Groups and Permutations

Raymond Feng

July 30, 2021

Outline

1. Groups and Permutations
    - Symmetric Group
    - Alternating Group
2. Subgroups
    - Lagrange's Theorem
    - Normal Subgroups
    - Simple Groups
3. Normal Subgroups of S_n and A_n
    - Conjugacy Classes
    - Normal Subgroups of S_n
    - Normal Subgroups of A_n
4. Acknowledgements

Definition of a Group

Definition

A group is a set G equipped with a binary operation $\cdot$ such that

- There is an identity element $1 \in G$ for which $1 \cdot g = g$ for all $g \in G$.
- Each $g \in G$ has an inverse $g^{-1} \in G$ such that $g \cdot g^{-1} = 1$.
- Multiplication is associative, meaning that for any three group elements f, g, h we have

$$f \cdot (g \cdot h) = (f \cdot g) \cdot h.$$

- We are lazy and will usually omit the $\cdot$ symbol. We will also frequently omit parentheses, since we already know the group operation is associative.

Example

$\mathbb{Z}/n$ (the integers modulo n) is a group whose group operation is $+$

Example

$\mathbb{Z}/n$ (the integers modulo n) with operation $\times$ is *not* a group. Why?

Permutations

Definition

A permutation of a set X is a bijective map $f : X \to X$.

Definition

The composition of two permutations f, g of X is the permutation $f \circ g$ so that $(f \circ g)(x) = f(g(x))$ for all $x \in X$.

Definition

The identity is the permutation $\mathrm{id}(x) = x$. We frequently use e to refer to this element as well.

Definition

Each permutation f has an inverse permutation f^{-1} with the property that $f^{-1} \circ f = \mathrm{id}$.

Permutations, cont.

Exercise

Show that every permutation is a composition of cycles; that is, for every x there is an index k such that $f^k(x) = x$.

- Sometimes mathematicians use cycle notation to denote permutations, in which $(x_1 x_2 \cdots x_k)$ means the permutation maps

$$x_1 \mapsto x_2 \mapsto \cdots \mapsto x_k \mapsto x_1.$$

- Permutations may have multiple cycles, in which case we stack the above notation; e.g. a permutation swapping $1 \leftrightarrow 2$ and $3 \leftrightarrow 4$ may be denoted $(12)(34)$.
- Fixed points, or cycles of length 1, are normally omitted from the cycle notation.

Permutations, cont.

- It is easy to see that permutation composition is associative; that is, for permutations f, g, h we have
$$f \circ (g \circ h) = (f \circ g) \circ h.$$
- However, permutation composition is *not always commutative*. If we take $X = \{1, 2, 3\}$, $f = (12)$, $g = (23)$, then
$$f \circ g = (123) \neq (132) = g \circ f.$$

Group of permutations

Definition

Let G be a set of permutations of X. We say that G is a group of permutations of X if

- $\mathrm{id} \in G$;
- for all $f \in G$, we have $f^{-1} \in G$; and
- for all $f, g \in G$, we have $f \circ g \in G$.

Exercise

Verify the group axioms in the above definition of a group of permutations.

- The only axiom which is not immediately given is associativity; however, function composition (in this case these are actually permutations, which are bijective functions from X to itself) is associative.

Definition

We define the symmetric group of order n, denoted S_n, to be the set of *all* permutations on a set of size n.

Example (S_3)

We have $S_3 = \{e, (12), (13), (23), (123), (132)\}$.

More on permutations

Definition

A transposition is a permutation which swaps two elements and fixes all other elements. For example, (12) is a transposition in our previous example of S_3.

Definition

An inversion of a permutation σ is a pair (i, j) such that $i < j$ but $\sigma(i) > \sigma(j)$.

Definition

Define the alternating group of order n, denoted A_n, to be the set of permutations in S_n which have an even number of inversions.

Lemmas on S_n

Lemma

Show that the transpositions generate S_n; that is, any element $\sigma \in S_n$ can be written as a composition of transpositions.

- Since each permutation is a product of cycles, it suffices to show the statement for a cycle.
- WLOG consider the cycle $(123 \ldots k)$. We have

$$(123 \ldots k) = (1k)(1(k-1)) \ldots (12).$$

Lemma

Show that A_n is also the set of permutations which can be written as the product of an even number of transpositions.

- It suffices to show that any transposition changes the parity of the number of inversions when composed on an arbitrary permutation.
- Work in S_n. Consider the transposition (ij) composed on the (arbitrary) permutation σ; if we write out

$$(\sigma(1), \sigma(2), \ldots, \sigma(n)),$$

  then the number of inversions is the number of pairs of elements in this tuple which are decreasing.
- Swapping i and j in the above tuple changes the number of inversions by ± 1 when considering the pair (i, j)
- For any element which appears in between i and j in the above tuple, that element contributes to a change of 0 or ± 2 in the number of inversions.
- For any element does not appear in between i and j, they contribute no change to the number of inversions.
- This shows that a transposition changes the parity of the number of inversions.

Lemma

Show that A_n is indeed a group, as its name suggests.

