

◇ **3.21** Give an example of a group G and it's subgroup H such that $gH \neq Hg$ for some $g \in G$.

Def 3.6 A subgroup H of a group G is called *normal subgroup* if if $gH = Hg$ $\forall g \in G$. (This is usually denoted as $H \lhd G$).

◇ **3.22** Prove that $H \lhd G \Leftrightarrow \forall g \in G \; \forall h \in H \; ghg^{-1} \in H$.

◇ **3.23** Prove that $(G : H) = 2 \Rightarrow H \lhd G$.

◇ **3.24** Prove that a kernel of a homomorphism is normal subgroup.

◇ **3.25** *Center* of a group G is the set $Z(G) = \{ a \in G \text{ such that } ag = ga \; \forall \; g \in G \}$.
a) Prove that $Z(G)$ is a normal subgroup in G.
b) Find $Z(Q_8)$. b) Find $Z(\mathcal{S}_3)$. c) Find $Z(\mathcal{S}_4)$. d) Find $Z(D_n)$. (The answer depends on n.)

◇ **3.26** Find all normal subgroups of
a) Q_8; b) D_4; b) D_6; c) $\mathcal{S}_3$; d) $\mathcal{S}_4$.

◇ **3.27** a) Fix an element $a \in G$. Prove that the mapping $\varphi_a : G \to G$ defined by $\varphi_a(g) = a^{-1}ga$ is an automorphism of the group G. Such φ_a is called an *internal automorphism* of G.
b) Prove that the set of all internal automorphisms $\mathrm{Int}\, G$ of the group G is a normal subgroup of $\mathrm{Aut}\, G$.

◇ **3.28** Find $\mathrm{Int}\, G$ and $\mathrm{Aut}\, G$ for
a) $G = \mathcal{S}_3$; b)) $G = D_4$; *c) $G = Q_8$.