MATH 6121 lecture notes

TRANSCRIBED AND FORMATTED BY JOHN M. CAMPBELL
jmaxwellcampbell@gmail.com

6 September 27 lecture

6.1 The Jordan-Hölder theorem

A **subnormal series** of a group G is a sequence of subgroups of G such that each such subgroup is a (proper) normal subgroup of the next.

If G is a finite group, then there exists a sequence of normal subgroups

$$\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_{k-1} \lhd N_k = G$$

such that $N_i \lhd N_{i+1}$ and N_{i+1}/N_i is simple. A sequence of this form is referred to as a **composition series**, and factors of the form N_{i+1}/N_i are referred to as **composition factors**.

So, a composition series may be defined as a subnormal series such that each factor group is simple.

There are mainly two types of applications of the group-theoretic results given in MATH 6121:

(i) Applications involving enumerative problems, e.g., enumerative problems involving permutations; and

(ii) Applications in Galois theory.

Question 6.1. What are some applications of structure theorems for finite groups?

Definition 6.2. A finite group G is said to be **solvable** if it has a subnormal series whose factor groups are all abelian.

Remark 6.3. A fundamental result in Galois theory states that a polynomial equation is solvable by radicals iff its corresponding Galois group is a solvable group.

Claim 6.4. Given a composition series

$$\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_{k-1} \lhd N_k = G,$$

and second composition series

$$\{1\} = M_0 \lhd M_1 \lhd \cdots \lhd M_{k-1} \lhd M_\ell = G,$$

then there exists a permutation π such that $N_{i+1}/N_i \cong M_{\pi(i)+1}/M_{\pi(i)}$ for all indices i.

The above claim is one way of formulating the Jordan-Hölder theorem.

Our strategy is to use induction. First of all, if G is or prime order, or is of order 1, then G is simple. So, in this base case, the only possible composition series is of the form $\{1\} \unlhd G$.

Now suppose that it is not the case that G is simple. So, there exists a nontrivial proper normal subgroup N of G.

So, there is a composition series for N and G/N, as illustrated below:

$$\boxed{\begin{array}{llllllllll} \{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_\ell = & N & \leq & H_{\ell+1} & \leq & H_{\ell+2} & \leq & \cdots & \leq & G \\ & \updownarrow & & \updownarrow & & \updownarrow & & & & \updownarrow \\ & N/N & \lhd & \overline{H}_{\ell+1} & \lhd & \overline{H}_{\ell+2} & \lhd & \cdots & \lhd & G/N \end{array}}$$

By the fourth isomorphism theorem, we have that there is a bijection between the set of expressions of the form $\overline{H}_{\ell+i} \leq G/N$ and the set of expressions of the form $H_{\ell+i} \leq G$.

If $\overline{H}_{\ell+i} \trianglelefteq G/N$, then $H_{\ell+i} \trianglelefteq G$, but we need to show the result given in the following exercise.

Exercise 6.5. Check that since $\overline{H}_{\ell+i} \trianglelefteq \overline{H}_{\ell+i+1}$ then $H_{\ell+i} \trianglelefteq H_{\ell+i+1}$.

Now, we want to show that given two composition series for a group, these composition series are "*essentially the same up to permutation*".

According to Wikipedia, the Jordan-Hölder theorem states that any two composition series of a given group are equivalent in the sense that they have the same composition length and the same composition factors, up to permutation and isomorphism.

$$\begin{array}{ccccccccc} \{1\} = N_0 & \trianglelefteq & N_1 & \trianglelefteq & \cdots & \trianglelefteq & N_k & \trianglelefteq & N_{k+1} \\ & & & & & & & & \parallel \\ & & & & & & & & G \\ & & & & & & & & \parallel \\ \{1\} = M_0 & \trianglelefteq & M_1 & \trianglelefteq & \cdots & \trianglelefteq & M_\ell & \trianglelefteq & M_{\ell+1} \end{array}$$

We want to show that the above composition factors are permuted. We may assume without loss of generality that $M_\ell \neq N_k$.

6.1.1 An illustration of the Jordan-Hölder theorem

To illustrate the Jordan-Hölder theorem, consider the normal subgroups of the cyclic group $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z} \cong C_6$. Since this group is abelian, each subgroup of this group is a normal subgroup.

Writing $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, we have that the set $\{0, 2, 4\}$ forms a normal subgroup of $\mathbb{Z}_6$ which is isomorphic to $\mathbb{Z}_3$, and the set $\{0, 3\}$ forms a normal subgroup of $\mathbb{Z}_6$ which is isomorphic to $\mathbb{Z}_2$.

