Group Theory

Lecture 12, Sunday January 15, 2023
Ari Feiglin

12.1 Applications of Sylow's Theorems

Remember that all the p-Sylow subgroups of a group G is equivalent to 1 modulo p. That is if we define n_p to be the number of p-Sylow subgroups of G then

$$n_p \equiv 1 \pmod p$$

Recall that if P is a p-Sylow subgroup then the number of conjugates of P is $[G : N_G(P)]$ by the Orbit-Stabilizer theorem (since $N_G(P)$ is the stabilizer of P under conjugation). And so $n_p = [G : N_G(P)]$. Suppose $|G| = p^t \cdot m$ where $p^t \parallel |G|$ (so necessarily m is coprime with p) so $n_p \cdot |N_G(P)| = p^t \cdot m$, since we know that

$$P \triangleleft N_G(P) \leq G$$

So p^t divides $|N_G(P)|$ (it is a supergroup of P), and so $n_p \mid m$.

Definition 12.1.1:

G is an **inner direct product** of two subgroups $A, B \leq G$ if

(1) $A, B \trianglelefteq G$

(2) $AB = G$

(3) $A \cap B$ is trivial

Proposition 12.1.2:

If G is an inner direct product of A and B then $G \cong A \times B$.

Proof:

If $A, B \trianglelefteq G$ and $A \cap B$ is trivial then $ab = ba$ for every $a \in A$ and $b \in B$ since $aba^{-1}b^{-1} = a(bab^{-1})^{-1} \in A$ since A is normal, and similarly it is equal to $(aba^{-1})b^{-1} \in B$ so $aba^{-1}b^{-1} = e$ since the intersection is trivial, and so $ab = ba$. So we define the isomorphism

$$\varphi\colon A \times B \longrightarrow G, \qquad (a, b) \mapsto ab$$

this is trivially a homomorphism and obviously surjective by definition of inner direct products. It is injective since $ab = a'b'$ if and only if $a'a^{-1} = bb'^{-1}$ (since elements of A and B commute) and so $a'a^{-1} = bb'^{-1} = e$ since $A \cap B$ is trivial so $a = a'$ and $b = b'$. So φ is an isomorphism as required.

■

We can generalize the definition of inner direct products of $A_1, \dots, A_n$ where

(1) $A_1, \dots, A_n \trianglelefteq G$

(2) $A_1 \cdots A_n = G$

(3) For every $i = 1, \dots, n$, $A_i \cap \big(A_1 \cdots A_{i-1} \cdot A_{i+1} \cdots A_n\big)$ is trivial

Then we can show that if G is the inner direct product of $A_1, \dots, A_n$ then $G \cong A_1 \times \cdots \times A_n$ similar to how we did above.

Proposition 12.1.3:

If P_i is the p_i-Sylow normal subgroup then

$$|P_1 \cdots P_k| = |P_1| \cdots |P_k|$$

Note that P_i is normal if and only if $N_G(P_i) = G$, that is only if $n_{p_i} = 1$ so P_i is the only p_i-Sylow group. That is P_i is normal if and only if it is the only p_i-Sylow group.

Proof:

We do this inductively. We know that $P_i \cap \big(P_1 \cdots P_{i-1} \cdot P_{i+1} \cdots P_k\big)$ is trivial since the order of P_i is coprime with this product (since it is inductively equal to a product of powers of p_j) and so the product is an inner direct product, and therefore isomorphic to the direct product $P_1 \times \cdots \times P_n$, which has order $|P_1| \cdots |P_n|$ as required.

■

Proposition 12.1.4:

If every p-Sylow subgroup is normal then G is the inner direct product of them.

The proof is simple: suppose P_i are the p-Sylow groups of G then the order of $|P_1 \cdots P_k| = p_1^{t_1} \cdots p_k^{t_k} = |G|$, so $P_1 \cdots P_k = G$ and this is an inner direct product.

Example:

We can show that every group of order $5 \cdot 13 \cdot 19$. Suppose P_5 is a 5-Sylow group, it must be unique since $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 13 \cdot 19$. Since $13, 19, 13 \cdot 19 \not\equiv 1$ we must have that $n_5 = 1$ and similarly $n_{13} = n_{19} = 1$, so P_5, P_{13} and P_{19} are all normal, so

$$G = P_5 \cdot P_{13} \cdot P_{19} \cong P_5 \times P_{13} \times P_{19}$$

this is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19}$ since groups of prime order are cyclic, and this is isomorphic to $\mathbb{Z}_{5 \cdot 13 \cdot 19}$.

