21-237: Math Studies Algebra I September 23, 2022

Lecture 11 : Sylow's Theorem

Lecturer: James Cummings

Scribe: Rajeev Godse

1 More notation

Let G act on X. We say $Y \subseteq X$ is **invariant** (G-invariant) if $g \cdot y \in Y$ for all $g \in G, y \in Y$. Equivalently, Y is a union of orbits. We get an action of G on Y.

Let $H \leq G$. Then we get an action of H on Y, in which each G-orbit may be split into many H-orbits.

2 Sylow

Let G be a finite group, p is a prime, $p \mid |G|$, p^t is the largest power of p dividing $|G|$.

Let $\text{Syl}_p(G) = \{H : H \leq G, |H| = p^t\}$. We call these the **Sylow p-subgroups**. We can say that a **p-subgroup** of G is $K \leq G$, where $|K|$ is a power of p.

Theorem (Sylow):

(a) For every p-subgroup K of G, there is $H \in \text{Syl}_p(G)$ where $K \leq H$

(b) All Sylow p-subgroups are conjugate.

(c) The number of Sylow p-subgroups, i.e. $|\text{Syl}_p(G)|$, divides $|G|$ and is $\equiv 1 \bmod p$.

Proof:

Let $\Sigma = \{K : K \text{ is a non-trivial } p\text{-subgroup of } G\}$. Let $\Omega = \{K \in \Sigma : K \text{ is maximal under inclusion}\}$. We say K is maximal under inclusion if for all $L \in \Sigma$, $K \subseteq L \implies L = K$.

Claim 1: $\Sigma \neq \varnothing$. *Proof*: Use Cauchy to show there is $K \leq G$ with $|K| = p$.

Claim 2: For all $K_1 \in \Sigma$, there is $K_2 \in \Omega$ such that $K_1 \leq K_2$. *Proof*: Let $|K_2|$ be largest among $\{K_2 \in \Sigma : K_1 \leq K_2\}$, which is non-empty since K_1 is in the set and finite since G is finite.

Claim 3: For all $K \in \Sigma$, $g \in G$, $K^g \in \Sigma$. *Proof*: K^g is a subgroup and $|K^g| = |K|$ since conjugation by a group element is an automorphism.

Claim 4: For all $K \in \Omega$, $g \in G$, $K^g \in \Omega$. *Proof*: If $A, B \leq G$, $g \in G$, $A \leq B \iff A^g \leq B^g$. Suppose K^g was strictly contained in some $L \in \Sigma$. Then, K is strictly contained in $L^{g^{-1}}$, so $K \notin \Omega$. By contrapositive, $K^g \in \Omega$.

Claim 5: Let $H \in \Omega$. As $H \leq G$ and G acts on Ω by conjugation, H acts on Σ by conjugation. H is the only fixed point for the action of H on Ω by conjugation. *Proof*: For all $h \in H$, $H^h = H$, so H is a fixed point. Suppose that $K \in \Omega$ is a fixed point, i.e. $K^h = K$ for all $h \in H$. So $K \leq N_G(K)$. By a fact from last lecture, $HK \leq G$. From the HW, $HK = \frac{|H||K|}{|H \cap K|}$. So $|HK|$ is a power of p, that is $HK \in \Sigma$. $H \in \Omega$ and $H \subseteq HK$, so $H = HK$. Similarly, $K \in \Omega$ and $K \subseteq HK$, so $K = HK = H$.

Claim 6: $|\Omega| \equiv 1 \bmod p$. *Proof*: Look at the orbits of the action of H on Ω. As H is the only fixed point, $\{H\}$ is the only orbit of size 1. Other orbits have sizes which are positive powers of p, as they must divide $|H|$ via the orbit-stabilizer theorem and LaGrange's theorem.

Claim 7: All elements of Ω are conjugate, i.e. Ω forms a single orbit for the action of G on Ω by conjugation. *Proof*: Otherwise, let H_1, H_2 lie in distinct orbits. Let O_i denote the orbit of H_i, i.e.

$\{H_i^g : g \in G\}$. As $H_1 \leq G$, H_1 acts on O_1 and on O_2 by conjugation. In the action of H_1 on O_1, H_1 is the only fixed point. In the action of H_1 on O_2, there are no fixed points. Thus, $|O_1| \equiv 1 \bmod p$ and $|O_2| \equiv 0 \bmod p$. To finish, swap H_1 and H_2 and derive a contradiction.

Claim 8: $|\Omega|$ divides $|G|$. *Proof*: Ω forms a single orbit in the action of G. In fact, $|\Omega| = [G : N_G(H)]$ for any $H \in \Omega$ by the orbit-stabilizer equation.

Claim 9: $\Omega = \mathrm{Syl}_p(G)$. *Proof*: Next lecture.