Chapter 11: Fundamental Theorem of Abelian Groups/Chapter 24: Sylow Theorems

Bret Benesh
College of St. Benedict/St. John’s University
Department of Mathematics

Math 331

**Outline**

1. **Fundamental Theorem of Abelian Groups**
2. **The Sylow Theorems**
3. **An application of the Sylow Theorems**

---

**Definition**

If $G$ and $H$ are groups, the *direct product* $G \times H$ is the set
\[ \{(g, h) \mid g \in G, h \in H\} \]

**Example**

$C_3 \times C_6 = \{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5), (1,0), (1,1), (1,2), (1,3), (1,4), (1,5), (2,0), (2,1), (2,2), (2,3), (2,4), (2,5)\}$

The operation is $(2,4) + (0,3) = (2 + 0, 4 + 3) = (2,7) = (2,1)$

**Example**

Note that $C_6 \cong C_2 \times C_3$ by $\phi((a,b)) = 3a + 4b$. So $\phi((1,1)) = 1$. (this works because 2 and 3 are relatively prime).

---

**Theorem (Fundamental Theorem of Abelian Groups)**

Let $G$ be a finite abelian group. Then $G \cong C_{p_1^{n_1}} \times C_{p_2^{n_2}} \times \ldots \times C_{p_m^{n_m}}$, where the $p_i$ are primes (although not necessarily distinct). Moreover, the $p_i$ and $m$ are uniquely determined.

**Proof.**

In Gallian’s textbook, but we will not discuss in class.
**Example**

Suppose $G$ is a finite abelian group of order $32 = 2^5$. Then $G$ is isomorphic to one of the following:

- $C_{32}$ corresponds to the partition $(5)$
- $C_{16} \times C_2$ corresponds to the partition $(4 + 1)$
- $C_8 \times C_4$ corresponds to the partition $(3 + 2)$
- $C_8 \times C_2 \times C_2$ corresponds to the partition $(3 + 1 + 1)$
- $C_4 \times C_4 \times C_2$ corresponds to the partition $(2 + 2 + 1)$
- $C_4 \times C_2 \times C_2 \times C_2$ corresponds to the partition $(2 + 1 + 1 + 1)$
- $C_2 \times C_2 \times C_2 \times C_2 \times C_2$ corresponds to the partition $(1 + 1 + 1 + 1 + 1)$

**Example**

Suppose $G$ is a finite abelian group of order $360 = 2^3 \cdot 3^2 \cdot 5$. Then $G$ is isomorphic to one of the following:

- $C_8 \times C_9 \times C_5 \cong C_{360}$
- $C_8 \times C_3 \times C_3 \times C_3$
- $C_2 \times C_4 \times C_9 \times C_3$
- $C_2 \times C_4 \times C_3 \times C_3 \times C_5$
- $C_2 \times C_2 \times C_2 \times C_3 \times C_5$
- $C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5$

**Significance of the Fundamental Theorem of Abelian Groups**

If you want to know about abelian groups, you only need to know about direct products of cyclic groups of prime power order.
Theorem (Lagrange’s Theorem)

Let $G$ be a finite group and $H$ be a subgroup of $G$. Then $|H|$ divides $|G|$.

Big Question: Is the converse of Lagrange’s Theorem true? i.e. Is it true that if $n$ divides $|G|$, then $G$ has a subgroup of order $n$?

No. We have already seen that $A_4$ ($|A_4| = 12 = 2 \cdot 6$) has no subgroup of order 6.

New Big Question: When is the converse of Lagrange’s Theorem true?

New Big Question: When is the converse of Lagrange’s Theorem true?

- All divisors of finite abelian groups
- The next theorem shows it is true for some divisors of all finite groups.

Theorem

The converse of Lagrange’s Theorem is true for all finite abelian groups.

Example

Let $G$ be an abelian group of order $360 = 2^3 \cdot 3^2 \cdot 5$, and suppose $G \cong C_2 \times C_2 \times C_2 \times C_3 \times C_5$. We will find a subgroup of order 60 = $2^2 \cdot 3 \cdot 5$.

We can take the subgroup generated by $(0,1,1,3,1)$. Note that

$\langle (0,1,1,3,1) \rangle \cong \{e\} \times C_2 \times C_2 \times C_3 \times C_5$,

which has order $1 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 60$.

Theorem

Let $G$ be a finite group and $p$ be a prime such that $p^n$ divides $|G|$. Then $G$ has a subgroup of order $p^n$.

Corollary (Cauchy’s Theorem)

Let $G$ be a finite group, and $p$ be a prime that divides $|G|$. Then $G$ has an element of order $p$.

Theorem (Sylow E (for “existence”))

Let $G$ be a finite group and $p$ be a prime that divides $|G| = p^n m$, where $p$ does not divide $m$. Then $G$ has a subgroup of order $p^n$. 
Definition
Let $p$ be a prime number. A finite $p$-group is a group of order $p^m$ for some integer $m$.

Definition
A Sylow $p$-subgroup of a group $G$ is a subgroup as the Sylow E Theorem.

Example
Consider $S_4$. Then $|S_4| = 24 = 2^3 \cdot 3$. We will find a subgroup of order $2^3 = 8$ and $3$.
- Let $H = \{(1,2,3), (1,3,2), (2,4), (1,4,2,3), (3,4), (1,2)(3,4), (1,3,2,4), (1,4)(2,3)\}$. Then $H$ is a subgroup (verify!) and $|H| = 2^3 = 8$.
- So $\langle (1,2,3) \rangle$ is a Sylow $3$-group of $S_4$ and $H$ is a Sylow $2$-group of $S_4$. 

