MATH 6121 lecture notes

Transcribed and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

9 October 04 lecture

9.1 Sylow Theory

Let G be a group such that $|G| = p^n m$, where p is prime and $\gcd(p, m) = 1$. Let $\mathrm{Syl}_p(G)$ denote the set of all Sylow p-subgroups, and write $n_p = |\mathrm{Syl}_p(G)|$.

First Sylow Theorem: Sylow p-subgroups always exist, i.e., $n_p \geq 1$.

Second Sylow Theorem: Sylow p-subgroups are all conjugate.

Third Sylow Theorem: n_p divides the order of G, and $n_p = kp + 1$ for some k, so $n_p \equiv 1 (\mathrm{mod}\ p)$.

Write in the details of the proofs of the above theorems given in the handout[1].

What are some consequences of Sylow's theorems? What are the main ideas behind the proofs of Sylow's theorems?

There are many different kinds of proofs of Sylow's theorems.

The orbit-stabilizer theorem may be used to prove Sylow's theorems. If G is a p-group and E is a G-set, we may break E into orbits modulo p as follows:

$$|E| \equiv |\mathrm{Fix}_G(E)| (\mathrm{mod}\ p).$$

Using the above congruence, it can be shown that

$$\binom{p^n m}{p^n} \equiv m (\mathrm{mod}\ p)$$

if p is a prime and m is an integer such that p does not divide m. This is explained in the given handout.

To prove Sylow's theorems, we can basically use the "same trick applied four different times", i.e., using the congruence $|E| \equiv |\mathrm{Fix}_G(E)| (\mathrm{mod}\ p)$, as indicated in the following table.

	Group	Set	Action
Sylow Thm. #1	G	$E =$ sets of cardinality p^n	Left multiplication
Sylow Thm. #2	S (a Sylow p-subgroup)	G/S	Left multiplication
Sylow Thm. #3 (pt. 1)	G	$\mathrm{Syl}_p(G)$	Conjugation
Sylow Thm. #3 (pt. 2)	S (a Sylow p-subgroup)	$\mathrm{Syl}_p(G)$	Conjugation

Question 9.1. Given a group G such that $|G| = 24$, is there a normal subgroup of index 3, i.e., of order 8?

[1] See http://garsia.math.yorku.ca/~zabrocki/math6121f16/documents/100616sylows.pdf.

Our strategy for answering the above question is based upon elementary Sylow theory.

Observe that $24 = 2^3 \cdot 3$.

The positive divisors of $24 = 2^3 \cdot 3$ are the natural numbers in the following set: $\{1, 2, 3, 4, 6, 8, 12, 24\}$.

How many Sylow 2-subgroups are there?

Let n_2 denote the number of Sylow 2-subgroups.

We know that $n_2 \equiv 1(\text{mod}2)$.

We also know that $n_2 \in \{1, 2, 3, 4, 6, 8, 12, 24\}$.

We may thus deduce that $n_2 \in \{1, 3\}$.

Observe that if $n_2 = 1$, then the corresponding group must be normal, since it could not have any distinct conjugates.

Is it true that there is no element of order 8 in S_4? Perhaps this may be shown using a combinatorial argument involving cycle notation for permutations.

Consider the classification of groups of order 8. Up to isomorphism, there are a total of 5 groups of order 8[2]:

(i) The cyclic group $\mathbb{Z}/8\mathbb{Z}$;

(ii) The group $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$;

(iii) The group $(\mathbb{Z}/2\mathbb{Z})^3$. Using the Fundamental Theorem of Finitely-Generated Abelian Groups, it is easily seen that there are only 3 abelian groups of order 8, up to isomorphism.

(iv) The dihedral group D_8. Recall that $D_8 \cong (\mathbb{Z}/4\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$;

(v) The **quaternion group** Q_8. We have not previously defined this group in class. This group may be defined using the following **presentation**:

$$\langle i, j, k | i^2 = j^2 = k^2 = ijk \rangle .$$

We also have not defined a presentation[3] of a group in class, but the above definition may be self-explanatory.

Remark 9.2. Sylow theory may be used to identify simple groups. Hölder's program basically tells to where to look for simple groups. Intuitively, Hölder's program tells us to "*look for places where simple groups could exist*". Sylow theory may be regarded as a tool for looking for where simple groups can exist, or better yet, where they don't exist.

As we previously discussed in class, there are 18 infinite families of simple groups, as well as 26 "random" ones[4].

[2] See https://en.wikipedia.org/wiki/List_of_small_groups.

[3] See http://groupprops.subwiki.org/wiki/Presentation_of_a_group.

[4] See https://en.wikipedia.org/wiki/List_of_finite_simple_groups.

Remark 9.3. During the 1990s, a large variety of results in "scattered" mathematical literature essentially "*filled all the holes in the major program for finding simple groups*". This has been a *very major* result in the history of mathematics.

