SYLOW THEOREMS
MATH 114

Let G be a finite group and $|G| = p^n q$, where p is prime and does not divide q. A subgroup of order p^n is called a Sylow p-subgroup.

Theorem 0.1. *There exists a Sylow p-subgroup.*

Proof. Proof goes by induction on $|G|$. For $|G| = p^n$ the statement is trivial. We assume that the statement is true for any group of order strictly less than $|G|$.

First, assume that G is abelian. Let $g \in G$ and $g \neq 1$. Let the order of g be $p^m b$ where p does not divide b.

First, assume that $m > 0$. Let N be the subgroup generated by g^b. Then $|N| = p^m$ and $|G/N| = p^{n-m}q$. By induction assumption there exists a subgroup H in G/N of order p^{n-m}. Consider the natural projection $\pi \colon G \to G/N$. The preimage $\pi^{-1}(H) = P$ is a subgroup in G of order p^n.

Now assume that $m = 0$. Let U be the subgroup generated by g. Then p does not divide $|U|$. By induction assumption G/U has a Sylow subgroup of order p^n. Hence there exists $u \in G/U$ of order p^k for some $k > 0$. Again consider the natural projection $\pi \colon G \to G/U$. Let $h \in G$ be such that $\pi(h) = u$. Then the order of h is $p^k d$. Now we can repeat the argument in the previous paragraph with $g = h$. The case of abelian G is done.

Now let G be not abelian. Let $c_1, \dots, c_k$ be all the conjugacy classes in G. Assume that $c_1 = \{1\}$. We have

$$|c_1| + \cdots + |c_k| = |G| = p^n q.$$

There is $i > 1$ such that $|c_i|$ is not divisible by p.

First, assume that $|c_i| > 1$. Pick up $x \in c_i$ and let

$$G_x = \left\{ g \in G \mid gxg^{-1} = x \right\}.$$

Since

$$|c_i||G_x| = |G| = p^n q$$

and p does not divide $|c_i|$ we obtain $|G_x| = p^n b$ for some $b < q$. By induction assumption G_x has a subgroup P of order p^n. Then P is a Sylow p-subgroup of G.

Now assume that we can not find c_i such that $|c_i| \neq 1$ and p does not divide $|c_i|$. All conjugacy classes of order 1 form the center $Z(G)$ of G. If $c_s, c_{s+1}, \dots, c_k$ are conjugacy classes of order > 1, then

$$|G| = p^n q = |c_s| + \cdots + |c_k| + |Z(G)|.$$

Date: February 1, 2006.

By our assumption p divides $|c_i|$ for all $i = s, \dots, k$. Therefore p divides $|Z(G)|$. Thus, we obtain that $|Z(G)| = p^k c$ for some $k > 0$, p does not divide c. By induction assumption one can find a subgroup N in $Z(G)$ of order p^k. Note that N is a normal subgroup of G. Again by induction assumption there is a subgroup H in G/N of order p^{n-k}. Consider the natural projection $\pi\colon G \to G/N$. The subgroup $P = \pi^{-1}(H)$ has order p^n.

Theorem is proven. □

Theorem 0.2. *The number of Sylow p-subgroup is congruent to 1 modulo p.*

Proof. Let Ω denote the set of all subgroups of G of order p^n. Then G acts on Ω by conjugation. Let $P \in \Omega$, define the subgroup

$$N(P) = \left\{ g \in G \mid gPg^{-1} = P \right\}.$$

Then the order of the G-orbit of P equals $\frac{|G|}{|N(P)|}$. By definition P is a normal subgroup of $N(P)$.

Lemma 0.3. *Let $P, P' \in \Omega$. Suppose that $P \subset N(P')$. Then $P = P'$.*

Proof. P' is normal in $N(P')$. By the second isomorphism theorem

$$P \cdot P'/P' = P/P \cap P'.$$

Let $|P/P \cap P'| = p^a$, then $|P \cdot P'| = p^{n+a}$. Therefore $a = 0$, $P' = P \cap P'$, that immediately implies $P = P'$. □

Consider now P-action on Ω by conjugation. Then every P-orbit has p^s elements and exactly one orbit has 1 element. Indeed, let C be a P-orbit of some $P' \in \Omega$. Then

$$|C| = \frac{|P|}{|N(P') \cap P|}.$$

Since $|P| = p^n$, $|C| = p^s$ for some s. If $|C| = 1$, then $P \subset N(P')$ and by Lemma 0.3 $P = P'$.

Since the number of elements in Ω is the sum of orders of all P-orbits, we obtain

$$|\Omega| \equiv 1 \mod p.$$

Theorem is proven. □

Theorem 0.4. *All Sylow p-subgroups are conjugate. In other words, if P and P' are two Sylow p-subgroups, then $P' = gPg^{-1}$ for some $g \in G$. In particular, all Sylow p-subgroups are isomorphic.*

Proof. We have to show that Ω has exactly one G-orbit. Assume that Ω' is a G-orbit of some $P \in \Omega$. It was proven above that all P-orbits have order p^s and there is only one P-orbit $\{P\}$ of order 1. But the order of Ω' is the sum of orders of P-orbits in Ω'. Hence

$$|\Omega'| \equiv 1 \mod p.$$

Suppose that $\Omega \neq \Omega'$. Then there is $Q \in \Omega$ such that $Q \notin \Omega'$. But then every Q-orbit in Ω' has order p^s with $s \geq 1$. Then we have

$$|\Omega'| \equiv 0 \mod p.$$

We obtain a contradiction. Hence our assumption $\Omega \neq \Omega'$ is wrong. □

Corollary 0.5. *The number of Sylow p-subgroups divides $|G|$.*