Proposition 12.1.5:

Suppose P is a p-Sylow subgroup of G then

$$N_G\big(N_G(P)\big) = N_G(P)$$

Proof:

Let $x \in N_G\big(N_G(P)\big)$ then

$$xPx^{-1} \subseteq xN_G(P)x^{-1} = P$$

since x normalizes $N_G(P)$. So xPx^{-1} is a p-Sylow subgroup of $N_G(P)$, but since P is normal in $N_G(P)$, it is unique in it, so $xPx^{-1} = P$ so $x \in N_G(P)$.

■

Proposition 12.1.6:

If P is a p-Sylow subgroup and $N_G(P) \subseteq H$ then $N_G(H) = H$.

Proof:

The proof here is similar to the proof above. Let $x \in N_G(H)$ then

$$xPx^{-1} \subseteq xN_G(P)x^{-1} \subseteq xHx^{-1} = H$$

since x normalizes H. And so $xPx^{-1} \subseteq H$ and so xPx^{-1} is a p-Sylow subgroup of H, and since all p-Sylow groups are conjugates there must be an $h \in H$ such that $xPx^{-1} = hPh^{-1}$. And so $(h^{-1}x)P(h^{-1}x)^{-1} = P$ and therefore $h^{-1}x \in N_G(P)$, so $x \in h \cdot N_G(P) \subseteq H$. So $H \subseteq N_G(H)$ and therefore are equal.

■

Example 12.1.7:

Groups of order 72 are not simple. We know that $72 = 2^3 \cdot 3^2$ so

$$n_2 = 1, 3, 9$$
$$n_3 = 1, 4$$

as these are the numbers coprime with their respective primes and equivalent to 1 modulo the prime. Suppose that 72 is simple, then the p-Sylow groups cannot be normal, so $n_2, n_3 \neq 1$ and so $n_3 = 4$.
Recall that by the refinement of Cayley's Theorem, if $H \leq G$ and $m = [G : H]$ then their is a homomorphism $G \to S_m$. So by this refinement on $N_G(P_3)$, there is a homomorphism $G \to S_4$, since $72 \nmid 4! = 24$, this cannot be an injective homomorphism, so it must have a kernel. Since kernels are normal subgroups, G cannot be simple in contradiction.

Example 12.1.8:

We can do something similar for groups of order $90 = 2 \cdot 3^2 \cdot 5$ since $n_3 = 1, 10$ and $n_5 = 1, 6$. If the group is simple then $n_3 = 10$ and $n_5 = 6$, notice then that $N_G(P_3) = P_3$. By Cayley's refinement there is a homomorphism $G \to S_6$, and if we assume G is simple this must be a monomorphism. We now use G to mean its image in S_6, notice that

$$G/_{G \cap A_6} \cong {}^{G \cdot A_6}/_{A_6}$$

and since G either has odd permutations or doesn't, so this is either trivial or $\mathbb{Z}_2$. If $G \nsubseteq A_6$ then this is $\mathbb{Z}_2$ so $G \cap A_6 \triangleleft G$ as it has index 2, but G is simple. So $G \subseteq A_6$, and since $[A_6 : G] = 4$ this creates a homomorphism $A_6 \to S_4$ and it must be a monomorphism since A_6 is simple. But this is cannot be since $\frac{6!}{2} = 360$ and $4! = 24$.

In general if G is simple and has a subgroup of index m then $G \hookrightarrow A_m$.

Example 12.1.9:

We will show that the only simple group of order 60 is A_5.
Suppose G is a simple group of order 60, then since $60 = 2^2 \cdot 3 \cdot 5$ so

$$n_2 = 3, 5, 15$$
$$n_3 = 4, 10$$
$$n_5 = 6$$

n_2 cannot be 3 since if it were, there'd be a monomorphism $G \hookrightarrow A_3$ which cannot be. And similarly $n_3 \neq 4$, so $n_3 = 10$. In any case, G has 6 5-Sylow groups which then must all be isomorphic to $\mathbb{Z}_5$, and their intersections must be trivial (since it divides 5). Each of these subgroups has 4 elements of order 5, so there are at least $6 \cdot 4 = 24$ elements of order 5. Similarly there must be $10 \cdot 2 = 20$ elemenets of order 3.
Now suppose $n_2 = 5$ then there is a monomorphism (in fact it is an isomorphism) $G \hookrightarrow A_5$ as required. So suppose $n_2 = 15$ then there are 15 elements of order 2. If all the 2-Sylow subgroups have trivial intersections, then since all these subgroups are of order 4, there must be $15 \cdot (4 - 1) = 45$ elements of orders powers of 2. But notice that