Now consider the following sequences of normal subgroups:

$$\begin{array}{ccccc} \{0\} & \lhd & \mathbb{Z}_3 & \lhd & \mathbb{Z}_6 \\ \updownarrow & & \updownarrow & & \updownarrow \\ \{0\} & \lhd & \mathbb{Z}_2 & \lhd & \mathbb{Z}_6 \end{array}$$

The above sequences are both subnormal series.

Since $\mathbb{Z}_3/\{0\} \cong \mathbb{Z}_3$ is a simple group, and since $\mathbb{Z}_6/\mathbb{Z}_3 \cong \mathbb{Z}_2$ is a simple group, we have that the sequence

$$\{0\} \lhd \mathbb{Z}_3 \lhd \mathbb{Z}_6$$

is a composition series.

Similarly, since $\mathbb{Z}_2/\{0\} \cong \mathbb{Z}_2$ is a simple group and since $\mathbb{Z}_6/\mathbb{Z}_2 \cong \mathbb{Z}_3$ is a simple group, we have that the sequence

$$\{0\} \lhd \mathbb{Z}_2 \lhd \mathbb{Z}_6$$

is also a composition series.

Consider the **lattice** structure formed by the subgroups of $\mathbb{Z}_6$ illustrated below [1].

$$
\begin{tikzcd}
 & \mathbb{Z}_6 \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Z}_2 \arrow[dr, dash] & & \mathbb{Z}_3 \arrow[dl, dash] \\
 & \{0\} &
\end{tikzcd}
$$

There is a natural isomorphism between the composition series $\{0\} \triangleleft \mathbb{Z}_3 \triangleleft \mathbb{Z}_6$ and the composition series $\{0\} \triangleleft \mathbb{Z}_2 \triangleleft \mathbb{Z}_6$. Moreover, there is a natural isomorphism between the *composition factors* in these series, as illustrated below:

$$
\begin{array}{cc}
\mathbb{Z}_3/\{0\} & \mathbb{Z}_6/\mathbb{Z}_3 \\
\updownarrow & \updownarrow \\
\mathbb{Z}_6/\mathbb{Z}_2 & \mathbb{Z}_2/\{0\}
\end{array}
$$

6.1.2 A sketch of an inductive argument involving the second isomorphism theorem

Again consider the following two composition series, and recall that we may assume without loss of generality that $M_\ell \neq N_k$.

$$
\begin{array}{ccccccccccc}
\{1\} = N_0 & \trianglelefteq & N_1 & \trianglelefteq & \cdots & \trianglelefteq & N_k & \trianglelefteq & N_{k+1} \\
 & & & & & & & & \| \\
 & & & & & & & & G \\
 & & & & & & & & \| \\
\{1\} = M_0 & \trianglelefteq & M_1 & \trianglelefteq & \cdots & \trianglelefteq & M_\ell & \trianglelefteq & M_{\ell+1}
\end{array}
$$

To prove that the composition factors given by each of the above series are permutations of each other, we make use of an inductive approach, illustrated by the following diagram.

$$
\begin{tikzcd}
 & & G \arrow[dl, dash, "\trianglelefteq"'] \arrow[dr, dash, "\trianglerighteq"] & & \\
 & N_k \arrow[dl, dash] \arrow[dr, dash] & & M_\ell \arrow[dl, dash] \arrow[dr, dash] & \\
N_{k-1} \arrow[r, leftrightarrow] & & N_k \cap M_\ell \arrow[l, leftrightarrow] \arrow[r, leftrightarrow] & & M_{\ell-1}
\end{tikzcd}
$$

composition factors permute

[1] See `https://en.wikipedia.org/wiki/Lattice_of_subgroups`.

Is it true that $N_k \cap M_\ell \trianglelefteq N_k$?

Verify that $N_k \cap M_\ell \trianglelefteq N_k$ and that $N_k \cap M_\ell \trianglelefteq M_\ell$.

To verify this, apply the second isomorphism theorem.

Observe that we're not *directly* showing how to obtain a permutation for the composition factors. We are using a complicated induction argument that "obliquely" shows that there exists a permutation for the composition factors.

By the second isomorphism theorem, we have that:

$$N_k/N_k \cap M_\ell \cong N_k M_\ell / M_\ell.$$

You need to show that:

(i) $N_k M_\ell$ forms a subgroup;

(ii) $N_k M_\ell$ is normal in G; and

(iii) $N_k M_\ell$ contains M_k and M_ℓ.

Use the above argument to show that $N_k M_\ell = G$.

$\therefore N_k/N_k \cap M_\ell \cong G/M_\ell$.

