MATH 3311, FALL 2025: LECTURE 19, OCTOBER 10

Video: `https://youtu.be/FY4ba7Z-jJ4`

We are ready today to prove our first actual theorem. This will use essentially every concept and important result we have seen so far this semester. If you are able to digest and internalize this proof, that means that you have made some real progress!

The Sylow theorems

We will fix a *finite* group G and a prime p. Let $m \geq 0$ be the integer such that p^m is the *largest* power of p dividing $|G|$. We can now state the theorem:

Theorem 1 (Sylow Theorem A)**.** *There exists a subgroup $Q \leq G$ of order $|Q| = p^m$.*

To prove this, we will actually show a more refined assertion in the form of the following proposition.

Proposition 1. *Suppose that $H \leq G$ is a subgroup with $|H| = p^k$ with $k < n$. Then there exists a subgroup $H' \leq G$ with $H \leq H' \leq G$ and with $|H'| = p^{k+1}$.*

Assuming this proposition, we can prove the theorem:

Proof of Theorem A assuming Proposition 1. We will construct the subgroup Q essentially by induction on the exponent m. If $m = 0$, then there is nothing to do: We can take $Q = \{e\}$.

For $m > 1$, the proposition shows that, if there is a subgroup $H_k \leq G$ with $|H_k| = p^k$ and $k < m$, then there is a subgroup $H_{k+1} \leq G$ containing H_k with $|H_{k+1}| = p^{k+1}$. Starting with $k = 0$ and $H_0 = \{e\}$, this gives us a chain of subgroups

$$H_0 \leq H_1 \leq \ldots \leq H_{m-1} \leq H_m$$

where $|H_k| = p^k$ for all $k \leq m$. The chain stops when $|H_m| = p^m$, and we take $Q = H_m$. □

The rest of this lecture will be devoted to the proof of Proposition 1. Let us begin with some useful observations.

Observation 1. Suppose that we have subgroups $H \leq H' \leq G$ with $|H| = p^k$ and $|H'| = p^{k+1}$. Then H is a *normal* subgroup of H'.

Proof. Our hypotheses show that $|H'/H| = [H' : H] = p$. Since p is the smallest prime dividing the order of H', we see using HW 6, Problem 2 that $H \trianglelefteq H'$ is *normal*. Therefore, H'/H is a *group* of order p (and so is necessarily a cyclic group). □

Observation 2. Suppose that $H \trianglelefteq G$ is normal in G with $|H| = p^k$ and $k < m$. Then finding $H' \leq G$ with $H \leq H' \leq G$ with $|H'| = p^{k+1}$ is *equivalent* to finding a subgroup $\overline{H}' \leq G/H$ of order p. Moreover, $p \mid |G/H|$, so such a subgroup $\overline{H}' \leq G/H$ always exists by Cauchy's theorem.

Proof. This is because by HW 6, Problem 3, subgroups of G containing H are in bijective correspondence with subgroups of G/H. More precisely, given $\overline{H}'$ of order p, we recover the subgroup $H' \leq G$ as the *pre-image* of $\overline{H}'$ under the quotient homomorphism $G \to G/H$. Further, the relationship between H' and $\overline{H}'$ is given by

$$\overline{H}' = H'/H \leq G/H.$$

Therefore, saying that $|H'|/|H| = |H'/H| = p$ is equivalent to saying that $|\overline{H}'| = p$. But this is of course the same as saying that $|H'| = p^{k+1}$.

Finally, since $k < m$, we see that $|G/H|$ is still divisible by p: Indeed, p^{m-k} is still a factor of $|G/H|$. Therefore, Cauchy's theorem tells us that there exists a subgroup $\overline{H}' \leq G/H$ of order p. □

Therefore, if H is *normal* in G, then we have shown that the proposition is valid. We would now like to *remove* this normality constraint. For this, we introduce the following definition, which gives us a somewhat *tautological* way of finding a group in which H is normal.

Definition 1. If $H \leq G$ is a subgroup[1], the **normalizer of H in G** is the subset

$$N_G(H) = \{g \in G : \ gHg^{-1} = H\}.$$

Fact 1. $N_G(H) \leq G$ is a subgroup and $H \trianglelefteq N_G(H)$ is a normal subgroup

Proof. The quickest way to see this is to note that G acts on the set X of subgroups of G via conjugation: $(g, K) \mapsto gKg^{-1}$. Then $N_G(H) \leq G$ is the stabilizer of H for this action. Moreover, we clearly have $H \leq N_G(H)$ and every element of $N_G(H)$ conjugates H back to itself by definition. Therefore, $H \trianglelefteq N_G(H)$ is a normal subgroup. □

Fact 2. We have $H \trianglelefteq G$ if and only if $N_G(H) = G$.

Proof. This is just a direct translation of the definition of what it means for H to be normal in G. □

Note that, by Observation 1, *if* H' existed, then H would be a normal subgroup of H', and this is equivalent to saying that $H' \leq N_G(H)$ (why?). Therefore, we would like to apply Observation 2 to H as a subgroup of $N_G(H)$. This would give us $H \leq H' \leq N_G(H)$ with $|H'| = p^{k+1}$, and would therefore complete the proof of Proposition 1. For this, we need to check two things:

(1) $H \trianglelefteq N_G(H)$;
(2) p is a factor of $|N_G(H)/H|$.

The first item is clear, while the second item is needed in order to apply Cauchy's theorem to the quotient group $N_G(H)/H$.

For this, recall the following fundamental congruence:

Proposition 2. *If H is a p-group acting on a finite set X, then we have*

$$|X^H| \equiv |X| \pmod{p}.$$

We apply this to the action of H on G/H by left multiplication. This gives us[2]:

$$|(G/H)^H| \equiv |G/H| \equiv 0 \pmod{p}. \tag{0.0.0.1}$$

To finish, you will check in Homework 7 that we have

$$N_G(H)/H = (G/H)^H \subset G/H. \tag{0.0.0.2}$$

Combining (0.0.0.1) and (0.0.0.2), we find

$$|N_G(H)/H| \equiv 0 \pmod{p}.$$

Therefore, Observation 2 can now be applied to $H \leq N_G(H)$ to show the existence of H' and thereby complete the proof of Proposition 1.

[1]This is a general definition and doesn't need any other hypotheses on G or H.

[2]Why is the second congruence true?