MATH 6121 lecture notes

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

5 September 22 lecture

5.1 Quotient groups and normal subgroups

The idea of a *quotient structure* comes up over and over again in different areas of algebra.

With respect to vector spaces, we can construct *quotient spaces*.

We can define quotient structures with respect to rings, modules, etc.

Exercise 5.1. If N is normal in G, then $\forall g \in G \; \exists g' \in G \; gN = Ng'$.

Claim 5.2. Letting $N \leq G$, we have that: $N \trianglelefteq G$ iff $\forall g \in G \; gN = Ng$.

Remark 5.3. Normal subgroups are commonly defined as subgroups which satisfy the property given in the above claim.

Proposition 5.4. *A (nonempty) subset S of a group G is a subgroup if $x^{-1}y \in S$ for all $x, y \in S$.*

Proof. Suppose that S is such that $x^{-1}y \in S$ for all $x, y \in S$. If we choose $x = y$, then $x^{-1}y = x^{-1}x = e = e_G \in S$, so S constains the identity element $e = e_G$ of G. If we choose $y = e$, then we have that $\forall x \in S \; x^{-1}e = x^{-1} \in S$. Letting $a, b \in S$ be arbitrary, letting $x = a^{-1}$ and $y = b$, since $x^{-1}y \in S$, we have that $(a^{-1})^{-1}b \in S$, and thus $ab \in S$, thus proving that S is closed with respect to the underlying binary operation of G. □

Remark 5.5. The property concerning subgroups given in the above proposition is sometimes referred to as the **One-Step Subgroup Test**[1].

Definition 5.6. Let $A \subseteq G$. We define the **centralizer** of A in G as the set

$$C_G(A) = \left\{ g \in G \;\middle|\; gag^{-1} = a \text{ for all } a \in A \right\},$$

[1] See Joseph A. Gallian's *Contemporary Abstract Algebra*.

and the set

$$N_G(A) = \{g \in G \mid gA = Ag\}$$

is referred to as the **normalizer** of A in G.

Warning: The term *normalizer* was defined differently in class as "$N_G(A) = \{g \in G \mid gag^{-1} \in A \text{ for all } a \in A\}$". It is appears that this definition is incorrect. Consider the following exercise to show that this definition is not even a group if G is not finite.

Exercise 5.7. Let $M_G(A) = \{g \in G \mid gag^{-1} \in A \text{ for all } a \in A\}$, then show that $M_G(A)$ is not a group in general. Hint: Take G to be the group of permutations of the set of integers and show that for $A = \{\sigma \in G : \sigma(i) = i, \text{ for } i < 0\}$ that $g(x) = x + 1 \in M_G(A)$, but $g^{-1}(x) = x - 1 \notin M_G(A)$.

Exercise 5.8. Show that if G is finite then $N_G(A) = M_G(A)$. Where does the proof fail if G is infinite?

Exercise 5.9. Show that $C_G(A) \leq N_G(A) \leq G$.

Remark 5.10. In fact, it is necessarily true that $C_G(A) \trianglelefteq N_G(A)$[2].

Definition 5.11. The set $C_G(G)$ is denoted as $Z(G)$ and is called the **center** of the group G.

Perfect example of a project: write a program that returns the center of a group, and which shows that the center of a group forms a subgroup.

5.2 Group isomorphism theorems

The First Isomorphism Theorem: Let H and G be groups. The for a morphsim $\phi\colon G \to H$, we have that $\ker(\phi) \trianglelefteq G$, and furthermore, we have that $G/\ker(\phi) \cong \text{im}(\phi)$.

The Second Isomorphism Theorem: Let G be a group, and let $H, K \leq G$ be such that $H \leq N_G(K)$, $H \cap K \trianglelefteq H$, and $HK/K \cong H/(H \cap K)$.

You are not expected to memorize the Second Isomorphism Theorem.

The Third Isomorphism Theorem: Let G be a group and let $H, K \trianglelefteq G$, with $H \trianglelefteq K$. Then K/H is normal in G/H, and furthermore, we have that $(G/H)/(K/H) \cong G/K$.

