Advanced Algebra I

Nilpotent and solvable groups, normal series, Jordan-Hölder theorem

Let G be a group, the center $Z(G)$ is a normal subgroup of G. And we have the canonical projection $G \to G/Z(G)$. Let $C_2(G)$ be the inverse image of $Z(G/Z(G))$ in G. By the correspondence theorem, $Z(G/Z(G))$ is a normal subgroup of $G/Z(G)$ hence $C_2(G)$ is a normal subgroup of G. And then let $C_3(G)$ to be the inverse image of $Z(G/C_2(G))$. By doing this inductively, one has an ascending chain of normal subgroups

$$\{e\} < C_1(G) := Z(G) < C_2(G) < ...$$

Definition 0.1. *G is nilpotent if $C_n(G) = G$ for some n.*

Proposition 0.2. *A finite p-group is nilpotent.*

Proof. We use the fact that a finite p-group has non-trivial center. Thus one has $C_i \lneqq C_{i+1}$. The group G has finite order thus the ascending chain must terminates, say at C_n. If $C_n \neq G$, then G/C_n has non-trivial center. One has $C_n \lneqq C_{n+1}$ which is impossible. Hence $C_n = G$. □

Theorem 0.3. *If H, K are nilpotent, so is $H \times K$.*

Proof. The key observation is that $Z(H \times K) = Z(H) \times Z(K)$. Then inductively, one proves that $C_i(H \times K) = C_i(H) \times C_i(K)$. If $C_n(H) = H, C_m(K) = K$ then $C_l(H \times K)$ for $l = max(m, n)$. □

Then we are ready to prove the following:

Theorem 0.4. *A finite group is nilpotent if and only if it's a direct product of Sylow p-subgroups.*

Proof. By the previous two results, it's clear that a direct product of Sylow p-subgroups is nilpotent.

Conversely, if G is nilpotent, then we can claim that every Sylow p-subgroup is a normal subgroup of G. Then by checking the decomposition criterion, one has the required decomposition.

Claim. If P is Sylow p-subgroup, then $P \lhd G$.

To this end, it suffices to prove that $N_G(P) = G$. We prove the following claim:

Claim. If H is a proper subgroup of a nilpotent group G, then H is a proper subgroup of $N_G(H)$.

By applying this Claim to $N_G(H)$, then it says that $N_G(H)$ can't be a proper subgroup of G since $N_G(N_G(H)) = N_G(H)$. Thus it follows that $N_G(H) = G$. □

We have seen that we have a series of subgroup by taking centers. Another similar construction is to take commutators.

Definition 0.5. *Let G be a group. The commutator of G, denoted G' is the subgroup generated by the subset $\{aba^{-1}b^{-1}\}$.*

Roughly speaking, the subgroup G' measures measure the commutativity of a group. The smaller G', the more commutative it is.

Theorem 0.6. *$G' \lhd G$, and G/G' is ableian. Moreover, if $N \lhd G$, then G/N is abelian if and only if $G' < N$.*

Proof. (1) for all $g \in G$, $g(aba^{-1}b^{-1}g^{-1} \in G'$, hence $gG'g < G'$. So $G' \lhd G$.

(2)

$$aG'bG' = abG' = ab(b^{-1}a^{-1}ba)G' = baG' = bG'aG'.$$

(3) Consider $\pi : G \to G/N$. If G/N is abelian, then $\pi(aba^{-1}b^{-1} = e$, hence $G' < N$. Conversely, if $G' < N$, we have a surjective homomorphism $G/G' \to G/N$. G/G' is abelian, hence so is it homomorphic image G/N.

□

Definition 0.7. *We can define the the commutator inductively, i.e. $G^{(2)} := (G')', etc.$ The $G^(i)$ is called the i-th derived subgroup of G. It's clear that $G > G' > G^{(2)} > ....$*

A group is solvable is $G^(n) = \{e\}$ for some n.

Example 0.8. *Take $G = S_4$. The commutator is the smallest subgroup that G/G' is abelian. Since the only non-trivial normal subgroups of S_4 are V, A_4. It's clear that $G' = A_4$ (Or one can prove this by hand). Similarly, one finds that $G^{(2)} = A_4' = V$, and $G^{(3)} = \{e\}$. Hence S_4 is solvable.*

Another useful description of solvable groups is the groups with *solvable series*.

