21-237: Math Studies Algebra I September 19, 2022

Lecture 9 : Cauchy's Theorem

Lecturer: James Cummings

Scribe: Rajeev Godse

1 Cauchy's Theorem

Theorem: If $|G| \in \mathbb{N}$ and there exists some prime p such that $p \mid |G|$, then G has an element of order p. Equivalently, there is $H \leq G$ such that $|H| = p$.

Proof: Let $X = \{(g_1, \ldots, g_p) : g_i \in G \text{ for all } 1 \leq i \leq p, g_1 \ldots g_p = 1\}$.

$(g_1, \ldots, g_p) \in X \iff gp = (g_1 \ldots g_{p-1})^{-1}$, so $|X| = |G|^{p-1}$ and $p \mid |X|$.

Let $(\mathbb{Z}/p\mathbb{Z}, +)$ act on X by cycling entries in the natural way. Cycling entries preserves membership in X (cycling once works fine since we already have $g_p = (g_1 \ldots g_{p-1})$, cycling by any amount then preserves membership in X by induction). Moreover, it is an action: cycling a tuple x by 0 gives x and cycling a tuple by i then j is the same as cycling it by $i + j$.

Fixed points of this action are tuples $(g, \ldots, g) \in X$, i.e. $g^p = 1$, which is true if and only if $|g| = 1$ or $|g| = p$.

Since $|\mathbb{Z}/p\mathbb{Z}| = p$, all orbits have sizes dividing p, i.e. all orbits have size 1 or size p.

Then, $|X| = |G|^{p-1} = \sum\limits_{O \text{ orbit}} = |O| = \text{number of fixed points} + \sum_{O, |O|>1} |O|$. The number of fixed points must thus divide p and is at least 1 due to $(1, \ldots, 1)$, so the number of fixed points is at least p. Each fixed point is an element repeated k times, so there is at least one non-identity element whose pth power is 1. Its order is either 1 or p, and it is not the identity, so its order must be p.

2 Sylow's Theorem(s) (Foreshadowing)

Theorem(s): Let $|G| \in \mathbb{N}$ such that there exists a prime p where $p \mid |G|$, let $|G| = p^t b$, where p does not divide b. Then,

(a) G has subgroups of order p^t.

(b) Every subgroup $H \leq G$ such that $|H|$ is a power of a prime is contained in some subgroup of order p^t.

(c) All subgroups of order p^t are conjugate.

(d) The number of subgroups of order p^t divides $|G|$ and is conjugate to 1 mod p.