Math 371 Lecture #38  
§8.3 (Ed.2), 9.3 (Ed.3): The Sylow Theorems

The classification of finite nonabelian groups is vastly more complicated that that for finite abelian groups.

The first basic steps are the Sylow Theorems (pronounced SEE-low).

As with finite abelian groups, the close connection between the structure of a finite nonabelian group $G$ and the arithmetic properties of $|G|$ plays a fundamental role.

In general, the converse of Lagrange’s Theorem is false, but there is a partial converse.

First Sylow Theorem. If $G$ is finite group and $p$ is a positive prime such that $p^k || G$ for some $k \in \mathbb{N}$, then $G$ has a subgroup of order $p^k$.

Example. The order of the $A_7$ is $(1/2)7! = 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

By the First Sylow Theorem, the nonabelian group $A_7$ has subgroups of order 2, 4, 8, subgroups of order 3, 9, a subgroup of order 5, and a subgroup of order 7.

Corollary 9.14 (Cauchy’s Theorem). If $G$ is a finite group whose order is divisible by a positive prime $p$, then $G$ contains an element of order $p$.

Proof. Suppose that $p || |G|$.

Then by the First Sylow Theorem, there is a subgroup $K$ of $G$ with $|K| = p$.

Since $p$ is prime, then $K$ is cyclic, say $K = \langle a \rangle$ for some $a \in K$.

Then $|a| = p$. □

Example (Continued). In the nonabelian group $A_7$ there are elements of order 2, 3, 5, and 7 by Cauchy’s Theorem.

Definition. Let $G$ be a finite group $G$ and $p$ a positive prime. If $p^n$ is the largest power of $p$ that divides $|G|$, then the subgroup of $G$ with order $p^n$ is called a Sylow $p$-subgroup.

That Sylow $p$-subgroups exist is a consequence of the First Sylow Theorem.

Example. The order of the nonabelian group $S_5$ is $120 = 2^3 \cdot 3 \cdot 5$.

Every subgroup of $S_5$ of order 8 is a Sylow 2-subgroup.

One such Sylow 2-subgroup of $S_5$ is

$$H = \{(1), (2345), (24)(35), (2543), (35), (23)(45), (24), (25)(34)\}.$$  

How many Sylow 2-subgroups may $S_5$ have?

For each $x \in S_5$, the map $f_x : S_5 \to S_5$ given by $f_x(a) = x^{-1}ax$ is an inner automorphism of $S_5$.

Then, for each $x \in S_5$, the image $f_x(H)$ is also a Sylow 2-subgroup of $S_5$ because the inner automorphism $f_x$ preserves the order.

Proposition. If $K$ is a Sylow $p$-subgroup of a group $G$, then for each $x \in G$, then image $f_x(K) = x^{-1}Kx$ is also a Sylow $p$-subgroup of $G$. 

This then leads to the question: if $P$ and $K$ are Sylow $p$-subgroups of $G$, how are $P$ and $K$ related?

Second Sylow Theorem. If $P$ and $K$ are Sylow $p$-subgroups of a group $G$, then there exist $x \in G$ such that $f_x(K) = P$, i.e., $P = x^{-1}Kx$.

The immediate consequence of the Second Sylow Theorem it that all Sylow $p$-subgroups are isomorphic.

Corollary 9.16. Let $G$ be a finite group and $K$ a Sylow $p$-subgroup of $G$. Then $K$ is normal in $G$ if and only if $K$ is the only Sylow $p$-subgroup in $G$.

Proof. If $K$ is the only Sylow $p$-subgroup of $G$, then $f_x(K) = K$, i.e., $x^{-1}Kx = K$, for all $x \in G$, and hence $K$ is normal.

Now suppose $K$ is normal.

For a Sylow $p$-subgroup $P$, there exists $x \in G$ such that $f_x(K) = P$.

Since $K$ is normal, then $f_x(K) = K$, so that $P = K$. □

Example. The order of $A_4$ is $(1/2)4! = 12 = 2^2 \cdot 3$.

You showed in a Homework Problem (8.5 #7 Ed.3), that

$$N = \{(1), (12)(34), (13)(24), (14)(23)\}$$

is a normal subgroup of $A_4$.

The normal subgroup $N$ has order $2^2$ and so it is a Sylow 2-subgroup of $A_4$.

By Corollary 9.16, this normal subgroup $N$ is the only Sylow 2-subgroup of $A_4$.

When a group has more than two Sylow $p$-subgroups, then none of the Sylow $p$-subgroups are normal.

