MATH 10
ASSIGNMENT 22: LAGRANGE THEOREM
MAY 22, 2016

Definition. SUMMARY OF PAST RESULTS

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 is given in problem 1 below.

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). Tnen n is a divisor of $|G|$.*

Proof. Let H be the cyclic subgrou[generated by a; then $|H| = n$, so the result follows from Lagrange theorem. $\square$

1. 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.

(a) List all cosets in the case when $G = \mathbb{Z}, H = 5\mathbb{Z}$.
(b) Show that two elements x, x' are in the same coset gH iff $x' = xh$ for some $h \in H$.
(c) Show that two cosets g_1H, g_2H either coincide (if $g_1 = g_2h$ for some $h \in H$) or do not intersect at all.
(d) Show that if H is finite, then every coset has exactly $|H|$ elements.
(e) Deduce Lagrange theorem: if G is finite, then

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

2. 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 a cube.

(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

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

6. 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.

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