Example 9.4. Let G be a group such that $|G| = p \cdot q$, where p and q are primes, with $p > q$. We know that n_p must divide the order $|G|$ of G. We thus find that $n_p \in \{1, p, q, pq\}$. We also know that $n_p \equiv 1 (\text{mod } p)$. So, we have that $n_p \neq p$. What else can we conclude?

Let G be a group such that $|G| = 2013 = 3 \cdot 11 \cdot 61$.

Could G be simple?

The divisors of the order of G are precisely the elements in the following set: $\{1, 3, 11, 61, 33, 183, 671, 2013\}$.

We have that $n_3 \in \{1, 61\}$, $n_{11} \in \{1\}$, and $n_{61} \in \{1\}$.

So G is definitely not simple, since there exists a normal subgroup $H_{11} \trianglelefteq G$, where H_{11} is the Sylow subgroup of order 11.

Can we find a composition series? Is it solvable? Observe that H_{11} cannot have nontrivial proper subgroups, since it must be of the form $\mathbb{Z}/p\mathbb{Z}$.

Using the Jordan-Hölder theorem, we begin by considering the sequence $H_{11}/H_{11} \trianglelefteq G/H_{11}$.

What can we say about G/H_{11}? It will be a group of order $183 = 3 \cdot 61$. The divisors are: divisors$(183) = \{1, 3, 61, 183\}$.

We thus observe that G/H_{11} has a normal Sylow 61-subgroup.

So we obtain a series of the following form: $\overline{H}_{61}/H_{11} \trianglelefteq G/H_{11}$.

By the Fourth Isomorphism Theorem, there exists a normal subgroup of G of order 671, H'. We thus obtain a subnormal series of the following form:

$$\{1\} \triangleleft H_{11} \triangleleft H' \triangleleft G.$$

Is this a composition series? Can we go further?

What is G/H'? This is a group of order 3.

Now observe that H'/H_{11} must be of order 61. Could there be a nontrivial proper subgroup? No, because $H'/H_{11} \cong \mathbb{Z}/61\mathbb{Z}$.

Now consider the quotient group $H_{11}/\{1\}$. Does there exists a nontrivial proper subgroup of this group? No, because it is isomorphic to $\mathbb{Z}/11\mathbb{Z}$.

We may thus deduce that if $|G| = 2013$, then G is solvable, i.e., each quotient is abelian.

9.2 Illustrating composition factors with Cayley tables

In class, we discussed a colored Cayley table for the symmetric group S_4 which was organized in order for one to visualize the composition factors. A URL for a website containing this Cayley table is given below:

http://lacim.uqam.ca/ saliola/maths/teaching/MAT2250-2014A/documents/tables-classes-modulo-sous-groupe.pdf

Is this Cayley table for S_4 abelian? No, because it is not symmetric along the main diagonal.

Question 9.5. What else can we learn by looking at this Cayley table?

First of all, this Cayley table makes it clear that there exists a subgroup of index 2 which is normal.

That is, this Cayley table is colored in such a way that it is apparent that there exists a subgroup $H \trianglelefteq G$ of order 12. The use of colors emphasizes that this subgroup is actually a normal subgroup of index 2. The use of colors also suggests that we may collapse elements in the cosets of $H \trianglelefteq G$ and thereby collapse collections of colors in the corresponding Cayley table to produce a composition table of the following form:

$\circ$	H	gH
H	H	gH
gH	gH	H

So, let H_1 denote a subgroup of $G = S_4$ of order 12. Consider a subnormal series of the following form:

$$H_2 \trianglelefteq H_1 \trianglelefteq G.$$

Now suppose that $H_2 \trianglelefteq H_1$ is of order 4, with $H_1/H_2 \cong \mathbb{Z}/3\mathbb{Z}$. Use the Cayley table given in the above website to visualize this subgroup.

Furthermore, suppose that $H_3 \trianglelefteq H_2$ where H_3 is a subgroup of order 2. We thus arrive at the following subnormal series:

$$\{1\} \trianglelefteq H_3 \trianglelefteq H_2 \trianglelefteq H_1 \trianglelefteq G.$$

Recall that a **subnormal series** of a group G is a sequence of the form

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G.$$

Also recall that a subnormal series

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G.$$

of a group G is a **composition series** if each factor group of the form H_{i+1}/H_i is simple, and that a group G is said to be **solvable** if it has a composition series

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G.$$

such that all factor groups of the form H_{i+1}/H_i are abelian. Returning to the subnormal series

$$\{1\} \trianglelefteq H_3 \trianglelefteq H_2 \trianglelefteq H_1 \trianglelefteq G = S_4$$

given above, we have that:

$$|G/H_1| = 2$$
$$|H_1/H_2| = 3$$

$$\begin{aligned}|H_2/H_3| &= 2\\ |H_3/\{1\}| &= 2.\end{aligned}$$

Therefore,

$$\begin{aligned}&G/H_1 \cong \mathbb{Z}/2\mathbb{Z}\\ &H_1/H_2 \cong \mathbb{Z}/3\mathbb{Z}\\ &H_2/H_3 \cong \mathbb{Z}/2\mathbb{Z}\\ &H_3/\{1\} \cong H_3 \cong \mathbb{Z}/2\mathbb{Z}.\end{aligned}$$

We thus find that the symmetric group S_4 is solvable, because it has a composition series

$$\{1\} \trianglelefteq H_3 \trianglelefteq H_2 \trianglelefteq H_1 \trianglelefteq G = S_4$$

such that all of the factor groups for this subnormal series are abelian.

