Abstract Algebra Lecture Notes

Simon Xiang

Lecture notes for the Fall 2020 graduate section of Abstract Algebra (Math 380C) at UT Austin, taught by Dr. Ciperiani. I'm currently auditing this course due to the fact that I'm not officially enrolled in it. These notes were taken live in class (and so they may contain many errors). You can view the source code here: `https://git.simonxiang.xyz/math_notes/file/freshman_year/abstract_algebra/master_notes.tex.html`.

Contents

§1 September 23, 2020

Last time: we finished a corollary that a group is never a union of conjugates of a subgroup. It is essential that G is finite. For example, $\mathrm{GL}_n(\mathbb{C})$ is a union of conjugate subgroups[1].

§1.1 Group Automorphisms

Today we'll talk about automorphisms of a group. We'll notate this as

$$\mathrm{Aut}(G) = \text{ the group of automorphisms } G \to G,$$

the operation is clearly composition. We can think of this as a subgroup of S_G, but in general, we won't have equality here. For any normal subgroup $H \trianglelefteq G$, we have a map $\varphi\colon G \to \mathrm{Aut}\, H$, where $g \mapsto (h \mapsto ghg^{-1})$. It's easy to see that φ is a group homomorphism.

Proposition 1.1. Let H be a subgroup of G. Then the normalizer of H in G quotient the centralizer of H in G, denoted $N_G(H)/C_G(H)$, is isomorphic to a subgroup of the automorphism group of H denoted $\mathrm{Aut}\, H$. In particular, $G/Z(G) \hookrightarrow \mathrm{Aut}\, G$. There won't be a proof for this, but just find a map from the normalizer to $\mathrm{Aut}\, H$, and look at the kernel of φ. Then it will follow from the FHT.

Definition 1.1. Let G be a group. The image of $G/Z(G)$ in $\mathrm{Aut}\, G$ is the group of inner automorphisms of G, denoted $\mathrm{Inn}(G)$. The inner automorphisms of G can be given by

$$\mathrm{Inn}\, G = \{[G \to G \mid g \mapsto g_0 g_0^{-1}] \mid g_0 \in G\}.$$

Here's something that make sense when you think about it: a group G is abelian iff $\mathrm{Inn}\, G = \{\mathrm{id}_G\}$. So inner automorphisms tell you nothing about an abelian group.

Example 1.1. What is $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$? $\mathbb{Z}/n\mathbb{Z}$ is abelian which implies $\mathrm{Inn}(\mathbb{Z}/n\mathbb{Z}) = \{\mathrm{id}\}$. Let $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be an isomorphism. The thing about cyclic groups is that if we know where something sends a generator, then we are done. Let's say $n = 6$ and $1 \mapsto 2$: is this possible? Since these are automorphisms, we have to send generators to generators, so no. So $\varphi_a(\bar{k}) = \overline{ak}$. So φ_a is uniquely determined by $a = \varphi[1 + n\mathbb{Z}]$. φ_a is surjective implies that a is a generator of $\mathbb{Z}/n\mathbb{Z}$, which his equivalent to the fact that $a \in \mathbb{Z}$, $\gcd(a, n) = 1$[2]. Recall that $\mathbb{Z}/n\mathbb{Z}$ is a ring, so $a \in (\mathbb{Z}/n\mathbb{Z})^*$, the group of units. Hence

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*,$$

and $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) < \mathrm{Inn}(\mathbb{Z}/n\mathbb{Z}) = \{\mathrm{id}\}$.

§1.2 Inner automorphisms of S_n

Example 1.2. We have our other extreme: in the symmetric group on n letters (it's leaking!), we have

$$\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n$$

for all $n \neq 6$. Observe that $\mathrm{Inn}(S_n) < \mathrm{Aut}\, S_n$, and that $\mathrm{Inn}(S_n) \cong S_n/Z(S_n)$. What's the center of S_n? Since every element of S_n can be written as a product of disjoint cycles. If we understand what conjugation does to cycles, we understand what conjugation does to an element of S_n. Let $\sigma, \tau \in S_n$, where $\sigma\colon i \to \sigma(i)$[3]. Then $\tau\sigma\tau^{-1}\colon \tau(i) \to \tau\sigma(i) \to \tau(\sigma(i))$. So if $\sigma = (a_1, \cdots, a_{k_1})(b_1, \cdots, b_{k_1}) \cdots$ a product of disjoint cycles, then

$$\tau\sigma\tau^{-1} = \big(\tau(a_1)\tau(a_2) \cdots (\tau(a_{k_1})\big)\big(\tau(b_1)\tau(b_2) \cdots (\tau(b_{k_2})\big) \cdots$$