Theorem
Let $G$ be a finite group and $p$ be a prime such that $p^n$ divides $|G|$. Then $G$ has a subgroup of order $p^n$.

Corollary (Cauchy's Theorem)
Let $G$ be a finite group, and $p$ be a prime that divides $|G|$. Then $G$ has an element of order $p$.

Theorem (Sylow E (for "existence"))
Let $G$ be a finite group and $p$ be a prime that divides $|G| = p^am$, where $p$ does not divide $m$. Then $G$ has a subgroup of order $p^a$.

Theorem (Sylow D (for "development"))
Let $G$ be a finite group and $P \subseteq G$ be a $p$-subgroup. Then there exists a Sylow $p$-subgroup $Q$ such that $P \subseteq Q$.

Theorem (Sylow C (for "conjugacy"))
Let $G$ be a finite group and $P, Q \subseteq G$ be Sylow $p$-subgroups. Then there exists a $g \in G$ such that $P^g = Q$.

Corollary
Let $G$ be a finite group and $P, Q \subseteq G$ be Sylow $p$-subgroups. Then $P \cong Q$. 
**Theorem (Sylow counting)**

Let $G$ be a finite group such that $|G| = p^a m$ where $p$ does not divide $m$. Let $n_p$ be the number of Sylow $p$-subgroups of $G$. Then $n_p \equiv 1 \mod p$ and $n_p$ divides $m$.

**Corollary**

If $P$ is the unique Sylow $p$-subgroup of a finite group $G$, then $P$ is normal in $G$.

---

**Example**

The Sylow $2$-subgroups of $S_3$ ($|S_3| = 2 \cdot 3$) are: $\langle (1,2) \rangle$, $\langle (1,3) \rangle$, and $\langle (2,3) \rangle$. So we have Sylow $E$, since one exists.

Since $\langle (1,3) \rangle^{(2,3)} = \langle (1,2) \rangle$, $\langle (2,3) \rangle^{(1,3)} = \langle (1,2) \rangle$, and $\langle (2,3) \rangle^{(1,2)} = \langle (1,3) \rangle$, Sylow $C$ holds in $S_3$ for $p = 2$.

Since there are $3 \equiv 1 \mod 2$ Sylow $2$-subgroups in $S_3$ and $3$ divides $6 = |S_3|$, we see that Sylow Counting holds.

Note that there is $1 \equiv 1 \mod 3$ Sylow $3$-subgroup in $S_3$ (namely, $\langle (1,2,3) \rangle$), so Sylow $E$, $C$, and Counting hold (since $1$ divides $6 = |S_3|$). (and the Sylow $3$-subgroup is normal in $G$).

---

**Theorem**

There are no simple groups of order $12$.

**Proof.**

Let $G$ be a group such that $|G| = 12 = 2^2 \cdot 3$. Let $n_3$ be the number of Sylow $3$-subgroups of $G$, and $n_2$ be the number of Sylow $2$-subgroups of $G$. If $n_3 = 1$, we are done by a previous corollary. So we may assume that $n_3 > 1$.

Since $n_3$ divides $2^2$ (since $|G| = 3 \cdot m$ with $m = 2^2$), we know that $n_3 \in \{1, 2, 4\}$. Since $n_3 > 1$ by assumption, $n_3 = 2$ or $n_3 = 4$. Since $2 \not\equiv 1 \mod 3$, we conclude $n_3 = 4$.

Now we count elements. Since each subgroup of order $3$ contains two unique non-identity elements, we know that $G$ has $2 \cdot n_3 = 2 \cdot 4 = 8$ elements of order $3$.

---

**Proof (continued).**

Let $X$ be the set of elements we have not counted yet. Then $|X| = |G| - 8 = 4$. But this is the size of the Sylow $2$-subgroup, so there can only be one Sylow $2$-subgroup. By a previous corollary, this Sylow $2$-subgroup must be normal, and $G$ is not simple.
Theorem
There are no simple groups of order $p^2q$ for primes $p$ and $q$.

Proof.
Let $G$ be a group such that $|G| = p^2q$. Let $n_q$ be the number of Sylow $q$-subgroups of $G$, and $n_p$ be the number of Sylow $p$-subgroups of $G$. If $n_q = 1$, we are done by a previous Corollary. So we may assume that $n_q > 1$.

Since $n_q$ divides $p^2$ (since $|G| = q \cdot m$ with $m = p^2$), we know that $n_q \in \{1, p, p^2\}$. Since $n_q > 1$ by assumption, $n_q = p$ or $n_q = p^2$.

Suppose $n_q = p$. Then $p \equiv 1 \pmod{q}$, and in particular, $p > q$. Therefore, $q \not\equiv 1 \pmod{p}$, so $n_p \neq q$. Then $n_p = 1$ and we have a normal Sylow $p$-subgroup.

So we may assume $n_q = p^2$, and we count elements. Since each subgroup of order $p$ contains $(q - 1)$ unique non-identity elements, we know that $G$ has $(q - 1) \cdot n_q = (q - 1)p^2$ elements of order $q$.

Let $X$ be the set of elements we have not counted yet. Then $|X| = |G| - (q - 1)p^2 = p^2q - (q - 1)p^2 = p^2$. But this is the size of the Sylow $p$-subgroup, so there can only be one Sylow $p$-subgroup. By a previous corollary, this Sylow $p$-subgroup must be normal, and $G$ is not simple.