Math 122 – Lecture 19 Notes

Last Time

If we write $|G| = p^k \cdot n$ (where $\gcd(n, p) = 1$), we have by the First Sylow Theorem that there exists some $H \subset G$ such that $|H| = p^k$; by the Second Sylow Theorem, if $H' \subset G$, then $H' = gHg^{-1}$ for some $g \in G$; and by the Third Sylow Theorem, if s is the number of Sylow p-subgroups, then $s \mid n$, where $s \equiv 1 \mod p$.

Classification of groups of order pq

Why are the Sylow theorems important?

Many reasons, one of which is that using them, one can *classify* <u>all</u> groups of order pq ($p < q$, where both are prime).

Theorem 0.1. *Let G be a group. If $|G| = pq$ then $G \simeq \mathbb{Z}/p\mathbb{Z} \ltimes (\mathbb{Z}/q\mathbb{Z})$ for some homomorphism $\varphi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z})$.*

How to describe homomorphisms φ?

Claim 0.1. *Use the mapping from $((\mathbb{Z}/q\mathbb{Z})^\times, \cdot)$ to $Aut(\mathbb{Z}/q\mathbb{Z}, +)$, so that $m \mapsto (x \mapsto mx)$. This is true in general for q not necessarily prime.*

For prime q, we have that $(\mathbb{Z}/q\mathbb{Z})^\times = \{1, 2, \ldots, q-1\}$, so $\varphi \leftrightarrow m \in \mathbb{Z}/q\mathbb{Z}$ such that $m^p = 1$.

Example. Take $q = 5$ and $p = 2$. Then $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$. Check $m = 1$: $1^2 = 1$, this works. $m = 2$: $2^2 = 4 \neq 1$, does not work. $m = 3$: $3^2 = 4 \neq 1$, does not work. $m = 4$: $4^2 = 1$, works. Now take $q = 5$ and $p = 4$; now all of $m = 1, 2, 3, 4$ work.

So moreover $\mathbb{Z}/p\mathbb{Z} \ltimes_m (\mathbb{Z}/q\mathbb{Z}) \leftarrow \langle x, y\rangle / \langle x^q = y^p = 1, yxy^{-1} = x^m\rangle$. Note that $(\mathbb{Z}/5\mathbb{Z})^\times \leftarrow \{1, 2, 2^2 = 4, 2^3 = 3\}$, so $(\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z}$ (it is a cyclic group). Moreover it is true in general that

$$(\mathbb{Z}/q\mathbb{Z})^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}.$$

We thus have the following:

- if $p \nmid (q-1)$, then φ must be trivial, so $G \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ and therefore is $\mathbb{Z}/pq\mathbb{Z}$.

- if $p \mid q$, then the subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ consisting of m such that $m^p = 1$ is *isomorphic* to $\mathbb{Z}/p\mathbb{Z}$ (in $\mathbb{Z}/(q-1)\mathbb{Z}$ it is $0, \frac{q-1}{p}, \frac{2(q-1)}{p}, \ldots$, i.e. $\mathbb{Z}/p\mathbb{Z}$).

So it's of the form $\{1, a, a^2, \ldots, a^{p-1}\}$ for some a. We see that $m = a^k$ for some k. If $k = 0$, then $G \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$. If $k \neq 0$, then $\mathbb{Z}/p\mathbb{Z} \ltimes_a (\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z} \ltimes_{a^k} (\mathbb{Z}/q\mathbb{Z})$, where we note that the former has the representation $\langle x, y\rangle / \langle x^q = y^p = 1, yxy^{-1} = x^a\rangle$. If you choose generators $\{x, y^k\}$ here then you get $\langle x, y\rangle / \langle x^q = y^p = 1, yxy^{-1} = x^{a^k}\rangle$. Thus:

Theorem 0.2. *If $p \nmid (q-1)$ then $G \simeq \mathbb{Z}/pq\mathbb{Z}$. If $p \mid (q-1)$ then either $G \simeq \mathbb{Z}/pq\mathbb{Z}$ or $G \simeq (\mathbb{Z}/p\mathbb{Z}) \ltimes (\mathbb{Z}/q\mathbb{Z})$.*

Proof. We have $p < q$.

- Let s be the number of q-subgroups of G. We have that $s \equiv 1 \mod q$ and $s \mid p$ (where $p < q$), so $s = 1$¿ Then pick $H \subset G$ such that H is our Sylow q-subgroup.
- $H \subset G$ is normal since $s = 1$, so $gHg^{-1} = H$.
- H is cyclic: $|H| = q$.
- Pick any cyclic $K \subset G$ that is a p-subgroup.
- Construct the homomorphism $K \to \mathrm{Aut}(H)$ where $k \mapsto (h \mapsto khk^{-1})$.
- $K \simeq \mathbb{Z}/p\mathbb{Z}$, $H \simeq \mathbb{Z}/q\mathbb{Z}$.
- $K \ltimes H \xrightarrow[\sim]{G}$, so that $(k, h) \mapsto kh$, is an injective homomorphism, and $K \ltimes H$ is $\mathbb{Z}/p\mathbb{Z} \ltimes (\mathbb{Z}/q\mathbb{Z})$.

□