

MA 553 LECTURE NOTES: FRIDAY, FEBRUARY 8

GROUPS ACTING BY LEFT MULTIPLICATION

Definitions. Let (G, \circ) be a group, and $H \leq G$ be a subgroup – not necessarily normal in G . We consider the action of G on the left cosets $A = G/H$ via left multiplication: $g \circ (a \circ H) = (g \circ a) \circ H$. This is a transitive group action on A : If $\bar{a} = a \circ H$ and $\bar{b} = b \circ H$ are two left cosets, then let $g = b \circ a^{-1}$. It is easy to see that $g \circ \bar{a} = \bar{b}$. Hence this group action has only one orbit.

Consider the map $\pi_H : G \rightarrow S_A$ which sends g to the permutation $\sigma_g : G/H \rightarrow G/H$ defined by $\sigma_g(\bar{a}) = \bar{g \circ a}$. This is the *permutation representation associated to H* .

Proposition 1. Let (G, \circ) be a group, and $H \leq G$ be a subgroup. Denote the set

$$K = \bigcap_{a \in G} (a \circ H \circ a^{-1}).$$

Then K is the largest normal subgroup of G contained in H .

Proof. Consider the associated permutation representation π_H as above. It has kernel

$$\begin{aligned} \ker(\pi_H) &= \{g \in G \mid \sigma_g = 1\} \\ &= \{g \in G \mid (g \circ a) \circ H = a \circ H \text{ for all } a \in G\} \\ &= \{g \in G \mid g \in a \circ H \circ a^{-1} \text{ for all } a \in G\} \\ &= \bigcap_{a \in G} (a \circ H \circ a^{-1}). \end{aligned}$$

Hence $K = \ker(\pi_H)$, so that K is a normal subgroup contained in H .

Say that N is some other normal subgroup of G contained in H . For any $a \in G$, we have

$$\begin{aligned} N \leq H \\ N = a \circ N \circ a^{-1} \quad \implies \quad N \leq a \circ H \circ a^{-1} \quad \implies \quad N \leq \bigcap_{a \in G} (a \circ H \circ a^{-1}) = K. \end{aligned}$$

Hence K is indeed the largest such normal subgroup. □

Cayley's Theorem. Let (G, \circ) be a group, and $H \leq G$ be a subgroup. Recall that the *permutation representation associated to H* is that map $\pi_H : G \rightarrow S_A$ which sends g to the permutation $\sigma_g : G/H \rightarrow G/H$ defined by $\sigma_g(\bar{a}) = \bar{g \circ a}$. In the previous lecture, we showed that

$$\ker(\pi_H) = \bigcap_{a \in G} (a \circ H \circ a^{-1})$$

is the largest normal subgroup of G contained in H . We give two applications of this result.

Proposition 2. Let (G, \circ) be a group. Assume that G has finite order n .

- (1) G is isomorphic to a subgroup of S_n .
- (2) If p is the smallest prime dividing n , then any subgroup $H \leq G$ of index $|G : H| = p$ is normal in G .

In particular, if G is a finite group, then any subgroup $H \leq G$ of index $|G : H| = 2$ is normal.

Proof. (1) Let $H = \{e\}$ be the trivial subgroup, and consider the permutation representation $\pi_H : G \rightarrow S_n$. Then $\ker(\pi_H) = \{e\}$, so that $G \cong \text{im}(\pi_H)$ is a subgroup of S_n by the First Isomorphism Theorem.

(2) Let $H \leq G$ be a subgroup of index $|G : H| = p$. Consider the permutation representation $\pi_H : G \rightarrow S_p$ with kernel $K = \ker(\pi_H)$. It suffices to show that $H = K$.

Assume the contrary, that $K \subsetneq H$. Since $|G| = |G : H| |H : K| |K|$, any prime q that divides $|H : K|$ must satisfy $q \geq p$. By the First Isomorphism Theorem, $G/K \cong \text{im}(\pi_H) \leq S_p$, so by Lagrange's Theorem the index $|G : K|$ must divide $|S_p| = p!$. But $|G : K| = p \cdot |H : K|$, so q divides $(p - 1)!$. This is a contradiction since the only primes that divide $(p - 1)!$ are less than p . □

GROUPS ACTING BY CONJUGATION

Definitions. Let (G, \circ) be a group. We consider an action by G on $A = \mathcal{P}(G)$ via *conjugation* i.e., the map $\cdot : G \times A \rightarrow A$ defined by $g \cdot S = g \circ S \circ g^{-1}$ for any subset $S \subseteq G$. Recall from lecture #5 (on Wednesday 8/30) that the *stabilizer* of a subset S is its normalizer:

$$G_S = \{g \in G \mid g \cdot S = S\} = \{g \in G \mid g \circ S \circ g^{-1} = S\} = N_G(S).$$

