MATH 10
ASSIGNMENT 23: ORDER OF AN ELEMENT
APR 2, 2023

Summary of previous results

Let $H \subset G$ be a subgroup. For any element $g \in G$, define the subset

$$[g] = gH = \{gh, h \in H\}$$

Subsets of this form are called *cosets*. Note that two different elements can define the same coset.

Theorem. *If G is a finite group, and H is a subgroup,*

$$|G| = |H| \cdot (\textit{number of cosets})$$

In particular, $|H|$ is a divisor of $|G|$.

We will denote by G/H the set of all cosets (i.e., each coset $[g]$ is one point in G/H). For example, if $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$, then G/H is the set of all remainders mod 5: $Z/5\mathbb{Z} = \mathbb{Z}_5$.

However, in general G/H is not a group.

The previous theorem can be reformulated as follows:

$$|G| = |H| \cdot |G/H|.$$

1. Let $x \in G$. We define the order of x to be the smallest positive integer n such that $x^n = e$ (if such an n does not exist, we say that x has infinite order). For example, in the symmetric group any transposition has order 2.

Show that if $x \in G$ has order n, then the set $e, x, x^2, \ldots, x^{n-1}$ is a subgroup in G. Show also that this subgroup can be identified with group $\mathbb{Z}_n$ of remainders mod n (this is called the cyclic group of order n).

2. (a) Deduce from the previous problem the following result:
In any finite group, the order of any element divides the order of the group.
(b) Prove that if G is a finite group, then for any $x \in G$ we have $x^{|G|} = e$.

3. In the symmetric group S_{12}, find two permutations x, y such that each of them has order 2, but the product xy has order 6. Can the order of xy be 7?

4. Let G be the group of all rotations of the regular icosahedron.
(a) Find the order of G.
(b) Explain why it can not have elements of order 7
(c) For each of the following subsets, verify that it is a subgroup in G, find its order and check Lagrange's theorem
H_v=all rotations that preserve a given vertex v
H_F=all rotations that preserve a given face F
H_e=all rotations that preserve a given edge e
(d) Construct another (non-trivial) subgroup in G and verify Lagrange's theorem

5. Recall that a number k has an inverse mod n if and only if k is relatively prime with n.

Let $\mathbb{Z}_n^*$ (note the star!) be the set of all remainders mod n which are relatively prime to n; for example, $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$. Show that then $\mathbb{Z}_n^*$ is a a group with respect to multiplication.

6. Prove that if $a \in \mathbb{Z}$ is relatively prime with n, then $a^{\varphi(n)} \equiv 1 \mod n$, where $\varphi(n) = |\mathbb{Z}_n^*|$ (it is called the Euler function). Hint: use the previous problem and problem 2. Deduce from this the Fermat theorem: if p is prime, then for any $a \in \mathbb{Z}$ we have $a^p \equiv a \mod p$.

Group actions

We say that a group G *acts* on a set M if each element of a group determines a permutation of elements of M, and product in the group corresponds to product of permutations.

For example, let G be the group of all rotations of a cube; then G acts on the set of edges of the cube.

We say that the action is *transitive* if we can move any element to any other: for any two $m, m' \in M$ there exists $g \in G$ such that applying g to m we get m'.

7. Consider the group of all rotations of the icosahedron. Is its action on each of the following sets transitive?
(a) Set of all vertices
(b) Set of all edges
(c) Set of all diagonals

8. Let G act transitively on a set M. Choose an element $m \in M$ and let $H = \{g \in G \mid g(m) = m\}$ (this is called the *stabilizer* of m).
(a) Show that H is a subgroup.
(b) Show that $gm = g'm$ if and only if $[g] = [g']$ (here $[g] = gH$ denotes the coset of g). Deduce from this that we have bijection between M and the coset space G/H.
(c) Show that $|M| = |G|/|H|$.

9. Use the previous problem to count the number of all words one can get by permuting letters of the word "cangaroo". [Hint: on the set of such words, you have a transitive action of group S_8]

10. Use problem 8 to count how many ways there are to split $2n$ people in pairs. HInt: on this set, you have an action of the group S_{2n}.