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

Proof exercise #1: Write $\psi\colon G/\ker(\phi) \to \mathrm{im}(\phi)$, so that

$$g\ker(\phi) \mapsto \phi(g)$$

for an arbitrary coset $g\ker(\phi)$ in the domain of ψ. Show that ψ is well-defined and bijective.

Proof exericse #2: Define $\tau\colon H \to HK/K$ so that

$$h \mapsto hK$$

for all $h \in H$. Show that τ is a group homomorphism, and that $\ker(\tau) = H \cap K$. You may also need to check that τ is surjective.

Proof exercise #3: Define $\gamma\colon G/H \to G/K$, so that

$$gH \mapsto gK$$

for each coset gH in the domain of γ. Show that γ is a well-defined group homomorphism, and show that $\ker(\gamma) = K/H$. You may also need to check that γ is surjective.

Let G denote the dihedral group D_4, and let D_4 be denoted as follows:

$$D_4 = \left\{1, a, a^2, a^3, b, ba, ba^2, ba^3\right\}.$$

Now let K and H denote the following cyclic subgroups of G:

$$K = \left\{1, a, a^2, a^3\right\} \cong C_4$$
$$H = \left\{1, a^2\right\} \cong C_2.$$

It is easily seen that $H \trianglelefteq K \trianglelefteq G$. Now, compute the quotient groups G/H and G/K:

$$G/H = \left\{\left\{1, a^2\right\}, \left\{a, a^3\right\}, \left\{b, ba^2\right\}, \left\{ba, ba^3\right\}\right\}$$
$$G/K = \left\{\left\{1, a, a^2, a^3\right\}, \left\{b, ba, ba^2, ba^3\right\}\right\}.$$

Now, let $\gamma\colon G/H \to G/K$ be as given above. Compute the expressions $\gamma(\{1, a^2\})$ and $\gamma(\{b, ba^2\})$ as indicated below.

$$\gamma(\{1, a^2\}) = \gamma(\{a, a^3\}) = \{1, a, a^2, a^3\},$$

$$\gamma(\{b, ba^2\}) = \gamma(\{ba, ba^3\}) = \{b, ba, ba^2, ba^3\}.$$

Now compute the kernel of γ:

$$\ker(\gamma) = \left\{\left\{1, a^2\right\}, \left\{a, a^3\right\}\right\} = K/H.$$

Now, by the third isomorphism theorem, we have that $(G/H)/(K/H)$ is isomorphic to G/K. This is illustrated below.

$$\begin{aligned}
&\left\{\left\{\left\{1, a^2\right\}, \left\{a, a^3\right\}\right\}, \left\{\left\{b, ba^2\right\}, \left\{ba, ba^3\right\}\right\}\right\} \\
&= (G/H)/(K/H) \\
&\cong G/K \\
&= \left\{\left\{1, a, a^2, a^3\right\}, \left\{b, ba, ba^2, ba^3\right\}\right\}.
\end{aligned}$$

The Fourth Isomorphism Theorem: Let G be a group and let $H \trianglelefteq G$. Then the canonical projection morphism $\pi\colon G \to G/H$ whereby

$$g \mapsto gH$$

"induces" the bijections indicated below:

$$\begin{aligned}
\{H \trianglelefteq K \leq G\} &\longleftrightarrow \left\{\overline{K} \leq G/H\right\} \\
\{H \trianglelefteq K \trianglelefteq H\} &\longleftrightarrow \left\{\overline{K} \trianglelefteq G/H\right\}.
\end{aligned}$$

Proof exercise #4: Show that the mappings indicated below are bijective.

$$\begin{aligned}
K &\mapsto \{kH : k \in K\} = \overline{K} \\
\left\{g \in G \;\middle|\; \pi(g) \in K\right\} &\hookleftarrow \overline{K} \leq G/H.
\end{aligned}$$

Remark 5.12. Intuitively, normal subgroups are important for "*pulling out the structure*" of larger groups. This is a very useful way of intuitively thinking about normal subgroups.

