MATH-F-303 handout 1: group theory

Rules: Exam problems would be similar to ones marked with ! sign. It is recommended to solve all unmarked and !-problems or to find the solution online. It's better to do it in order starting from the beginning, because the solutions are often contained in the previous problems. The problems with * are harder, and ** are very hard; don't be disappointed if you can't solve them, but feel free to try. Have fun!

1.1 Bijective maps and permutations

Definition 1.1. A map $f : A \to B$ from the set A to B is **injective** if it puts different elements to different ones, and **surjective** if for each element $b \in B$ there is some $a \in A$ such that $f(a) = b$. A map f is **bijective** or **one to one** or **1-to-1** if it is injective and surjective.

Definition 1.2. Let A be a set (finite or not). Denote by $\Sigma(A)$ the set of all bijective maps from A to itself. For any $f, g \in \Sigma(A)$, a composition of f and g is denoted by $f \circ g$,

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

The set $\Sigma(A)$ equipped with such an operation is called **the group of permutations of elements of** A. The identity map is denoted by Id_A: it is a permutation which maps a to a for each $a \in A$. Sometimes it is denoted as 1_A or just Id. When A is a finite set of n elements, the permutation group is called **symmetric group** and denoted by Σ_n.

Remark 1.1. One can write permutations as a table: for instance, the permutation $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 1$, $4 \mapsto 2$ on the set $A = \{1, 2, 3, 4\}$ is written as $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$.

Exercise 1.1. a. Find the number of elements in the set Σ_5.

b. How many of these map 1 to 5?

c. For how many of $\sigma \in \Sigma(A)$ one has $\sigma(1) < \sigma(2)$?

d. For how many of $\sigma \in \Sigma(A)$ $\sigma(1) < \sigma(2) < \sigma(3)$?

Exercise 1.2. Find the number of elements in the set Σ_n. for any $n = 1, 2, 3, ...$

Remark 1.2. For any permutation $f \in \Sigma(A)$ there exists a unique "inverse permutation" f^{-1} satisfying $f \circ f^{-1} = f^{-1} \circ f = \mathsf{Id}_A$.

Definition 1.3. Order of a permutation $\sigma \in \Sigma(A)$ is the smallest $n \in \mathbb{Z}^{\geqslant 1}$ such that $\sigma^n = \mathsf{Id}_A$. If such number does not exist, we say that its order is **infinite**.

Exercise 1.3. Let $\sigma \in \Sigma_n$. Prove that order of σ is finite.

Definition 1.4. Cyclic permutation of the set $a, b, c, d, \dots, w$ maps a to b, b to c and so on up to v to w and w to a. This permutation is denoted as $(a, b, c, d, \dots, w)$. Its order is the number of elements in parentheses. This notation makes sense if $A = \{a, b, c, ..., w\}$ and if $A \subsetneq \{a, b, c, ..., w\}$.

Exercise 1.4. Let $\sigma \in \Sigma_4$ be a permutation of order 3. Prove that $\sigma = (abc)$.

Exercise 1.5. Let $\sigma = (123)$, $\tau = (34)$. Express the permutation $\tau \circ \sigma \circ \tau^{-1}$ in cyclic notation.

Definition 1.5. Transposition is a permutation written as (ab), that is, a permutation which exchanges a and b and fixes the rest of the elements.

Exercise 1.6. Prove that each permutation of a finite set can be expressed as a product of transpositions.

Exercise 1.7 (*). Find a permutation of an infinite set which cannot be expressed as a product of transpositions

1.2 Groups: axiomatic definition

The permutation group is equipped with a number of algebraic structures: the product map, taking the inverse, the identity element. This is a situation which can be put into axioms as follows.

Definition 1.6. Let G be a set equipped with the following data:

(a) an operation of "multiplication" $G \times G \longrightarrow G$ denoted as $f, g \mapsto fg$ or $f, g \mapsto f \cdot g$

(b) "taking the inverse" a map $f \mapsto f^{-1}$ from G to itself

(c) "unity": we fix the unity element $1_G \in G$.

Suppose that these data satisfy the following axioms.

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

"Unity": $f \cdot 1_G = 1_G \cdot f = f$ for all $f \in G$.

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

Then G is called **a group**. A subset of G which is closed with respect to these operations is called **a subgroup of** G.

Exercise 1.8. Let G be a group, $f, g \in G$.

a. Let $fg = f$. Prove that $g = 1_G$.

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

Remark 1.3. This implies that the group structure on G is uniquely determined by the multiplication map. The unity and the inverse are recovered from the multiplication uniquely.