Lemma 1.1. *If $n > 2$, then $\mathbb{Z}(S_n) = \mathrm{id}$.*

Lemma 1.2. *For every $\sigma, \tau \in S_n$, σ and $\tau\sigma\tau^{-1}$ have the same[4] cycle composition into disjoint cycles.*

Proposition 1.2. Two elements of S_n are conjugate in S_n if and only if they have the same cycle decomposition.

Proof. ($\implies$) follows from our lemma.

($\impliedby$) Let $\sigma_1, \sigma_2 \in S_n$ with the same cycle decomposition. Write σ_1 and σ_2 are a product of disjoint cycles by ordering the cycles in increasing length including all 1-cycles. Let τ be the ith element of the cycle deomposition of σ_1, which must map to the ith element of the cycle decomposition of σ_2. Together, these give the fact that $\tau \in S_n$: all the elements appear (including 1-cycles) and no elements repeat because these are disjoint cycles. Notice that $\tau \in S_n$ and $\sigma_2 = \tau\sigma_1\tau^{-1}$, then this finishes the proof. ⊠

Corollary 1.1. *The number of conjugacy classes of S_n is equal to the number of partitions of n.*

[1] The subgroups are the upper triangular matrices.

[2] Finally, I understand when she tells me something is obvious that it is indeed, obvious.

[3] Very informal abuse of notation here, think of it intuitively.

[4] By "same", we mean they have the same length.

Eg, you can break up $n = 3$ as $n = 1 + 1 + 1, 1 + 2, 3$. So S_3 has three conjugacy classes. Observe that this proposition implies that $\operatorname{Aut} S_n = \operatorname{Inn} S_n$ iff every automorphism $\varphi\colon S_n \to S_n$ preserves the cycle decomposition, that is, $(\sigma, \varphi(\sigma))$ have the same cycle decomposition. We start with an automorphism, and we have to show that it sends a-cycles to a-cycles for $1 \leq a \leq n$, and then everything follows. So we start with 2-cycles, and that's when it breaks: a 2-cycle can go to a disjoint product of 3-cycles.

Apparently today we only covered half of what Dr. Ciperiani thought we would cover. Should we go faster?? Hmm...

§2 September 25, 2020

§2.1 Whoops

Whoops, I was working on some Dehn presentation homework problem for Algebraic Topology (due at 1:00), and couldn't make it to class today.

§3 September 28, 2020

§3.1 The alternating group

We have S_n generated by transpositions: this is because S_n is generated by cycles, which are generated by transpositions. Within $S_n = \langle \text{transpositions} \rangle$, we have $A_n = \langle \text{pairs of transpositions} \rangle$. For $\tau \in S_n$, elements of $\tau A_n \tau^{-1}$ still has an even number of transpositions. For example, say $\tau = (12)(14)(46)$, then $\tau^{-1} = (46)(14)(12)$. We know $\sigma \in A_n$ is a product of an even number of transpositions, say $2n$. Then $\tau\sigma\tau^{-1}$ is a product of $2m + 2 \cdot 3$ transpositions, which is even, so $\tau\sigma\tau^{-1} \in A_n$ for all $\sigma \in A_n$. Hence $\tau A_n \tau^{-1} \subseteq A_n$ for all $\tau \in S_n$, which implies that $A_n \trianglelefteq S_n$.

Observe that $(12)(13) = (12)(31) = (132)$. If two cycles are adjacent and have a number in common, then we can transform it into a 3-cycle as shown above. Also observe that $(12)(34) = (12)(23)(23)(34) = (123)(234)$[5]. So we can write any two adjacent cycles by a product of two or less 3-cycles. Hence A_n is generated by 3-cycles, and any even transposition can be written as a product of 3-cycles.