How many Sylow $p$-subgroups can there be?

Third Sylow Theorem. The number of Sylow $p$-subgroups of a finite group $G$ divides $|G|$ and is of the form $1 + pk$ for some $k = 0, 1, 2, \ldots$.

Example. A group $G$ of order $20 = 2^2 \cdot 5$ has at least one Sylow 5-subgroup by the First Sylow Theorem.

The number of Sylow 5-subgroups of $G$ divides 20 and is of the form $1 + 5t$ for $t \geq 0$ by the Third Sylow Theorem.

The divisors of 20 are 1, 2, 4, 5, 10, 20.

The numbers of the form $1 + pt$ are 1, 6, 11, 16, 21, \ldots.

The only number common to both of these lists is 1.

So a group of order 20 has exactly one Sylow 5-group, and because there is only one, it is a normal subgroup (by the Corollary of the Second Sylow Theorem).

Consequently, any group of order 20 is never simple, because it always has a normal subgroup (the Sylow 5-subgroup)!

The Third Sylow Theorem can also be used to classify certain groups.
Corollary 9.18. Let $G$ be a group of order $pq$ where $p$ and $q$ are primes such that $p > q$. If $q \nmid (p - 1)$, then $G \cong \mathbb{Z}_{pq}$.

Proof. By the First Sylow Theorem, there exists a Sylow $p$-subgroup of $G$.

By the Third Sylow Theorem, the number of Sylow $p$-subgroups of $G$ must divide $|G| = pq$ and be of the form $1 + pt$ for $t \geq 0$.

The only divisors of $pq$ are $1$, $p$, $q$, and $pq$.

Since $q < p$ there is no $t \geq 0$ such that $q = 1 + pt$.

If $p = 1 + pt$ for some $t \geq 0$, then $p(1 - t) = 1$, which says that $p \mid 1$, a contradiction.

If $pq = 1 + pt$ for some $t \geq 0$, then $p(q - t) = 1$, which says that $p \mid 1$, another contradiction.

Thus there is only one integer that divides $|G| = pq$ and is of the form $1 + pt$ for some $t \geq 0$, and that integer is $1$.

So there is only one Sylow $p$-subgroup $H$ of $G$.

By the Corollary of the Second Sylow Theorem, this Sylow $p$-subgroup is normal.

Now considering $q$, there is by the First Sylow Theorem a Sylow $q$-subgroup in $G$.

The number of Sylow $q$-subgroups of $G$ must divide $|G| = pq$ and be of the form $1 + qt$ for some $t \geq 0$.

The only divisor of $pq$ are $1$, $p$, $q$, and $pq$.

If $p = 1 + qt$ for some $t$, then $qt = p - 1$, which says that $q \mid (p - 1)$.

But this contradicts the hypothesis that $q \nmid (p - 1)$.

If $q = 1 + tq$ for some $t \geq 0$, then $q(t - 1) = 1$, which says that $q \mid 1$, a contradiction.

If $pq = 1 + tq$ for some $t \geq 0$, then $q(p - t) = 1$, which says that $q \mid 1$, another contradiction.

So there is only one Sylow $q$-subgroup $K$ of $G$, which by the Corollary of the Second Sylow Theorem, is normal.

We now have two normal subgroups $H$ and $K$ of $G$.

The intersection $H \cap K$ is a subgroup of both $H$ and $K$, and order of $H \cap K$ divides the orders of $H$ and $K$ by Lagrange’s Theorem.

With $|H| = p$ and $|K| = q$ being prime, we have that $|H \cap K| = 1$, so that $H \cap K = \{e\}$.

As we saw in the proof of Theorem 9.3 (Ed.3), every element of $HK = \{hk : h \in H, k \in K\}$ is uniquely written because $H \cap K = \{e\}$.

So the numbers of products in $HK$ is precisely $|H| \cdot |K|$.

Since $|G| = pq = |H| \cdot |K|$, we have that $G = HK$.

So by Theorem 9.3, we have that $G \cong H \times K$.

Since $p$ and $q$ are prime, we know that $H \cong \mathbb{Z}_p$ and $K \cong \mathbb{Z}_q$.

Thus $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$.

Since $(p, q) = 1$, therefore we have $G \cong \mathbb{Z}_{pq}$.

$\square$
Example. How many groups are there of order $95 = 19 \cdot 5$?

With $p = 19$, $q = 5$, we have $q \nmid (p - 1) = 18$.

By the Corollary to the Third Sylow Theorem, any group of order 95 is isomorphic to $\mathbb{Z}_{95}$. 