Similarly, we have that $M_\ell/N_k \cap M_\ell \cong G/N_k$.

Exercise 6.6. "Fill in the details" of the complicated induction argument illustrated above, to show that all of the composition factors are permuted.

Remark 6.7. In a way, the above argument is "*telling us something about the integers in general*" if we look at this induction argument in a "larger context".

For abelian groups, this type of induction argument works out fairly simply. Recall that if G is abelian and simple, then $G \cong \mathbb{Z}_p$ for some prime p.

Claim 6.8. For abelian groups, the composition series is such that the difference between each term is given by a prime order. In this case, the composition series must have factors which are of prime order.

Proof. If G is abelian, take any element x in G, and let $\mathrm{order}(x) = n$. If n is not prime then $x^{n/p}$ is an element of order $p = \mathrm{order}(x^{n/p})$. So there is a subgroup of G of order p. Consider the composition series of $G/\langle x^{n/p} \rangle$. By the fourth isomorphism theorem, there is a composition series of $G/\langle x^{n/p} \rangle$, and as a consequence, there exists a composition series of G whose "last step" is $\langle x^{n/p} \rangle$. $\square$

Exercise 6.9. "Fill in the details" of the above proof.

Question 6.10. What does the fundamental theorem of finitely-generated abelian groups tell us about the composition series for finitely-generated abelian groups?

Exercise 6.11. There are 5 groups of order $8 = 2^3$. Find all the possible composition series.

Remark 6.12. The above exercise really gives you a good idea as to how to "exhaust all possibilities" in terms of finding abelian subgroups.

Recall that **Hölder's program** may be regarded as being based on exact sequences of the following form.

$$\{1\} \longrightarrow A \xrightarrow{\alpha} G \xrightarrow{\beta} B \longrightarrow \{1\}. \tag{6.1}$$

With respect to the above exact sequence, observe that $B \cong G/A$ implies $|G| = |A||B|$.

Now let G be a group of order 8, letting G be as given in (6.1).

What are the possible choices for A and B with respect to the exact sequence given in (6.1)? It should be fairly clear that the possible groups for A and B are: $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, and $\mathbb{Z}_4$.

Informally, the "second part" of Hölder's program is related to the following question: How can the terms in the series given in (6.1) "combine" to form a new group? This question leads us to the important concept of *semidirect products of groups*.

6.2 The semidirect product

Exercise 6.13. Let A and B be groups, and for $b \in B$, let ϕ_b be an automorphism of A. Define $A \rtimes_\phi B$ as the set

$$\{(a, b) : a \in A, b \in B\}$$

endowed with the binary operation $\circ_{A \rtimes_\phi B}$ on $A \rtimes_\phi B$ whereby

$$(a, b) \circ_{A \rtimes_\phi B} (a', b') = (a\phi_b(a'), b(b'))$$

for $a, a' \in A$ and $b, b' \in B$. Show that $A \rtimes B$ forms a group, and show that $A \rtimes_\phi B = A \times B$ if $\phi_b(a) = a$ for all $b \in B$, i.e. ϕ_b is the identity automorphism on A for all $b \in B$.

Exercise 6.14. Construct morphisms α and β such that the sequence

$$\{1\} \longrightarrow A \xrightarrow{\alpha} A \rtimes_\phi B \xrightarrow{\beta} B \longrightarrow \{1\}.$$

is an exact sequence.

6.2.1 Dihedral groups as semidirect products

To illustrate the concept of semidirect products of groups, we offer a proof of the elegant formula

$$D_n \cong \mathbb{Z}_n \rtimes_\gamma \mathbb{Z}_2,$$

writing $\mathbb{Z}_2 = \mathbb{Z}_2^+ = (\{0, 1\}, +_2)$, and letting γ be given as follows, for $i \in \{0, 1, \ldots, n-1\} = \mathbb{Z}_n^+$:

$$\gamma_0(i) = i$$
$$\gamma_1(i) = n - i.$$

It is convenient to use a different kind of notation with respect to the automorphisms γ_0 and γ_1. Let the dihedral group D_n be denoted as

$$D_n = \left\{1, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}\right\},$$

and let C_n denote the cyclic subgroup

$$C_n = \{1, a, \dots, a^{n-1}\}$$

for $n > 2$. Similarly, let C_2 denote the set $\{1, b\}$ under composition, which forms a cyclic subgroup isomorphic to $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$.

Recall that $a^n = 1$ and $b^2 = 1$.