$$60 = 1 + 20 + 24 + 15$$

the 1 is the identity, there are 20 elements of order 3 and 24 of power 5, so there can only be 15 elements of order powers of 2. So there must be two 2-Sylow groups with non-trivial intersections, let them be P and P'. Let $Q = P \cap P'$ which has order 2, and let $Q = N_G(P \cap P')$. Since P, P' are abelian we must have that $P \subset Q$, so the order of Q must be a multiple of 4, namely $12, 20, 60$. It cannot be 60 since then Q would be normal. If it is 12 then its index is 3, which is a contradiction (as $N_G(P) \supseteq Q$ and so $n_2 = 15$ is smaller than its index), and similarly it cannot be 20, in contradiction.

12.2 Subnormal Sequences

Definition 12.2.1:

A **sub-normal series** is a sequence of subgroups $G_i \leq G$ such that

$$\{e\} = G_k \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$$

if $G_i \triangleleft G$ then the sequence is considered to be a **normal series**.

Definition 12.2.2:

A subnormal series is a **composition series** if the quotients ${}^{G_i}\!/\!_{G_{i+1}}$ are simple.

This is equivalent to saying the sequence cannot be extended, ie we cannot add another subgroup into the sequence. Suppose we could add a subgroup, $G_{i+1} \triangleleft G' \triangleleft G_i$ then ${}^{G'}\!\Big/\!_{G_{i+1}} \triangleleft {}^{G_i}\!/\!_{G_{i+1}}$, in contradiction.
In a finite group we can extend every subnormal series to a composition series.
The quotients in a composition series are called the *composition factors*.

Theorem 12.2.3 (Jordan-Holder Theorem):

Every two composition seriess of the same group have the same composition factors, up to order. Specifically, they have the same lengths.

Proof:

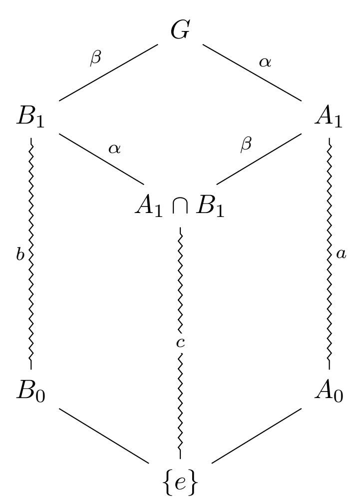
Suppose we have two composition seriess:

$$\{e\} \triangleleft A_n \triangleleft \cdots \triangleleft A_1 \triangleleft A_0 = G$$
$$\{e\} \triangleleft B_m \triangleleft \cdots \triangleleft B_1 \triangleleft B_0 = G$$

If $A_1 = B_1$ then the rest of the sequences (without A_0 and B_0) are composition seriess of A_1 and B_1 and so are equal inductively.
Otherwise by the isomorphism theorems

$${}^{A_1}\!/\!_{A_1 \cap B_1} \cong {}^{A_1 B_1}\!/\!_{A_1}$$

and since we can't add another group between $G = A_0$ and A_1, we must have that $A_1 B_1 = G$ (since $A_1 \triangleleft A_1 B_1$).
If we create a new composition series from $A_1 \cap B_1$ we get



Notice that the composition factor from G to A_1 is α which is also the composition factor from A_1 to $A_1 \cap B_1$ because

$$\alpha = {}^{G}\!/\!_{A_1} \cong {}^{A_1}\!/\!_{A_1 \cap B_1}$$

as explained above, similar for β.

Inductively

$$a \sim \beta + c \qquad b \sim \alpha + c$$

where $+$ denotes adding the composition factor to the composition chain, and so

$$\alpha + a \sim \alpha + (\beta + c) \qquad \beta + b \sim \beta + (\alpha + c)$$

and so the composition factors in $\alpha + a$ and $\beta + b$ are the same (since they are the composition factors in c, and α and β), as required.

■

There is a small loose end here where we assumed that there exists a composition series on $A_1 \cap B_1$. This is true if $A_1 \cap B_1$ is finite.