Abstract Algebra
: Lecture 11

Leo

2024.10.31

Let G be a finite group with $|G| = p^e m$ s.t. $\gcd(p, m) = 1$. $|G|_p = p^e$. Recall: A Sylow p-subgroup of G is a subgroup $H \leq G$ s.t. $|H| = p^e$. We already proved the existance of Sylow p-subgroups. Today we will talk about the relation between Sylow p-subgroups and the number of Sylow p-subgroups.

Theorem 1. ***Sylow 1st Theorem:*** *Let G be a finite group with $|G| = p^e m$ s.t. $\gcd(p, m) = 1$. Then Sylow p-subgroup exists.*

Theorem 2. ***Sylow 2nd Theorem:*** *Let G be a finite group with $|G| = p^e m$ s.t. $\gcd(p, m) = 1$. Let P be a Sylow p-subgroup of G. Let $H \leq G$ s.t. $|H| \mid p^e$. Then H is conjugated to a subgroup of P. In particular, all Sylow p-subgroups are conjugate to each other. G has only one Sylow p-subgroup if and only if P is normal in G.*

证明. Let $\Omega = [G : P] = \{Px | x \in G\}$, then G acts on Ω by right multiplication. $g : Px \mapsto Pxg, \forall g, x \in G$. Then the map is a group action of G on Ω, and it is transitive. This is called a coset action. (transitive permutation representation).
Of course, H acts on the set Ω in the same way. Which may be intransitive. The size $|\Omega| = \frac{|G|}{|P|} = m$, is coprime to p. And each orbit of H on Ω has size dividing $|H|$ by orbit-stabilizer theorem.
So there exists at least one orbit of H of size 1. Namely H fixes a point Px for some $x \in G$. Now $G_{Px} = \{g \in G | Pxg = Px\}$ is conjugate to $G_P = P$, and it shows $H \leq G_{Px}$ for some $x \in G$, i.e. H is conjugated to a subgroup of P (all stabilizers are conjugate because of transitivity).
If $G \curvearrowleft \Omega$ transitive then all stabilizers are conjugate: Let $x \in g^{-1} G_\alpha g$. Then $x = g^{-1} h g$ for some $h \in G_\alpha$. And $(\alpha^g)^x = (\alpha^g)^{g^{-1} h g} = (\alpha^h)^g = \alpha$. So $g^{-1} G_\alpha g \leq G_\alpha$. Similarly $g^{-1} G_\alpha g \geq G_\alpha$. So $g^{-1} G_\alpha g = G_\alpha$. □

Theorem 3. ***Sylow 3rd theorem.*** *Let G be a finite group and p a prime dividing $|G|$. Then $n_p \mid m$ and $n_p \equiv 1 \pmod{p}$.*

证明. Let $P \in Syl_p(G)$, and let $N = N_G(P) = \{g \in G | g^{-1} P g = P\}$, called the normalizer of P in G. Then P is a normal subgroup of N, and N is a subgroup of G. Then $m = \frac{|G|}{|P|}$, and $n_p = |Syl_p(G)|$. By thm 2 G is transitive on the set $Syl_p(G)$ with stabilizer of P which is $N_G(P)$. Thus $n_p = |Syl_p(G)| = \frac{|G|}{|N_G(P)|}$ i.e $n_p \frac{|N_G(P)|}{|P|} = \frac{|G|}{|N_G(P)|} \frac{|N_G(P)|}{|P|} = m$, it shows $n_p \mid m$.

G is transitive on $Syl_P(G)$ with stabilizer $N_G(P)$ (by conjugate action). Recall $Syl_p(G)$, size n_p . Now P acts on $Syl_p(G)$ by conjugation. Then each orbit of P has size dividing $|P|$. As $\gcd(p, n_p) = 1$, there exists **exactly one** orbit of size 1. Therefore $n_P \equiv 1 \pmod p$.

Proof for **exactly one**: Let $P, Q \in Syl_p(G)$. Then by conjugation, P fixes Q iff $\forall x \in P$, $x^{-1}Qx = Q$, so $x \in N_G(Q)$, in other words $P \leq N_G(Q)$. But according to Sylow 2nd thm, $N_G(Q)$ has only one Sylow p-subgroup which is Q, thus $P = Q$. $\square$

Example 4. *Consider A_4 and S_4. $|A_4| = 12$, $|S_4| = 24$. A_4 dose not have a subgroup of order 6. S_4 has a subgroup of order 6.*

Exercise 5. *Prove: A_4 dose not have a subgroup of order 6. S_4 has a subgroup of order 6.*

Example 6. *Conjecture: Let n be a positive integer which is not a power of a prime. Then there exist a finite group G which $n \mid |G|$ s.t. G dose not have a subgroup of order n.*

Exercise 7. *If $|G| = 2p$, then $G = C_{2p}$ or $G = D_{2p}$.*

证明. By Sylow 3rd thm $G_p \lhd G$ so let $x \in G_2$ the conjugation action induces an order $\leq$ two automorphism of $< g >= G_p = C_p$ we already know $\mathrm{Aut}(C_p) = C_{p-1}$ only identity and $\sigma : g \mapsto g^{-1}$ has order 2. The fist one shows $G = C_{2p}$ and the second one shows $G = D_{2p}$. $\square$

Exercise 8. *Let $|G| = pq$ where $p > q$ are primes. Prove that $G_p \lhd G$, and either G is cyclic or $q \mid p - 1$.*

证明. Just consider Sylow 3rd thm. $\square$