SYLOW THEOREMS

CHARLES REZK

This is a discussion of the Sylow theorems, as I presented it in class (mostly). It is presented a little differently than the book does it.

A **p-Sylow subgroup** of finite group G is a non-trivial subgroup $P \leq G$ which is a p-group, and is such that $|G : P|$ is prime to p. (Note: the book allows a p-Sylow subgroup to be trivial.)

Write $\mathrm{Syl}_p(G)$ for the set of p-Sylow subgroups, and write $n_p = \left|\mathrm{Syl}_p(G)\right|$.

Theorem 1 (Sylow)**.** *Let G be a group of order $p^a m$, where p is prime, p does not divide m, and $a \geq 1$.*

1. $\mathrm{Syl}_p(G) \neq \varnothing$.
2. *Any two p-Sylow subgroups are conjugate.*
3. *If P is any p-Sylow subgroup, then $n_p = |G : N_G(P)|$, whence $n_p | m$, and we also have $n_p \equiv 1 \mod p$.*

Proof of (1). This is an induction on $|G|$. If $|G| = p$, then G is its own p-Sylow subgroup.

Supose $|G| = p^a m > p$ with $a > 0$, and we've proved it for all subgroups of smaller order.

Claim.

(a) G has a proper subgroup $H \leq G$ of index prime to p, or
(b) G has a non-trivial normal subgroup $N \trianglelefteq G$ of order a power of p.

If (a) is true, then a p-Sylow subgroup of H is automatically a p-Sylow subgroup of G. If (b) is true, then G/N has a p-Sylow subgroup Q by induction. Since $|G/N| = p^b m$ with $b < a$, we see Q has index m in G/N. Thus, the preimage $P = \{\, g \in G \mid gN \in Q \,\}$ also has index m in G, so is a p-Sylow subgroup.

Now we prove the claim. Consider the class equation

$$p^a m = |G| = |Z(G)| + \sum |G : C_G(g_i)| \, .$$

Remember that $|G : C_G(g_i)| > 1$. We need to show if (a) is false, then (b) is true. If (a) is false, then p divides each $|G : C_G(g_i)|$. Since p divides $|G|$, it follows that p divides $Z(G)$. So ZG is an abelian group with order divisible by p, and we have shown that such a group has an element $x \in ZG$ of order p. Then $N = \langle x \rangle \trianglelefteq G$ satisfies the conditions of (b).

For part (2), we use the following fact.

Lemma 2. *Let $H, K \leq G$ be subgroups. Then there exists $x \in G$ such that $xKx^{-1} \subseteq H$ if and only if the left action of K on G/H has a fixed point.*

Proof. Suppose xH is a fixed point of the action of K on G/H. This means that for all $k \in K$, we have

$$kxH = xH.$$

Date: October 13, 2009.

Thus $x^{-1}kxH = H$, and so $x^{-1}Kx \subseteq H$.

Conversely, if $x^{-1}Kx \subseteq H$ for some x, then $k(xH) = xH$ for all $k \in K$. □

Proof of (2). Let $P, Q \in \mathrm{Syl}_p(G)$. We have $|G/P| = m$, which is not divisible by p. Consider the action of Q on G/P; the set G/P must be a disjoint union of orbits of the Q-action, so we have

$$m = |G/P| = c + \sum_{k=1}^{r} |O_k|,$$

where c is the number of fixed points of the action, and each orbit O_k has size bigger than one. Since $|O_k|$ divides $|Q| = p^a$, this means p divides $|O_k|$ for $k = 1, \dots, r$. If $c = 0$, then it follows that p divides m, a contradiction. Thus $c > 0$, and by the lemma we must have that Q is conjugate to P.

This proves more.

Proposition 3. *If $P \in \mathrm{Syl}_p(G)$, and $Q \leq G$ is any p-group, then Q is conjugate to a subgroup of P. In particular, any p-group of G is contained in a p-Sylow subgroup.*

The proposition is also proved by showing that the action of Q on G/P has a fixed point, in the same way.

Proof of (3). The G action on $\mathrm{Syl}_p(G)$ is transitive, by part (2) and the stabilizer group of $P \in \mathrm{Syl}_p(G)$ is $N_G(P)$. Thus $n_p = |G : N_G(P)|$ for any $P \in \mathrm{Syl}_p(G)$. Since $P \leq N_G(P)$, it follows that $n_p = |G : N_G(P)|$ divides $|G : P| = m$.

For the congruence result, we examine the action of P on the set $\mathrm{Syl}_p(G)$ by left multiplication. The set $\mathrm{Syl}_p(G)$ must be a disjoint union of orbits. Let c be the number of fixed points of this action, corresponding to the number of orbits which consist of one point sets. Then we have

$$n_p = \left|\mathrm{Syl}_p(G)\right| = c + \sum_{k=1}^{r} |O_k|$$

where the sum is over the orbits $O_1, \dots, O_r$ of size bigger than 1. Since each $|O_k|$ must divide $|P| = p^a$, it follows that p divides $|O_k|$ for each $k = 1, \dots, r$. Therefore $n_p \equiv c \mod p$. It remains to show that $c = 1$. It is clear that $P \in \mathrm{Syl}_p(G)$ is fixed under the action of conjugation by P, so we only need to show there are no others.

Suppose $Q \in \mathrm{Syl}_p(G)$ is fixed under conjugation by P; i.e., $pQp^{-1} = Q$ for all $p \in P$, which means that $P \leq N_G(Q)$. The groups P and Q must be p-Sylow subgroups of $N_G(Q)$, since $|N_G(Q)|$ divides $|G|$. But all p-Sylow subgroups of $N_G(Q)$ must be conjugate, and since Q is normal in $N_G(Q)$, it follows that $P = Q$.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, URBANA, IL
E-mail address: `rezk@math.uiuc.edu`