Definition 0.9. *A groups G has a subnormal series if there is a series of subgroups of G*

$$G = H_0 > H_1 > H_2 > ... > H_n,$$

such that $H_i \lhd H_{i-1}$ for all $1 \leq i \leq n$.

A subnormal series is a solvable series if $H_n = \{e\}$ and H_{i-1}/H_i is abelian for all $1 \leq i \leq n$.

A subnormal series is a normal series if all H_i are normal subgroups of G.

Theorem 0.10. *A group is solvable if and only it has a solvable series.*

Proof. It's clear that $G > G' > ...G^{(n)} = \{e\}$ is a solvable series. It suffices to prove that a group with a solvable series is solvable. Suppose now that G has a sovable series $\{e\} = H_n < ... < H_0 = G$. First observe that $G' < H_1$ since G/H_1 is abelian. We claim that $G^(i) < H_i$

for all i inductively. Which can be prove by the observation that the intersection of the series $\{e\} = H_n < ... < H_0 = G$ with $G^{(i)}$ gives a solvable series of $G^{(i)}$. □

Example 0.11. *A finite p-group has a solvable series, hence is solvable. Moreover, a nilpotent group is solvable.*

Proposition 0.12. *Let H be a subgroup of a solvable group G, then H is solvable.*

Let N be a normal subgroup of G. Then G is solvable if and only if both N and G/N are solvable.

Example 0.13. *A_5 is not solvable, hence so is S_n for $n \geq 5$.*

0.1. **simplicity of A_5.** An element in S_n is said to be have cycle structure $(m_1, .., m_r)$ with $m_1 \geq m_2 \geq ... \geq m_r$, $m_1 + ... + m_r = n$ if its cycle decomposition is of length $m_1, ..., m_r$ respectively. For example, $(1, 2)(3, 4) \in S_4$ has cycle structure $(2, 2)$ and $(1, 2) \in S_4$ has cycle structure $(2, 1, 1)$.

Remark 0.14. *There is a one-to-one correspondence between cycle structures of S_n and partition of the integer n.*

A key observation is that any two elements are conjugate to each other if and only if they have the same cycle structure. Let's call the set of all elements of cycle structure $(m_1, ..., m_r)$ the cycle class of $(m_1, ...m_r)$. A consequence of this fact is that a subgroup $N < S_n$ is normal if and only if N is union of cycle classes.

Let's put it another way, given a group G, we can always consider the group action $G \times G \to G$ by conjugation. The conjugate classes are the orbits. A subgroup $H < G$ is normal if and only if it is union of orbits. If $G = S_n$, then orbits are cycle classes.

Example 0.15. *In S_4, V is the union of class $(1, 1, 1, 1)$ and $(2, 2)$. A_4 is the union of V and the class $(3, 1)$.*

The purpose of this subsection is to show that A_5 is a simple non-abelian group, hence a non-solvable group.

Theorem 0.16. *A_5 is a simple non-abelian group.*

Proof. One note that in S_5, possible cycle structures are $(5), (4, 1),(3, 1 , 1),(3, 2), (2, 2, 1), (2, 1, 1, 1), (1, 1, 1, 1, 1)$ with $24, 30, 20, 20, 15, 10, 1$ elements in each class. While A_5 is the union of classes of $(5), (3, 1, 1), (2, 2, 1), (1, 1, 1, 1, 1)$.

We consider the actions of conjugation $\alpha : S_5 \times A_5 \to A_5$ and its restriction $\beta : A_5 \times A_5 \to A_5$. For $\sigma \in A_5$, let $\mathcal{O}_{\alpha,\sigma}$ be the orbit of the α and $\mathcal{O}_{\beta,\sigma}$ be the orbit of the β. And let $G_{\alpha,\sigma}, G_{\beta,\sigma}$ be the stabilizer.

