Groups; permutation groups

Lecture 1

Groups: main properties and examples. Lagrange Theorem and corollaries.

DEFINITION 1. A set G with an operation $*$ is called a *group*, if the following properties hold:

1) $\forall x, y, z \in G \ (x * y) * z = x * (y * z)$ (associativity);

2) $\exists e \in G \forall x \in G \ e * x = x * e = x$ (this element e is called a *unity* of the group G);

3) $\forall x \in G \exists y \in G \ x * y = y * x = e$ (this element y is called *inverse* for x and is denoted by x^{-1}).

If in the group G additionally the property of *commutativity*

$$\forall x, y \in G \ x * y = y * x$$

holds, then G is called an *Abelian group*.

The sign $*$ is often omitted, the result of applying the operation $*$ to the elements x and y can be written by xy.

PROBLEM 1. In any group a unity is unique.

PROBLEM 2. In a group G for any elements $a, b \in G$ a solution of the equation

$$ax = b \quad (xa = b)$$

exists and is unique.

PROBLEM 3. Find examples of groups of 2, 3, 4 elements. Find and example of any non-Abelian group. Is there any non-Abelian group of 4 elements?

DEFINITION 2. Two groups $(G, *)$ and $(H, \circ)$ are called *isomorphic*, if there exists a one-to-one mapping $\Phi : G \to H$ such that

$$\forall x, y \in G \ \Phi(x * y) = \Phi(x) \circ \Phi(y).$$

PROBLEM 4. The relation *to be isomorphic groups* is an equivalence relation.

PROBLEM 5. Find all groups of 2, 3, 4 elements which are not isomorphic to each other.

PROBLEM 6. What following sets with operations are groups?

a) $(A, +)$, where A is one of the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$;

b) $(A, \cdot)$, where A is one of the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$;

c) $(A_0, \cdot)$, where A is one of the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $A_0 = A \setminus \{0\}$;

d) the numbers $\{0, 1, 2, \ldots, n-2, n-1\}$ with the operation of addition modulo n;

e) the numbers $\{1, 2, \ldots, n-2, n-1\}$ with the operation of multiplication modulo n?

PROBLEM 7. What of the following sets of mappings from the set $M = \{1, 2, \ldots, n\}$ into itself form a group (under the operation of composition):

a) the set of all mappings;

b) the set of all injective (surjective, bijective) mappings?

Definition 3. The group from the part b) of the previous problem is called the *permutation group of the order* n and is denoted by $\mathbf{S}_n$.

Problem 8. How many elements are there in the group $\mathbf{S}_n$?

Problem 9. Is the group $\mathbf{S}_n$ Abelian?

Problem 10. Introduce the natural notion of *degree* of an element $g \in G$: g^k. Proof usual properties of degree: $(g^n)^m = g^{nm}$, $g^n g^m = g^{n+m}$. Does the property $g^n h^n = (gh)^n$ hold?

Definition 4. A subset H of a group G is called a *subgroup*, if

$$\forall x, y \in H \; xy \in H \wedge x^{-1} \in H.$$

Problem 11. The following two statements about a subset H of a group G are equivalent:
1) H is a subgroup of G;
2) $\forall x, y \in H \; xy^{-1} \in H$.

Problem 12. Prove that any finite subset of a group closed under multiplication is a subgroup. Is it true for infinite subsets?

Problem 13. Find all subgroups of the group of integer numbers $(\mathbb{Z}, +)$; of the permutation group $\mathbf{S}_3$.

Definition 5. Let H be a subgroup of a group G, $g \in G$. Then the *right* (*left*) *residue class of* g *by* H is the set

$$gH = \{gh \mid h \in H\} \quad (Hg = \{hg \mid h \in H\}).$$

Problem 14. Let G be a group, H its subgroup, $g_1, g_2 \in G$. Then either $g_1H = g_2H$, or $g_1H \cap g_2H = \emptyset$.

Problem 15. Let g_1, g_2 be elements of a group G and H_1, H_2 be subgroups of G. Prove that the following properties are equivalent:
a) $g_1H_1 \subseteq g_2H_2$; b) $H_1 \subseteq H_2$ and $g_2^{-1}g_1 \in H_2$.

Problem 16. Let g_1, g_2 be elements of a group G, H_1, H_2 be subgroups of G. Prove that the nonempty set $g_1H_1 \cap g_2H_2$ is the left residue class of G by $H_1 \cap H_2$.

Problem 17 *. Let H be a subgroup of a group G, $g_1, g_2 \in G$, $g_1H \subseteq Hg_2$. Is it true that $g_1H = Hg_2$?

Problem 18 (Lagrange Theorem). If G is a finite group, H is its subgroup, then the number of right (left) residue classes of G by H is $|G| : |H|$ (this number is called the *index* of H in G). Therefore the order of a subgroup always divides the order of a group.

Definition 6. The *order* of an element g of a group G is the minimal natural number $n > 0$ such that $g^n = e$. If such a number does not exist, the order of g is supposed to be infinite.

Problem 19. In a finite group the order of any element divides the order of the group.

Problem 20 (Small Fermat Theorem). For any simple number p and any natural a

$$a^p \equiv a \mod p.$$

Problem 21. Find all non-isomorphic groups of the order p (p is simple).

Problem 22. If in a group G for any $g \in G$ we have $g^2 = e$, then $G$is an Abelian group.

Problem 23. Find all non-isomorphic groups of the order 6.

Problem 24. Find an example of an infinite non-Abelian group.

Problem 25. Is there an infinite group with all elements of finite order?

Problem 26. Find all finite groups containing the greatest proper subgroup.