The semidirect product $C_n \rtimes_\gamma C_2$ is the set

$$C_n \rtimes_\gamma C_2 = \left\{\left(a^i, b^j\right) : 0 \leq i \leq n-1, 0 \leq j \leq 1\right\}$$

and letting $\gamma_1(a) = a$ and $\gamma_b(a) = a^{-1}$, we thus have that the underlying binary operation

$$\circ_{C_n \rtimes_\gamma C_2} = \circ$$

on the semidirect product $C_n \rtimes_\gamma C_2$ is given as follows.

$$\begin{aligned}
\left(a^i, 1\right) \circ \left(a^{i'}, b^j\right) &= \left(a^{i+i'}, b^j\right) \\
\left(a^i, b\right) \circ \left(a^{i'}, b^j\right) &= \left(a^i \gamma_b\left(a^{i'}\right), b(b^j)\right) = \left(a^{i-i'}, b(b^j)\right).
\end{aligned}$$

Now recall that the dihedral group D_n may be defined as the set

$$D_n = \left\{a^i b^j : 0 \leq i \leq n-1, 0 \leq j \leq 1\right\}$$

endowed with a binary operation $\circ_{D_n}$ whereby:

$$\begin{aligned}
a^i \circ_{D_n} a^{i'} \circ_{D_n} b^j &= a^{i+i'} b^j, \\
a^i b \circ_{D_n} a^{i'} b^j &= a^{i+i'} b(b^j).
\end{aligned}$$

So, the semidirect product shows you where the dihedral group "comes from" in a sense. The following dihedral relations may be interpreted in a natural way using the semidirect product:

$$\begin{aligned}
ba &= a^{n-1} b = a^{-1} b, \\
ba^i &= a^{n-i} b = a^{-i} b, \\
a^n &= 1.
\end{aligned}$$

There are many other examples of the process of "constructing larger groups from smaller groups".

Question 6.15. To what extent does the semidirect product construct depend on one's choice of automorphisms?

In answer to the above question, this construct really depends on the structure of the automorphism group $\mathrm{Aut}(A)$ of A. Recall that if we let each automorphism defining a semidirect product be equal to the identity automorphism, then this semidirect product is actually the direct product. However, different morphisms from B to $\mathrm{Aut}(A)$ generally result in different kinds of semidirect products.

6.3 Groups of prime power order

Let G be a (finite) group, and let S be a subset of the underlying set of G.

For $g \in G$, write $g.S = gSg^{-1} = \{gsg^{-1} : s \in S\}$.

What are the orbits of G when it acts on itself with this action?

This particular group action is especially useful.

The orbits with respect to this action are referred to as the **conjugacy classes** of G.

Now, recall that by Burnside's lemma, we have that:

$$\begin{aligned} \# \text{ of orbits} &= \frac{1}{|G|} \sum_{g \in G} |\mathrm{Stab}_G(\{g\})| \\ &= \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_g(G)| \,. \end{aligned}$$

Intuitively, Burnside's lemma is useful because if the set you're acting on is large, you can "reduce" the computation of the number of orbits using Burnside's lemma:

$$\mathrm{Stab}_G(\{g\}) = \mathrm{Fix}_g(G) = C_G(\{g\}) = N_G(\{g\}).$$

Now, for $x \in G$, let $c(x)$ denote the following set.

$$\begin{aligned} c(x) &= \text{the set of all elements in } G \text{ which are conjugate to } x \\ &= \text{the set of all expressions of the form } gxg^{-1} \text{ for some } g \in G \\ &= \left\{gxg^{-1}\right\}_{g \in G}. \end{aligned}$$

Now observe that G may be written as a disjoint union of orbits, i.e. a disjoint union of conjugacy classes, with

$$G = c(x_1) \uplus c(x_2) \uplus \cdots \uplus c(x_n)$$

and $|c(x_i)| = 1$ iff $x_i \in Z(G)$.

We thus obtain the following formulas:

$$\begin{aligned} |G| &= \sum_{i=1}^{n} |c(x_i)| \\ &= \sum_{\substack{i=1 \\ |c(x_i)|=1}}^{n} |c(x_i)| + \sum_{\substack{i=1 \\ |c(x_i)|>1}}^{n} |c(x_i)| \\ &= |Z(G)| + \sum_{\substack{i=1 \\ |c(x_i)|>1}}^{n} \frac{|G|}{|C_G(\{g\})|}. \end{aligned}$$

As a corollary, we have that if $|G| = p^n$ for some $n \geq 1$, then $|Z(G)| \neq 1$. This is because if

$$p \big| |G|$$

and

$$p \Big| \frac{|G|}{|C_G(\{g\})|}$$

then $p \Big| |Z(G)|$.

Therefore, if $N \triangleleft G$, then $|N \cap Z(G)| \neq 1$.