As in the last lecture, the relation $S \sim T$ defined by $T = g \cdot S = g \circ S \circ g^{-1}$ for some $g \in G$ is an equivalence relation on A . We define the *conjugacy class* of S to be the *orbit* $\mathcal{O}_S = \{g \circ S \circ g^{-1} \mid g \in G\}$. The number of conjugates of S is the index of the normalizer of S in G :

$$\#\mathcal{O}_S = |G : N_G(S)|.$$

Class Equation. We prove a result that states how to compute the size of a finite group.

Proposition 3. *Let (G, \circ) be a finite group. There exist elements $a_1, \dots, a_r \notin Z(G)$ such that*

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

Proof. Consider the action of G on the singletons in $A = \mathcal{P}(G)$ i.e., sets $S = \{g\}$. Then the equivalence relation \sim on A gives a partition of G :

$$\mathcal{O}_a = \{g \circ a \circ g^{-1} \mid g \in G\} \quad \Longrightarrow \quad G = \bigcup_{a \in G} \mathcal{O}_a = \bigcup_{i=1}^m \mathcal{O}_{a_i} \quad \Longrightarrow \quad |G| = \sum_{i=1}^m \#\mathcal{O}_{a_i}.$$

The stabilizer of $S = \{a\}$ is the centralizer of a in G :

$$G_a = \{g \in G \mid g \circ a \circ g^{-1} = a\} = C_G(a) \quad \Longrightarrow \quad \#\mathcal{O}_a = |G : C_G(a)|.$$

An orbit \mathcal{O}_a has order 1 if and only $C_G(a) = G$, which happens if and only if $a \in Z(G)$. Hence

$$|G| = \sum_{i=1}^m \#\mathcal{O}_{a_i} = \sum_{i=1}^r |G : C_G(a_i)| + \underbrace{\sum_{i=r+1}^m 1}_{a_i \in Z(G)} = \sum_{i=1}^r |G : C_G(a_i)| + |Z(G)|$$

where the elements $a_i \notin Z(G)$ because $C_G(a_i) \neq G$. □

We list an immediate consequence.

Proposition 4. *Let p be a prime, and P be a group with order $|P| = p^\alpha$.*

- (1) $Z(P)$ is a nontrivial subgroup.
- (2) If $\alpha = 2$, then either $P \cong Z_p \times Z_p$ or $P \cong Z_{p^2}$.

Proof. (1) The Class Equation reads

$$|P| = |Z(P)| + \sum_{i=1}^r |P : C_P(a_i)|$$

The left-hand side is divisible by p since $|P| = p^\alpha$ by assumption. We know that $C_P(a_i) \neq P$ because $a_i \in Z(P)$, so according to Lagrange's Theorem, p divides $|P : C_P(a_i)|$. Hence p must divide $|Z(P)|$ as well.

(2) Assume that $|P| = p^2$. We know that $|Z(P)| = p$ or p^2 , so that $|P/Z(P)| = p$ or 1, respectively, by Lagrange's Theorem. In either case, $P/Z(P)$ is cyclic, so that P must be abelian. (Note that this fails if $|P| = p^3$: The quaternions have order $|Q_8| = 2^3$, but do not form an abelian group.)

If P has an element of order p^2 , say z , then $P = \langle z \rangle$ is cyclic of order p^2 . This shows that $P \cong Z_{p^2}$. Assume otherwise, that P does not have an element of order p^2 . We show that $P \cong Z_p \times Z_p$.

Pick a nontrivial element $x \in P$. Since $H = \langle x \rangle$ is nontrivial, we see that H must have order p . Similarly, pick an element $y \in P - \langle x \rangle$; then $K = \langle y \rangle$ must have order p . The subgroup $HK = \langle x, y \rangle$ is strictly larger than $H = \langle x \rangle$, so $|HK| = p^2 = |P|$, showing that $P = HK$. It is easy to see that the map $\varphi : HK \rightarrow H \times K$ defined by $x^a y^b \mapsto (x^a, y^b)$ is a well-defined group homomorphism because P is abelian. (This is not well-defined otherwise!) It is also easy to see that this map is an isomorphism. This shows that $P = HK \cong H \times K \cong Z_p \times Z_p$. □