date: thursday, february 1, 2024

Sylow Theorem 1

Recall: (Lagrange's Theorem) If H is a subgroup of G, then $|H| \mid |G|$.

The Sylow theorems give us a partial converse, ie. if $|G|=n$ and if we know the factorization of n, we can deduce some things about its subgroup.

(First Sylow Theorem) If p is a prime and if $p^k \mid |G|$, then G has a subgroup of order p^k.

eg. $|S_7| = 7! = 1 \cdot 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \cdot 3) \cdot 7$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7$

Then S_7 has subgroups of order $2, 2^2, 2^3, 2^4, 3, 3^2, 5, 7$.

Def^n: A group G is a p-group (p is a prime) if for all $g \in G$, $|g| = p^t$ for some t (note $|e| = p^0$).
A subgroup H of G is a p-subgroup if H is a p-group.

Theorem: (Cauchy) Let G be a finite group and p a prime such that $p \mid |G|$. Then G has a subgroup of order p.

Proof (already proved this for abelian groups in lecture 4)
Use the class equation. Do induction on $|G|=n$. If $|G|=p$ (a prime), then G is cyclic and G is a subgroup of itself of order p. Takes care of $p=2,3$.
Assume $|G|=n$ and result holds for all $k<n$. If $n=p$, then done!
Via the class equation, there exists $x_1, \ldots, x_n \in G$ such that

$$|G| = |Z(G)| + [G:C(x_1)] + \cdots + [G:C(x_n)]$$

with $[G:C(x_i)] > 1$.
Note: If $|G| = |Z(G)|$, then G is abelian so previous result for abelian groups hold.

Case 1: Suppose $p \nmid [G:C(x_i)]$ for some x_i. So $|G| = [G:C(x_i)]|C(x_i)|$. So $p \mid |C(x_i)|$ and $|C(x_i)| < |G|$. So by induction, $C(x_i)$ has an element of order p and then so does G.

Case 2: Suppose $p \mid [G:C(x_i)]$ for all x_i. So $p \mid |Z(G)|$ since

$$|Z(G)| = -[G:C(x_1)] - \cdots - [G:C(x_n)] + |G|.$$

But $Z(G)$ has an element of order p. Then so does G.

□

Corollary: G is a p-group iff $|G| = p^t$ for some t.

Proof

"<=" Let $g \in G$. So $|g| \mid |G| = p^t$, so $|g| = p^\ell$ for some ℓ.

"=>" Suppose q is another prime such that $q \mid |G|$. But then G has an element of order q (previous result). This contradicts fact that G is a p-group.

□

Proof (Sylow #1)

Do induction on $|G| = n$. The result holds if $|G| = p$, since $G \simeq \mathbb{Z}_p$, and $\mathbb{Z}_p$ has a subgroup of order p^0 and p^1. Assume $|G| = n$, true for $\ell < n$, and can assume n not prime.

Via the class equation, exists $x_1, \dots, x_n$ such that

$$|G| = |Z(G)| + [G:C(x_1)] + \cdots + [G:C(x_n)]$$

with $[G:C(x_i)] > 1$.

Case 1: Suppose $p \nmid [G:C(x_i)]$ for some i. So $|G| = [G:C(x_i)]|C(x_i)|$, so $p^k \mid |C(x_i)|$ with $|C(x_i)| < |G|$. By induction, $C(x_i)$ has a subgroup of order p^k.

Case 2: If $p \mid [G:C(x_i)]$ for all i, then via class equation, $p \mid |Z(G)|$. By Cauchy's theorem, there exists $g \in Z(G)$ with $N = \langle g \rangle \subseteq Z(G)$ with $|g| = p$.

Claim: N is normal in G.

Let $h \in G$ and $m \in N$. Then $hmh^{-1} \overset{m \in Z(G)}{=} hh^{-1}m = m \in N$.

Consider the quotient group G/N. Because $|N| = p$, $|G/N| = \frac{|G|}{p} = n/p$.

So $p^{k-1} \mid |G/N| = n/p$. So G/N has a subgroup of order p^{k-1}. Call this subgroup $L \subseteq G/N$.

Recall that $L \subseteq G/N$ is a subgroup $\Leftrightarrow$ exists a subgroup $N \subseteq H \subseteq G$ such that $H/N = L$ (Correspondence theorem)
So there exists a subgroup $N \subseteq H \subseteq G$ such that $L = H/N$ so $|L| = |H|/|N| = p^{k-1}$. So $|H| = p^{k-1}|N| = p^{k-1}p = p^k$.

$\square$

eg. Let G be a finite abelian group with $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

$$G \simeq (\mathbb{Z}_{p_1}^{r_{11}} \times \mathbb{Z}_{p_1}^{r_{12}} \times \cdots \times \mathbb{Z}_{p_1}^{r_{1s_1}}) \times \mathbb{Z}_{p_2}^{r_{21}} \times \cdots$$

$r_{11} + \cdots + r_{1s_1} = a_1$.
Note $\mathbb{Z}_{p_1}^{r_{11}} \times \cdots \times \mathbb{Z}_{p_1}^{r_{1s}}$ is a p-subgroup of G and also $|\mathbb{Z}_{p_1}^{r_{11}} \times \cdots \times \mathbb{Z}_{p_1}^{r_{1s}}| = p_1^{a_1}$.

eg. Suppose N is normal in G and G/N and N are p-groups. Then, G is also a p-group.
Infinite case: Let $g \in G$. If $g \in N$, then $|g| = p^t$. If $g \notin N$, consider $gN \in G/N$.
So $|(gN)| = p^{\ell}$. This means $(g)^{p^{\ell}} \in N$. But N a p-group so $((g)^{p^{\ell}})^{p^t} = g^{p^{\ell+t}} = e$.