Exercise 1.9. Find whether the following sets equipped with a binary operation are groups.

a. Natural numbers with the operation of addition.

b. Integer numbers with the operation of addition.

c. Integer numbers with the operation of multiplication.

d. Rational numbers with the operation of multiplication.

e. Rational numbers with the operation of substraction.

f. Isometries of the plane $\mathbb{R}^2$ with the operation of composition.

g. Numbers $u, v \in]-1, 1[$ with operation $u \cdot v = (u + v)/(1 + uv)$.

h. Subsets of $\mathbb{R}^2$ with the operation $X, Y \longrightarrow X \cup Y$ (taking the union).

i. Subsets of $\mathbb{R}^2$ with the operation of taking the symmetric difference: $A, B \longrightarrow (A \cup B)\backslash(A \cap B)$.

j. Maps from a fixed set S to a group G with the operation $(f \cdot g)(s) = f(s)g(s)$, $s \in S$, $f, g \in G$.

Definition 1.7. Group product of groups G_1 and G_2 is the set $G_1 \times G_2$ with the group operation

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

A map $\phi : G \longrightarrow G'$ from the group G to G' is called **a homomorphism** if it is compatible with the product: $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$. A homomorphism is called **a monomorphism** if it is injective, **an epimorphism** if it is surjective and **an isomorphism** ig it is bijective. Groups G_1, G_2 are **isomorphic** if there exists an isomorphism from G_1 to G_2. An isomorphism from a group to itself is called **an automorphism**.

Exercise 1.10. Suppose that $\phi : G \to G'$ is a group homomorphism. Prove that $\phi(1_G) = 1_{G'}$ and $\phi(g^{-1}) = \phi(g^{-1})$ for any $g \in G$.

Exercise 1.11. Prove that automorphisms of a group with the composition operation form a group.

Exercise 1.12. Let $g \in G$ be an element. Consider the following map $\phi_g : G \longrightarrow G$, with $\phi_g(x) = gxg^{-1}$. Prove that this is an automorphism of G.

Exercise 1.13 (*). Prove that the group of automorphisms of the symmetric group Σ_3 is isomorphic to Σ_3.

Definition 1.8. Consider a homomorphism $G \longrightarrow \Sigma(A)$ from a group G to the group $\Sigma(A)$ of bijective self-maps (permutations) on A. Such a homomorphism is called **action of G on A**. One also says that G **acts on** A. Indeed, in this case each element of G permutes somehow the elements of A. An action of G on A can be written as a map $G \times A \overset{\rho}{\to} A$, with $g \mapsto \rho(g, a)$ or $g \mapsto \rho(g)a$. Often an action of a group on a set is written simply as $a, g \mapsto g(a)$.

Exercise 1.14 (!). (Cayley's theorem)
Prove that any group G admits an injective homomorphism to the group $\Sigma(G)$ of permutations of G.

Hint. Meditate on a possible meaning of a phrase "a group acts on itself by the left multiplication".

Exercise 1.15. Prove that

a. Any group of two elements is isomorphic to the permutation group Σ_2.

b. (*) Any non-commutative group of six elements is isomorphic to the premutation group Σ_3.

Exercise 1.16 (*). Prove that the permutation group Σ_n is not isomorphic to a product of two non-trivial groups.

Exercise 1.17. Let G be a finite group, and $g \in G$ its element. We denote by g^i the product of g with itself i times. Show that the sequence $g, g^2, g^3, \ldots$ is periodic.

Definition 1.9. For any group element $g \in G$, **order of** g is the smallest integer number $n > 0$ such that $g^n = 1$. If there are no such integer, we say that g **is of infinte order**. **Order** of a group G is the umber of its elements.

Exercise 1.18 (!). Let G be a finite group of order n. Prove that order of any $g \in G$ divides n.

Hint. Let d be the order of g. Consider G as a union of subsets $\langle g \rangle x := \{x, gx, g^2x, ...g^{d-1}x\}$. Prove that all $\langle g \rangle x$ are disjoint or coincide, all of these sets have cardinality d.

Exercise 1.19. Let G be a group of even order. Prove that G contains an element of order 2.

Exercise 1.20 (*). Is it true that...

a. The group D_{12} of isometries of a regular dodecagon is isomorphic to the product $D_6 \times S_2$, where D_6 is the group of isometries of a regular hexadon.

b. The group D_6 is isomprhic to the product $D_3 \times S_2$, where D_3 is the group of isometries of a regular hexagon.

Definition 1.10. A group G is called **commutative**, or **abelian**, if $ab = ba$ for all $a, b \in G$. Two elements $a, b \in G$ **commute** if $ab = ba$.

Exercise 1.21. Center of a group G is the set of all $x \in G$ such that x commutes with all $y \in G$. Prove that the center is a subgroup.

Exercise 1.22 (*). Let G be a group of order p^2, where p is prime. Prove that G is abelian.

Exercise 1.23 (*). Construct a non-abelian group of order p^3 for $p = 2$ and $p = 3$.