Graduate Algebra, Fall 2014
Lecture 11

Andrei Jorza

2014-09-19

1 Group Theory

1.16 The Sylow theorems

Theorem 1. *Let G be a finite group with $p^r m$ elements, where $p \nmid m$ and $r > 0$.*

1. *G has at least one p-Sylow subgroup and denote $n_p = |\operatorname{Syl}_p(G)| \geq 1$.*
2. *$n_p \equiv 1 \pmod p$.*
3. *Every p-subgroup of G is contained in a p-Sylow subgroup.*
4. *If $P \in \operatorname{Syl}_p(G)$ then $\operatorname{Syl}_p(G) = \{gPg^{-1} | g \in G\}$, i.e., every two p-Sylow subgroups are conjugate.*
5. *$n_p \mid m$.*

Proof. Part one: Let X be the set of subsets of G of cardinality p^r. Then $|X| = \binom{p^r m}{p^r}$. The group G acts on X and

$$|X| = \sum [G : \operatorname{Stab}_G(S)]$$

where the sum is taken over distinct orbits $\mathcal{O}$ having chosen $S \in \mathcal{O}$. By the base p lemma we see that $\binom{p^r m}{p^r} \equiv \binom{m}{1} \pmod p$ and so $p \nmid |X|$. Thus the RHS is also not divisible by p so for at least one orbit $\mathcal{O}$ and $S \in \mathcal{O}$, $p \nmid [G : \operatorname{Stab}_G(S)]$ which implies that $p^r \mid \operatorname{Stab}_G(S)$. Let's show that $\operatorname{Stab}_G(S)$ is in fact a p-Sylow subgroup of G. Since S is an orbit of G we get a map $\operatorname{Stab}_G(S) \to S$ taking $g \mapsto gx_0$ for a fixed $x_0 \in S$. This map is clearly injective and so we deduce that $|\operatorname{Stab}_G(S)| \leq |S| = p^r$. The conclusion follows.

Part two: Let X now be the set of all p-Sylow subgroups on which a fixed p-Sylow subgroup $P \subset G$ acts by conjugation. Again,

$$n_p = |X| = \sum [P : \operatorname{Stab}_P(S)]$$

where the sum is over distinct conjugacy classes of p-Sylow subgroups and S is a choice in each such conjugacy class. First, if for some S, $\operatorname{Stab}_P(S) = P$ then $gSg^{-1} = S$ for every $g \in P$. We have $PS = SP$ and so PS is a subgroup of G. But $|PS/S| = |P/P \cap S|$ and so $|PS|$ is also a power of p, at least as large as $|P| = |S|$. This can only happen if $PS = P = S$ as p-Sylow subgroups have largest power of p cardinality. Thus exactly one conjugacy class has one element and for every other conjugacy class $[P : \operatorname{Stab}_P(S)]$ is divisible by p. Thus we get

$$n_p = 1 + \sum [P : \operatorname{Stab}_P(S)] \equiv 1 \pmod p$$

Part three: Now suppose R is a p-subgroup of G, acting on G/P via the left regular action. Since $p \nmid |G/P|$ at least one orbit of R acting on G/P has size coprime to p. This orbit has cardinality $[R : \operatorname{Stab}_R(gP)]$ for some coset gP and since $|R|$ is a power of p, the only way this cardinality is coprime to p is if it is 1. Thus $\operatorname{Stab}_R(gP) = gP$ so for $r \in R$, $rgP = gP$ which is equivalent to $r \in gPg^{-1}$ and so $R \subset gPg^{-1}$, which is also a p-Sylow subgroup.

Part four: Applying part three to a p-Sylow subgroup shows that $R = gPg^{-1}$ so all p-Sylow subgroups are conjugate.

Part five: Consider the conjugate action of G on its subgroups. All p-Sylow subgroups, by part four, form one conjugacy class under this action and the size of the orbit is $[G : \mathrm{Stab}_G(P)] \mid |G|$ and so $n_p \mid |G| = p^r m$. Since n_p and p are coprime we deduce that $n_p \mid m$. □

1.17 Application of the Sylow theorems: classifying finite groups

This is a large list of examples. Throughout, p, q are primes.

The main technical tool in using the Sylow theorems to studying finite groups is that if $p \mid |G|$ then $n_p = 1$ iff G has a normal p-Sylow subgroup.

Example 2. Suppose $|G| = pq$ with $p > q$. We already saw that $n_p = 1$ so $\mathrm{Syl}_p(G) = \{P\}$ with $P \lhd G$. If $q \nmid p - 1$ we saw last time that G must be cyclic. Suppose $q \mid p - 1$. Let $Q \in \mathrm{Syl}_q(G)$. Then $P \cap Q = 1$ and comparing sizes $G = PQ$ so $G = P \rtimes Q$ wrt a homomorphism $\phi : Q \to \mathrm{Aut}(P) = \langle g \rangle \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Such a homomorphism is either trivial, giving G cyclic, or the map sending k to multiplication by $g^{k(p-1)/q}$.

Example 3. Suppose $G = p^2 q$ with $p \neq q$. Let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. Then one of P and Q is normal in G.

Proof. Assume this is not the case. Then $n_p, n_q > 1$ and $n_p \mid q$, $n_q \mid p^2$ implies that $n_p = q$ and $n_q = p$ or p^2. Also $n_p = q \equiv 1 \pmod{p}$ and so $q \geq p + 1$ and $n_q \equiv 1 \pmod{q}$ implies $n_q \geq q + 1 \geq p + 2$ so $n_q = p^2$. But then $q \mid n_q - 1 = (p-1)(p+1)$. We already saw that $q \geq p + 1$ so necessarily $q \mid p + 1$ and we deduce that $q = p + 1$ which implies $(p, q) = (2, 3)$.

Thus if $|G| = p^2 q \neq 12$ we showed G has a normal Sylow subgroup. The case $|G| = 12$ remains for next time. □