Exercise 9.6. Is it possible to rearrange the multiplication table so that the composition factors are of the form $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3)$ or of the form $(\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2)$?

9.3 Introduction to representation theory

Recall that there is a correspondence between actions of a group G on a set X and homomorphisms to the symmetric group on X:

$$G \text{ is a group acting on a set } X \iff \text{homomorphism to symmetric group on } X$$

We thus have that there is a correspondence between subgroups of S_X and G-sets X.

Remark 9.7. Informally, we want to "*lift this idea, so that we're not just acting on a set X, but we're acting on a vector space V.*"

To describe a group G acting on a vector space V, we consider morphisms of the form

$$\phi\colon G \to \mathrm{Aut}_{\mathbb{C}}(V)$$

such that $\phi(g)$ is a linear transformation, and

$$\phi(g)\phi(g') = \phi(g \cdot g'),$$

and

$$\phi(e) = \mathrm{id} \in \mathrm{Aut}_{\mathbb{C}}(V),$$

letting id denote the identity transformation in V.

In this case, V is referred to as a G-module (instead of a G-set).

Fix a basis $\mathcal{B}$ of V. Then every one of these linear transformations $\phi(g)$ corresponds to a matrix, as suggested through the following **commutative diagram**[5].

[5] See `https://en.wikipedia.org/wiki/Commutative_diagram`.

$$\begin{tikzcd}
G \arrow[r] \arrow[dr, "A_{\mathcal{B}}"'] & \mathrm{Aut}_{\mathbb{C}}(V) \arrow[d, "\mathcal{B} \text{ basis}"] \\
 & \mathrm{GL}_n(\mathbb{C}) \subseteq \mathrm{Mat}_{n \times n}(\mathbb{C})
\end{tikzcd}$$

$A_{\mathcal{B}}(g)$ is a matrix with the property that:

$$A_{\mathcal{B}}(g) \circ [\vec{V}]_{\mathcal{B}} = [\phi(g)(\vec{v})]_{\mathcal{B}}.$$

Write $\mathcal{B} = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$. We thus have that $A_{\mathcal{B}}(g)$ may be written in terms of column vectors as follows:

$$A_{\mathcal{B}}(g) = [[\phi(g)(\vec{b}_1)]_{\mathcal{B}}, [\phi(g)(\vec{b}_2)]_{\mathcal{B}}, \ldots, [\phi(g)(\vec{b}_n)]_{\mathcal{B}}].$$

For example, let G denote the multiplicative group such that the underlying set of G is $\{e, a, a^2\}$.

Now, let V denote the linear span over $\mathbb{C}$ of the underlying set of G: $\mathscr{L}_{\mathbb{C}}\{e, a, a^2\}$.

Write $\mathcal{B} = \{e, a, a^2\}$. Define $\phi(a) \in \mathrm{Aut}_{\mathbb{C}}(V)$ as follows:

$$\begin{aligned}
\phi(a)(e) &= a \\
\phi(a)(a) &= a^2 \\
\phi(a)(a^2) &= e.
\end{aligned}$$

Now compute $[\phi(a)(e)]_{\mathcal{B}}$, $[\phi(a)(a)]_{\mathcal{B}}$, and $[\phi(a)(a^2)]_{\mathcal{B}}$:

$$[\phi(a)(e)]_{\mathcal{B}} = [a]_{\mathcal{B}} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$$[\phi(a)(a)]_{\mathcal{B}} = [a^2]_{\mathcal{B}} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$[\phi(a)(a^2)]_{\mathcal{B}} = [e]_{\mathcal{B}} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Now compute the matrix $A_{\mathcal{B}}(a)$ as follows:

$$A_{\mathcal{B}}(a) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

For example, we have that

$$\phi(a)(4e + 3a - a^2) = 4a + 3a^2 - e.$$

Now take the vector corresponding to this, with respect to the basis $\mathcal{B}$:

$$\begin{bmatrix} -1 \\ 4 \\ 3 \end{bmatrix}.$$

Now observe that:

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \\ -1 \end{bmatrix} = \begin{bmatrix} -1 \\ 4 \\ 3 \end{bmatrix}.$$

This illustrates how to “turn a group into a matrix group”. Just as there is a correspondence between subgroups of the symmetric group and orbits, there is a correspondence between representations and subgroups of general linear groups.

Exercise 9.8. Do all of the exercises given in the given handout, which is available on the course webpage. The total number of pages for your solutions to this handout should be at least 5 pages.

Example of a midterm problem: analyze groups of a given order using Sylow theory.