MATH 10
ASSIGNMENT 24: LAGRANGE'S THEOREM
MAY 2, 2021

Summary of past results

Definition. Let G be a group. A subgroup of G is a subset $H \subset G$ which is itself a group, with the same operation as in G. In other words, H must be

1. closed under multiplication: if $H_1, h_2 \in H$, then $h_1 h_2 \in H$
2. contain the group unit e
3. for any element $h \in H$, we have $h^{-1} \in H$.

An example of a subgroup is the *cyclic subgroup* generated by an element of a group: if $a \in G$, then the set

$$H = \{a^n \mid n \in \mathbb{Z}\} \subset G$$

is a subgroup. (Note that n can be negative).

Lagrange theorem

The main result of today is Lagrange theorem:

Theorem. *If G is a finite group, and H is a subgroup, then $|H|$ is a divisor of $|G|$, where $|G|$ is the number of elements in G (also called the order of G).*

Proof. For an element $g \in G$, recall the notation $gH = \{gh,\ h \in H\}$; such subsets are called H-*cosets*. It was proved in the last homework that

- Each coset has exactly $|H|$ elements.
- Two cosets either coincide or do not intersect at all.

Thus, if there are k distinct cosets, then the total number of elements in them is $k|H|$, so $|G| = k|H|$. □

Corollary. Let G be a finite group, and let $a \in G$. Let n be the smallest positive integer such that $a^n = 1$ (this number is called the *order* of a). Then n is a divisor of $|G|$.

Proof. Let H be the cyclic subgroup generated by a; then $|H| = n$, so the result follows from Lagrange theorem. □

1. Prove that if G is a finite group, then for any $x \in G$ we have $x^{|G|} = e$.

2. Describe all subgroups in the group $\mathbb{Z}_{10}$.

3. 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.

4. 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 1.

Deduce from this Fermat's little theorem: if p is prime, then for any $a \in \mathbb{Z}$ we have $a^p \equiv a \mod p$.