GROUP THEORY

5TH SEMESTER - LECTURE 3
BY

NILOFAR NAHID

DEPARTMENT OF MATHEMATICS
MAHARAJA MANINDRA CHANDRA COLLEGE

August 19, 2020

Theorem

If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal but the converse is not true.

Proof. Suppose H is a subgroup of G and $[G : H] = p$. let π_H be the permutation representation afforded by multiplication on the set of left cosets of H in G, i.e.,

$$\pi_H : G \to S_A,$$

where A be the set of all left cosets of H in G. Let $K = ker\pi_H$

$$\begin{aligned} K = ker\pi_H =& \{g \in G | \pi_H(g) = \text{identity permutation}\} \\ =& \{g \in G | \sigma_g(aH) = gaH = aH, \forall\, aH \in A\}. \end{aligned}$$

This shows that K is a subgroup of H as

$$\text{for } g \in K\ \sigma_g(H) = g \cdot H = gH = H \Rightarrow g \in H.$$

Let $[H : K] = k$. Then $[G : K] = [G : H][H : K] = pk$. Since H has p left cosets, G/K is isomorphic to a subgroup of S_p by the First Isomorphism Theorem.

Proof. By Lagrange's Theorem, $pk = |G/K|$ divides $p!$. Thus $k|p!/p = (p-1)!$. But all prime divisors of $(p-1)!$ are less than p and by the minimality of p, every prime divisor of k is greater than or equal to p (if not, then there exists a prime number $p' < p$ and it divides $|G|$ contradiction). This forces $k = 1$, so $H = K$ be a normal subgroup of G.

Converse is not true

In general, a group of order n need not have a subgroup of index p. For example A_4 has no subgroup of index 2.

Group action

In this section G is any group and we first consider G acting on itself (i.e., $A = G$) by conjugation:

$$g \cdot a = gag^{-1}, \quad \forall \quad a, g \in G,$$

where gag^{-1} is computed in the group G as usual. This definition satisfies the two axioms for a group action.

Definition.

Two elements a and b of G are said to be conjugate in G if there is some $g \in G$ such that $b = gag^{-1}$. The orbits of G acting on itself by conjugation are called the conjugacy classes of G.

Examples

1. If G is an abelian group then the action of G on itself by conjugation is the trivial action $g \cdot a = a, \forall a, g \in G$ and for each $a \in G$ the conjugacy class of a is $\{a\}$.

2. If $|G| > 1$ then, unlike the action by left multiplication, G does not act transitively on itself by conjugation because $\{e\}$ is always a conjugacy class (i.e., an orbit for this action). More generally, the one element subset $\{a\}$ is a conjugacy class if and only if $gag^{-1} = a, \forall g \in G$ if and only if a is in the center of G.

Group action

Note

If G acts on itself by conjugation and $|G| > 1$ then it does not act transitively.

Examples

In S_3 one can compute directly that the conjugacy classes are $\{e\}, \{(12), (13), (23)\}$ and $\{(123)(132)\}$.

As in the case of a group acting on itself by left multiplication, the action by conjugation can be generalized. If S is any subset of G, define

$$gSg^{-1} = \{gsg^{-1} | s \in S\}.$$

A group G acts on the set $\mathcal{P}(G)$ of all subsets of itself by defining $g \cdot S = gSg^{-1}$ for any $g \in G$ and $S \in \mathcal{P}(G)$. As above, this defines a group action of G on $\mathcal{P}(G)$. Note that if S is the one element set $\{s\}$ then $g \cdot S$ is the one element set $\{gsg^{-1}\}$ and so this action of G on all subsets of G may be considered as an extension of the action of G on itself by conjugation.

Normalizer

Let S be a subset of a group G then

$$G_S = \{g \in G | gSg^{-1} = S\} = N_G(S)$$

is the normalizer of S in G.

Orbit-Stabilizer lemma

Suppose G is a finite group which acts on A. For any $a \in A$, we have

$$|G| = |G_a||O_a|,$$

where G_a be the stabilizer of a in G and O_a be the orbit.

