Sylow's Theorem

August-11-10
8:05 AM

D&F pp 140.

$|G| = p^\alpha m$, p prime, $p \nmid m$; $Syl_p(G) := \{P < G : |P| = p^\alpha\}$ are "Sylow p-subgroups of G". A "p-subgroup" in general, is any subgroup of G of order a power of p.

Sylow 1 $Syl_p(G) \neq \emptyset$.

Proof. By induction on $|G|$, if G has a normal subgroup of order p (or p^β) or if G has a subgroup of order divisible by p^α, we are done. The existance of one of the said types follows from the class equation:

$$|G| = \underbrace{|Z(G)|}_{\text{The centre of } G} + \sum_i (G : \underbrace{C_G(y_i)}_{\text{the centralizer of } y_i \text{ in } G})$$

Where $\{y_i\}$ are representatives from the non-central conjugacy classes of G. $\square$

Sylow 2. Let P be a Sylow p-subgroup of G and let $n_p(G)$ be the number of conjugates of P in G. Then

1. $n_P(G) = |G : N_G(P)| \mid |G|$ } No proof required.

2. $n_P(G) \equiv 1 \mod p$.

Lemma If $P \in Syl_p(G)$ and Q is a p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$. Alternatively, define a "p-element" of G to be an element whose order is a power of p. Then if a p-element normalizes P, then it is in P. Alternatively, if H is a p-subgroup of $N_G(P)$, then $H \subset P$.

Proof. The equivalence of the three statements is easy. Now if H is a p-subgroup of $N_G(P)$, and $P \cap H \neq H$, Then PH is a group and $|PH| = \frac{|P| \cdot |H|}{|P \cap H|}$, so $p \mid |PH| > |P|$ contradicting the maximallity of P.

Proof of Sylow 2 P acts on the set Θ of its conjugates by conjugation. One orbit is P itself, a singleton. All other orbits are non-trivial — if $P' \neq P$ is a conjugate of P, then $P \not\subset N_G(P')$, or else we'd have $P \subset P'$ (by lemma), contradicting $P' \neq P$. But $P \not\subset N_G(P')$ means that the orbit of P' is non-trivial. So Θ is decomposed into a singleton and non-trivial P orbits, whose size must be divisible by p. So $|\Theta| = 1 \mod p$. □

Sylow 3 If $P \in Syl_p(G)$ and Q is a p-subgroup, then Q is contained in a conjugate of P. (So in particular, all Sylow p-subgroups of G are conjugate, and n_p can be re-written n_p).

Proof. Q acts on the set Θ of conjugates of P by conjugation. All orbits are either singletons or divisible by p. Since $|\Theta| = 1 \mod p$, there must be a singleton – a P' s.t. $Q \subset N_G(P')$. But then $Q \subset P'$. $\square$