§3.2 A_n is simple for $n \geq 5$

Dr. Ciperiani just told some story that I lost, but it's in the book (Dummit and Foote).

Lemma 3.1. *Let $(abc), (ijk) \in A_n$ for $n \geq 5$. Then $\pi(abc)\pi^{-1} = (ijk)$ for some $\pi \in A_n$.*

Note that this would be no suprise if $\pi \in S_n$.

Proof. We know that there exists $\pi' \in S_n$ such that $(ijk) = \pi'(abc)\pi'^{-1}$. If $\pi' \in A_n$, then set $\pi = \pi'$ and we are done. If $\pi' \notin A_n$, we know there exists some (kd) that is a conjugate of (abc), that is, $k, d \neq a, b, c$, which we can do since $n \geq 5$.So

$$\pi'(kd)(abc)(kd)^{-1}\pi'^{-1} = \pi'(abc)\pi'^{-1} = (ijk).$$

Then set $\pi = \pi^{-1}(kd)$, together with the fact that $\pi' \notin A_n$ we have $\pi \in A_n$. ☒

Theorem 3.1. *A_n is simple in S_n for every $n \geq 5$.*

Proof. Say we have some nontrivial subgroup $N \trianglelefteq A_n$. We want to show $N = A_n$. If $N = A_n$, then of course N contains a 3-cycle. By our lemma, if N contains a 3-cycle, then $N = A_n$ (N is normal, conjugates). So $N = A_n \iff N$ contains a 3-cycle.

Let $\pi \in N \setminus \{\text{id}\}$ such that π fixes as many symbols as possible. We will choose an element of N that fixes more symbols than π, which is a contradiction. Suppose π is not a 3-cycle (if not, then $N = A_n$). Then

1. $\pi = (12)(34)\cdots$ (we get this by conjugation) – moves at least four symbols, starting with a product of two disjoint transpositions.

2. $\pi = (123\cdots)\cdots$ – moves two more symbols, say $4, 5$. π cannot equal (1234), since π is even and 4-cycles don't live in A_n.

Consider $\sigma = (345)$, $\pi' = \sigma^{-1}\pi^{-1}\sigma\pi \in N$, since $\pi \in N, \sigma \in A_n$ ($N \trianglelefteq A_n \trianglelefteq S_n$). Notice that $\pi(x) = x$ implies that $\pi'(x) = x$ for any $x > 5$. For π',

$$1 \overset{\pi}{\mapsto} 2 \overset{\sigma}{\mapsto} 2 \overset{\pi^{-1}}{\mapsto} 1 \overset{\sigma^{-1}}{\mapsto} 1,$$

which implies $\pi'(1) = 1$. So π' fixes more elements than π. Now we want to show that $\pi' \neq \text{id}$. Now $\pi'(2) = 2$, so this isn't very helpful. What's $\pi'(3)$? in case 1, $\pi' \colon 3 \mapsto 4 \mapsto 5$, and 5 either maps to 5 or some $k > 5$ (because the cycles are disjoint). If $5 \mapsto 5$, then $5 \overset{\sigma^{-1}}{\mapsto} 4$, and if $5 \mapsto k$, $k \overset{\sigma^{-1}}{\mapsto} k$ for some $k \geq 5$, which together imply $\pi'(3) > 3$. For case 2, $\pi' \colon 2 \overset{\pi}{\mapsto} 3 \overset{\sigma}{\mapsto} 4 \overset{\pi^{-1}}{\mapsto} ?$ Either $\pi = (12345)\cdots$, $(1234)(5\cdots)$, $(123)(45)\cdots$ $(123)(45\cdots)$. In the first two cases, $4 \overset{\pi^{-1}}{\mapsto} 3$, in the third case, $4 \overset{\pi^{-1}}{\mapsto} 5$, and in the fourth case, $4 \overset{\pi^{-1}}{\mapsto} k$ for $k > 5$. None of these are 2, so $\pi'(2) \neq 2$, which implies π' is not the identity. This is a contradiction, since the π' we constructed lives in N, is not the identity, and fixes more symbols than π. So π is a $3 - \mathit{cycle}$, which implies $N = A_n$ by the lemma. There A_n is simple in S_n for all $n \geq 5$. ☒

[5] I like how the thing we struggle the most with is manually calculating what cycles are.