Proof. Fix $a \in A$. We know that G_a is a subgroup of G, and it follows from Lagrange's Theorem that the number of left cosets of $H = G_a$ in G is $[G : H] = |G|/|H|$. Let $\mathcal{L}$ denote the set of left cosets of H in G. Define a function

$$f : O_a \to \mathcal{L},$$

by

$$f(g \cdot a) = gH.$$

Proof. First, we check that f is well-defined, and at the same time check that f is injective. If $g_1, g_2 \in G, g_1 \cdot a = g_2 \cdot a \in O_a$ iff $(g_2^{-1} g_1) \cdot a = a$, iff $g_2^{-1} g_1 \in H = G_a$ which is equivalent to $g_2 H = g_1 H$. So

$$g_1 \cdot a = g_2 \cdot a$$

iff

$$f(g_1 \cdot a) = f(g_2 \cdot a),$$

and f is well-defined and injective. It is immediate that f is onto, since for any $gH \in \mathcal{L}, f(g \cdot a) = gH$. Now, f gives a one-to-one correspondence between elements of O_a and the left cosets of G_a in G. Thus, these are equal in number, and we have

$$|O_a| = |\mathcal{L}| = |G|/|G_a|,$$

which gives the desired result.

The Class Equation

Let G be a finite group and let $g_1, g_2, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : G_{g_i}|.$$

Proof. Let $x \in Z(G)$, then $O_x = \{b | b = g \cdot x\} = \{b | b = gxg^{-1}\} = \{b | b = x\} = \{x\}$. Let $Z(G) = \{e, z_2, z_3 \ldots z_m\}$, let $K_1, K_2, \ldots, K_r$ be the conjugacy classes of G not contained in the center, and let g_i be a representative of K_i for each i. Then the full set of conjugacy classes of G is given by

$$\{e\}, \{z_2\}, \ldots, \{z_m\}, K_1, K_2, \ldots, K_r.$$

Since these partition G we have

$$|G| = \sum_{i=1}^{m} 1 + \sum_{1}^{r} |K_i|$$

$$= |Z(G)| + \sum_{1}^{r} |G : G_{g_i}|.$$

This proves the class equation.

Applications of Class Equation:-

Theorem

If p is a prime and P is a group of prime power order p^α for some $\alpha \geq 1$, then P has a nontrivial center $Z(P) \neq 1$.

Proof. By the class equation

$$|P| = |Z(P)| + \sum_{i=1}^{r} |P : P_{g_i}|,$$

where

$$g_1, g_2, \ldots, g_r$$

are representatives of the distinct non-central conjugacy classes. By definition, $P_{g_i} \neq P$ for $i = 1, 2, \ldots, r$ so p divides $|P : P_{g_i}|$ (from orbit stabilizer lemma) Since p also divides $|P|$ it follows that p divides $|Z(P)|$ hence the center must be nontrivial.

Theorem

If $|P| = p^2$ for some prime p, then P is abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$.

Proof. Since $Z(P) \neq e$ hence, it follows that $P/Z(P)$ is cyclic and also P is abelian (check). If P has an element of order p^2, then P is cyclic. Assume therefore that every nonidentity element of P has order p . Let x be any nonidentity element of P and let $y \in P- < x >$. Since

$$| < x, y > | > | < x > | = p,$$

we must have that

$$P =< x, y > .$$

Both x and y have order p so

$$< x > \times < y >= Z_p \times Z_p.$$

It now follows directly that the map

$$(x^a, y^b) \rightarrow x^a y^b$$

is an isomorphism from $< x > \times < y >$ to P (check). This completes the proof.

Group action

Theorem

Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition

$$(a_1, a_2, \ldots, a_{k_1})(b_1, b_2, \ldots, b_{k_2})\ldots.$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1), \tau(a_2), \ldots, \tau(a_{k_1}))(\tau(b_1), \tau(b_2), \ldots, \tau(b_{k_2}))\ldots$$

i.e., $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.

Proof. Observe that if $\sigma(i) = j$, then

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau(j).$$

Thus, if the ordered pair i, j appears in the cycle decomposition of σ then the ordered pair $\tau(i), \tau(j)$ appears in the cycle decomposition of $\tau\sigma\tau^{-1}$. This completes the proof.

Example:

Let $\sigma = (12)(345)(6789)$ and let $\tau = (1357)(2468)$ then

$$\tau\sigma\tau^{-1} = (34)(567)(8129).$$

Definition.

1. If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$ (including its 1 -cycles) then the integers $n_1, n_2, \ldots, n_r$ are called the cycle type of σ.

2. If $n \in \mathbb{Z}^+$ a partition of n is any nondecreasing sequence of positive integers whose sum is n.