5.3 Hölder's program

Question 5.13. Given a certain class of rings or algebras, how can we list or classify them all?

Remark 5.14. Intuitively, there is something very difficult to understand about the classification of finite groups.

Remark 5.15. The classification of finite groups is relevant to many other fields in algebra.

Hölder proposed a way of classifying finite groups.

STEP 1: Classify all of the groups that do not have a normal subgroup, except for the trivial subgroup and the corresponding group itself. These groups are referred to as **simple groups**.

STEP 2: What are all the ways you can "put together" simple groups to make the rest?

Definition 5.16. Let A, B, and C be groups, and let f_1 and f_2 be group homomorphisms as given in the sequence

$$A \xrightarrow{f_1} B \xrightarrow{f_2} C.$$

Then this sequence is said to be an **exact sequence** if $\text{im}(f_1) = \ker(f_2)$. This definition may be generalized inductively.

Remark 5.17. Observe that if $B \xrightarrow{\alpha} C \to \{1\}$ is exact, then it necessarily follows that $\text{im}(\alpha) = C$, so α must be onto (surjective) as a result.

Remark 5.18. Observe that if $\{1\} \to A \xrightarrow{\alpha} B$ is exact, then letting id denote the mapping from $\{1\}$ to A which maps 1 to the identity element in A, we have that $\text{im}(\text{id}) = \{1_A\} = \ker(\alpha)$, so it necessarily follows that α is one-to-one (injective). Recall that a group homomorphism is injective if and only if its kernel is trivial.

Now, suppose that the following sequence is exact, where the "cloud" symbol denotes an unknown group. What can "go between" the mappings α and β illustrated below?

$$\{1\} \longrightarrow A \xrightarrow{\alpha} \quad \xrightarrow{\beta} B \longrightarrow \{1\}$$

Since the above sequence is exact by assumption, from the definition of the term *exact sequence* given in Definition 5.16, we have that:

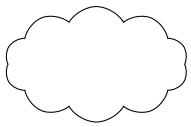
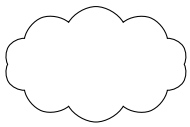
(i) $\{1\} = \ker(\alpha)$;

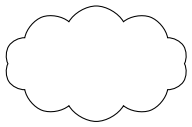
(ii) $\mathrm{im}(\alpha) = \ker(\beta)$; and

(iii) $\mathrm{im}(\beta) = B$.

Observe that α is injective and β is surjective.

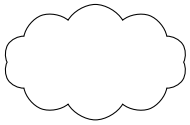
Now, using the first isomorphism theorem, we thus obtain the following sequence of group isomorphisms.

$\mathrm{im}(\beta) = B \cong$  $/\ \ker(\beta) \cong$  $/\ \mathrm{im}(\alpha) \cong$

 $/\ A$

Note that $\mathrm{im}(\alpha) \cong A$, since:

$$\mathrm{im}(\alpha) \cong A/\ker(\alpha) = A/\left\{1_A\right\} \cong A.$$

Now, observe that if  is a simple group, then A is either the trivial subgroup or the entire group itself.

Recall that "**STEP 1**" in the above formulation of Hölder's program concerns the classification of finite simple groups.

STEP 1 SOLUTION: There are a total of 18 infinite families of simple groups, and there are a total of 26 simple groups that don't "fit in" these infinite families.

5.3.1 Infinite families of simple groups

Observe that $\mathbb{Z}/p\mathbb{Z}$ is simple for each prime number p, where:

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \left\{\ldots, -2, -1, 0, 1, 2, \ldots\right\} / \left\{\ldots, -2p, -p, 0, p, 2p, \ldots\right\}.$$

By Lagrange's theorem, it is clear that $\mathbb{Z}/p\mathbb{Z}$ is a simple group for a prime p: given a subgroup $H \leq \mathbb{Z}/p\mathbb{Z}$, then the order $|H|$ of the subgroup H must

divide the order of $\mathbb{Z}/p\mathbb{Z}$, but since the order of $\mathbb{Z}/p\mathbb{Z}$ is equal to the prime p, the order of H is either 1 or p, so H is either the trivial subgroup, or $H = \mathbb{Z}/p\mathbb{Z}$.