It's clear that $G_{\alpha,\sigma} = C_{S_5}(\sigma)$ and $G_{\beta,\sigma} = C_{A_5}(\sigma) = C_{S_5}(\sigma) \cap A_5$. Thus we have either $|G_{\beta,\sigma}| = \frac{1}{2}|G_{\alpha,\sigma}|$ or $|G_{\beta,\sigma}| = |G_{\alpha,\sigma}|$. Hence $|\mathcal{O}_{\beta,\sigma}| = |\mathcal{O}_{\alpha,\sigma}|$ or $|\mathcal{O}_{\beta,\sigma}| = \frac{1}{2}|\mathcal{O}_{\alpha,\sigma}|$.

case 1. If σ has cycle structure (5), then $|\mathcal{O}_{\alpha,\sigma}| = 24, |G_{\alpha,\sigma}| = 5$. It follows that $|G_{\beta,\sigma}| = 5$ and hence $|\mathcal{O}_{\beta,\sigma}| = 12$.

case 2. If σ has cycle structure $(3,1,1)$, then $|\mathcal{O}_{\alpha,\sigma}| = 20, |G_{\alpha,\sigma}| = 6$. However, one notice that there is an element $\tau \in C_{S_5}(\sigma) - C_{A_5}(\sigma)$ (e.g. $(45)(123) = (123)(45)$). Hence $|G_{\beta,\sigma}| \neq |G_{\alpha,\sigma}|$ and must be $\frac{1}{2}|G_{\alpha,\sigma}| = 3$. Therefore $|\mathcal{O}_{\beta,\sigma}| = 20$.

case 3. If σ has cycle structure $(2,2,1)$,then $|\mathcal{O}_{\alpha,\sigma}| = 15, |G_{\alpha,\sigma}| = 8$. It follows that $|\mathcal{O}_{\beta,\sigma}| = 15$.

Combining all this, if $H < A_5$ is a normal subgroup, then $|H| = 1 + 12r_1 + 20r_2 + 15r_3$, where r_i are integers. Moreover $|H| \mid |A_5| = 60$, which is impossible unless $|H| = 1$ or 60.

□

WE turning back to series a little bit more. A subnormal series is called a composition series if every quotient is a simple group.

Definition 0.17. *For a subnormal series, $\{e\} = H_n < ... < H_0 = G$, the factors of the series are the quotient groups H_{i-1}/H_i and the length is the number of non-trivial factors. A refinement is a series obtained by finite steps of one-step refinement which is $\{e\} = H_n < . < K < .. < H_0 = G$.*

Definition 0.18. *Two series are said to be equivalent if there is a one-to-one correspondence between the non-trivial factors. And the corresponding factors groups are isomorphism.*

It's clear that this defines an equivalent relation on subnormal series.

The main theorems are

Theorem 0.19 (Schreier)**.** *Any two subnormal (resp. normal) series of a group G have a subnormal (resp. normal) refinement that are equivalent.*

An immediate corollary is the famous Jordan-Hölder theorem.

Theorem 0.20 (Jordan-Hölder)**.** *Any two composition series of a group are equivalent.*

The main technique is the Zassenhaus Lemma, or sometimes called butterfly Lemma.

Lemma 0.21 (Zassenhaus)**.** *Let $A^* \lhd A$ and $B^* \lhd B$ be subgroups of G. Then*

(1) $A^*(A \cap B^*) \lhd A^*(A \cap B)$.
(2) $B^*(A \cap B) \lhd B^*(A \cap B)$.
(3) $A^*(A \cap B)/A^*(A \cap B^*) \cong B^*(A \cap B)/B^*(A^* \cap B)$.

proof of the lemma. It's clear that $A \cap B^* = (A \cap B) \cap B^* \lhd A \cap B$. And similarly, $A^* \cap B \lhd A \cap B$. Let $D = (A \cap B^*)(A^* \cap B) \lhd A \cap B$. One can have a well-defined homomorphism $f : A^*(A \cap B) \to A \cap B/D$ with kernel $A^*(A \cap B^*)$. And similarly for the other homomorphism. □

proof of Schreier's theorem. Let $\{e\} = G_{n+1} < ... < G_0 = G$ and $\{e\} = H_{m+1} < ... < H_0 = G$ be two subnormal series. Let $G(i,j) =:= G_{i+1}(G_i \cap H_j)$ (resp. $H(i,j) := H_{j+1}(G_i \cap H_j)$). Then one has a refinement

$$G = G(0,0) > G(0,1) > ... > G(0,m) > G(1,0) > ... > G(n,m),$$

$$G = H(0,0) > H(1,0) > ... > H(n,0) > H(0,1) > ... > H(n,m).$$

By applying Zaseenhaus Lemma to $G_{i+1}, G_i, H_{j+1}, H_j$, one has

$$G(i,j)/G(i,j+1) \cong H(i,j)/H(i+1,j).$$

□