Sylow theorems, proof of

Canonical name	SylowTheoremsProofOf
Date of creation	2013-03-22 12:51:02
Last modified on	2013-03-22 12:51:02
Owner	Henry (455)
Last modified by	Henry (455)
Numerical id	12
Author	Henry (455)
Entry type	Proof
Classification	msc 20D20
Related topic	SylowPSubgroup
Related topic	SylowsThirdTheorem

We let G be a group of order $p^m k$ where $p \nmid k$ and prove Sylow's theorems. First, a fact which will be used several times in the proof:

Proposition 1. *If p divides the size of every conjugacy class outside the center then p divides the order of the center.*

Proof. This follows from the class equation:

$$|G| = |Z(G)| + \sum_{[a] \neq Z(G)} |[a]|$$

If p divides the left hand side, and divides all but one entry on the right hand side, it must divide every entry on the right side of the equation, so $p|Z(G)$. $\square$

Proposition 2. *G has a Sylow p-subgroup*

Proof. By induction on $|G|$. If $|G| = 1$ then there is no p which divides its order, so the condition is trivial.

Suppose $|G| = p^m k$, $p \nmid k$, and the holds for all groups of smaller order. Then we can consider whether p divides the order of the center, $Z(G)$.

If it does, then by Cauchy's theorem, there is an element f of $Z(G)$ of order p, and therefore a cyclic subgroup generated by f, $\langle f \rangle$, also of order p. Since this is a subgroup of the center, it is normal, so $G/\langle f \rangle$ is well-defined and of order $p^{m-1}k$. By the inductive hypothesis, this group has a subgroup $P/\langle f \rangle$ of order p^{m-1}. Then there is a corresponding subgroup P of G which has $|P| = |P/\langle f \rangle| \cdot |\langle f \rangle| = p^m$.

On the other hand, if $p \nmid |Z(G)|$ then consider the conjugacy classes not in the center. By the proposition above, since $Z(G)$ is not divisible by p, at least one conjugacy class can't be. If a is a representative of this class then we have $p \nmid |[a]| = [G : C(a)]$, and since $|C(a)| \cdot [G : C(a)] = |G|$, $p^m \mid |C(a)|$. But $C(a) \neq G$, since $a \notin Z(G)$, so $C(a)$ has a subgroup of order p^m, and this is also a subgroup of G. $\square$

Proposition 3. *The intersection of a Sylow p-subgroup with the normalizer of a Sylow p-subgroup is the intersection of the subgroups. That is, $Q \cap N_G(P) = Q \cap P$.*

Proof. If P and Q are Sylow p-subgroups, consider $R = Q \cap N_G(P)$. Obviously $Q \cap P \subseteq R$. In addition, since $R \subseteq N_G(P)$, the second isomorphism theorem tells us that RP is a group, and $|RP| = \frac{|R|\cdot|P|}{|R\cap P|}$. P is a subgroup of RP, so $p^m \mid |RP|$. But R is a subgroup of Q and P is a Sylow p-subgroup, so $|R| \cdot |P|$ is a multiple of p. Then it must be that $|RP| = p^m$, and therefore $P = RP$, and so $R \subseteq P$. Obviously $R \subseteq Q$, so $R \subseteq Q \cap P$. $\square$

The following construction will be used in the remainder of the proof:

Given any Sylow p-subgroup P, consider the set of its conjugates C. Then $X \in C \leftrightarrow X = xPx^{-1} = \{xpx^{-1} | \forall p \in P\}$ for some $x \in G$. Observe that every $X \in C$ is a Sylow p-subgroup (and we will show that the converse holds as well). We let G act on C by conjugation:

$$g \cdot X = g \cdot xPx^{-1} = gxPx^{-1}g^{-1} = (gx)P(gx)^{-1}$$

This is clearly a group action, so we can consider the orbits of P under it; this remains true if we only consider elements from some subset of G. Of course, if all G is used then there is only one orbit, so we restrict the action to a Sylow p-subgroup Q. the orbits $O_1, \ldots, O_s$, and let $P_1, \ldots, P_s$ be representatives of the corresponding orbits. By the orbit-stabilizer theorem, the size of an orbit is the index of the stabilizer, and under this action the stabilizer of any P_i is just $N_Q(P_i) = Q \cap N_G(P_i) = Q \cap P$, so $|O_i| = [Q : Q \cap P_i]$.

There are two easy results on this construction. If $Q = P_i$ then $|O_i| = [P_i : P_i \cap P_i] = 1$. If $Q \neq P_i$ then $[Q : Q \cap P_i] > 1$, and since the index of any subgroup of Q divides Q, $p \mid |O_i|$.

Proposition 4. *The number of conjugates of any Sylow p-subgroup of G is congruent to* 1 *modulo p*

In the construction above, let $Q = P_1$. Then $|O_1| = 1$ and $p \mid |O_i|$ for $i \neq 1$. Since the number of conjugates of P is the sum of the number in each orbit, the number of conjugates is of the form $1 + k_2p + k_3p + \cdots + k_sp$, which is obviously congruent to 1 modulo p.

Proposition 5. *Any two Sylow p-subgroups are conjugate*

Proof. Given a Sylow p-subgroup P and any other Sylow p-subgroup Q, consider again the construction given above. If Q is not conjugate to P then $Q \neq P_i$ for every i, and therefore $p \mid |O_i|$ for every orbit. But then the number of conjugates of P is divisible by p, contradicting the previous result. Therefore Q must be conjugate to P. $\square$

Proposition 6. *The number of subgroups of G of order p^m is congruent to* 1 *modulo p and is a factor of k*

Proof. Since conjugates of a Sylow p-subgroup are precisely the Sylow p-subgroups, and since a Sylow p-subgroup has 1 modulo p conjugates, there are 1 modulo p Sylow p-subgroups.

Since the number of conjugates is the index of the normalizer, it must be $|G : N_G(P)|$. Since P is a subgroup of its normalizer, $p^m \mid N_G(P)$, and therefore $|G : N_G(P)| \mid k$. $\square$