Remark 5.19. Arguably, one should avoid using the notation "$\mathbb{Z}_p$" to denote the structure $\mathbb{Z}/p\mathbb{Z}$, because the symbol $\mathbb{Z}_p$ is commonly used to denote the ring of p-adic integers[3].

Definition 5.20. The **alternating group** A_n is the group consisting of all even permutations in S_n. Equivalently, this group may be defined as the group of $n \times n$ permutation matrices of determinant 1.

Recall that a **permutation matrix** is a square binary matrix with has exactly one entry equal to 1 in each row and each column. For example, the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

is a permutation matrix. Since the $(1, 2)$-entry of this matrix is equal to 1, the above permutation matrix corresponds to a permutation $\sigma \in S_4$ whereby $\sigma_1 = 2$. Similarly, we have that $\sigma_2 = 3$, since the $(2, 3)$-entry in the above matrix is equal to 1. Continuing in this manner, we have that the above matrix corresponds to the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

in the symmetric group S_4.

Observe that the determinant of a permutation matrix either 1 or -1. The mapping

$$\phi \colon S_n \to \{1, -1\} \cong C_2$$

whereby $\phi(\sigma) = \det(\sigma) = \operatorname{sign}(\sigma)$ for all $\sigma \in S_n$ is group homomorphism if we endow the codomain of ϕ with a multiplicative group structure, and $\ker(\phi) = A_n$. Observe that $A_n \trianglelefteq S_n$.

The following theorem is historically significant with respect to the history of group theory.

[3]See `https://en.wikipedia.org/wiki/P-adic_number`.

Theorem 5.21. *The alternating group A_n is simple for $n \geq 5$.*

There are more complicated examples of infinite families of finite simple groups, as suggested by the following result.

Claim 5.22. The quotient group $\mathrm{SL}_n(\mathbb{F})/Z(\mathrm{SL}_n(\mathbb{F}))$ is simple for each finite field $\mathbb{F}$, and each natural number $n \geq 4$.

A really good project idea: "get your hands on" $\mathrm{SL}_n(\mathbb{F})/Z(\mathrm{SL}_n(\mathbb{F}))$ for any finite field $\mathbb{F}$ using a computer algebra system.

The following result is easily verified using the **Fundamental Theorem of Finitely-generated Abelian Groups**, which we have not covered in class.

Claim 5.23. A finite abelian group is simple iff it is isomorphic to $\mathbb{Z}_p$ for some prime number p.

The Feit-Thompson Theorem (1963): A finite group of odd order is simple iff it is isomorphic to $\mathbb{Z}_p$.

Remark 5.24. Intuitively, trying to study finite groups is really a motivation for "*what group theory is all about.*"

Question 5.25. Given two groups A and B, how can we "combine" these groups to form a larger group? In other, how can we "create" larger groups from smaller groups?

Consider an exactly sequence of the form

$$\{1\} \longrightarrow A \longrightarrow A \times B \longrightarrow B \longrightarrow \{1\}$$

where

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

is endowed with a binary operation $\circ = \circ_{A \times B}$ whereby

$$(a, b) \circ_{A \times B} (a', b') = (aa', bb')$$

for $a, a' \in A$ and $b, b' \in B$.

The set $A \times B$ endowed with the binary operation $\circ_{A \times B}$ given above forms a group, which is referred to as the **direct product** of A and B.

With regard to **Question** 5.25, there are other constructions to "put" two groups together. The **semidirect product** is an example of a construction of this form.

Exercise 5.26. Recall that A_n is simple for $n \geq 5$. However, it is not true that A_4 is a simple group. Prove that A_4 is not a simple group using a counterexample, and write out all 12 elements in A_4.