- $\sigma \in S_n$ is in A_n if and only if it is the product of an even number of transpositions from the above lemma.
- e is the product of 0 transpositions, so $e \in A_n$.
- If $a = t_1 \cdots t_{2k}$ is a product of $2k$ transpositions so that $a \in A_n$, then $a^{-1} = t_{2k} \cdots t_1$ is also a product of $2k$ transpositions, so $a^{-1} \in A_n$ as well.
- It is also clear that the product of 2 elements in A_n must be in A_n as well, so A_n is closed.
- Associativity of the group operation is inherited from S_n.

Lemmas on A_n

Definition

A 3-cycle is defined as an element of the form (xyz) which sends $x \mapsto y \mapsto z \mapsto x$ and fixes all other elements.

Lemma

Show that the 3-cycles are in A_n, and moreover, that the 3-cycles generate A_n.

- First, we have $(xyz) = (xz)(xy)$ is the product of 2 transpositions, so all 3-cycles are in A_n.
- We also have that

$$(wx)(yz) = (wx)(wy)(yw)(yz) = (wyx)(yzw),$$

  so the product of any two transpositions is generated by 3-cycles. But any element $a \in A_n$ can be written as the product of "products of two transpositions," which finishes.

Subgroups

Definition

For a group G, we define a subset $H \subseteq G$ to be a subgroup of G if

(i) The identity, 1, is in H.

(ii) For each $h \in H$, we have $h^{-1} \in H$.

(iii) For all $g, h \in H$, we have $gh \in H$.

Example

We have shown earlier that A_n is a subgroup of S_n for all n.

Example

The trivial subgroup $\{e\}$ which only contains the identity is a subgroup of every group G.

Definition

For H a subgroup of G:

- For $g \in G$, the right coset of H containing g is $\{hg : h \in H\}$.
- For $g \in G$, the left coset of H containing g is $\{gh : h \in H\}$.

Lagrange's Theorem

One nice property about subgroups of a finite group is given by Lagrange's Theorem:

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $\#(H) \mid \#(G)$.

Proof.

- The key is to show that the (left) cosets of H in G partition G (which obviously suffices).
- Suppose that $g_1 H$ and $g_2 H$ are two cosets of H sharing an element $g_1 h_1 = g_2 h_2$ in common.
- From $g_1 h_1 = g_2 h_2$ we get

$$g_2^{-1} g_1 h_1 h_1^{-1} = g_2^{-1} g_2 h_2 h_1^{-1}$$
$$\implies g_2^{-1} g_1 = h_2 h_1^{-1}.$$

- Since H is closed under the group operation, $g_2^{-1} g_1 = h_2 h_1^{-1} \in H$, so for all h,

$$g_1 h = g_2 g_2^{-1} g_1 h = g_2 h_2 h_1^{-1} h \in g_2 H,$$

  implying $g_1 H \subseteq g_2 H$.
- Analogously $g_2 H \subseteq g_1 H$, so $g_1 H = g_2 H$. □

Normal Subgroups

Definition

Let N be a subgroup of G. We say that N is a normal subgroup of G if for every element g, we have that the left coset gN is equal to the right coset Ng.

Warning

Just because the cosets are equal doesn't necessarily mean that $gn = ng$ for any $g \in G$ and $n \in N$; we only know that for any $g \in G$ and $n_1 \in N$, $gn_1 = n_2 g$ for some other element $n_2 \in N$.

Exercise

Show that the condition for a subgroup N of G being normal is equivalent to the condition that $gng^{-1} \in N$ for every $g \in G$ and $n \in N$.

- Let $gn = n'g$ for some $n' \in N$, then $gng^{-1} = n' \in N$, as desired.

Why do normal subgroups matter? One answer is that normal subgroups N of G can generate a quotient group G/N whose elements are the cosets of N. The operation $gN \cdot hN$ is given by the coset $(gh)N$; one example of this is $\mathbb{Z}/2\mathbb{Z}$, which gives the quotient group of the integers modulo 2. Verifying that the quotient group is well defined and is indeed a group is not hard, but not our focus today. Instead, we derive some more properties of S_n and A_n.

Definition

A group G is simple if the only normal subgroups of G are $\{e\}$ and G.

Goal for the rest of the talk

For the rest of the talk, we aim to prove the following two theorems:

Theorem

For $n \geq 5$, the only normal subgroups of S_n are $\{e\}$, A_n, and S_n.

Theorem

For $n \geq 5$, the A_n is simple.

These two theorems have deep implications such as the impossibility of the quintic formula despite formulas existing for quadratics, cubics, and quartics!

Conjugacy classes

To prove the above theorems, we will need to introduce the concept of a conjugacy class. Note how the definition is similar to the condition for a normal subgroup.

Definition

Let G be a group and let $g_1, g_2 \in G$. We say that g_1 is conjugate to g_2 if there is some $h \in G$ with $g_1 = hg_2h^{-1}$.

Lemma

Conjugacy is an equivalence relation. The equivalence classes of this relation are called conjugacy classes. By the definition of a normal subgroup, a conjugacy class is either entirely contained in the normal subgroup or completely disjoint from it.

Proof.

We will verify the three properties of equivalence relations:

- **Reflexivity:** Take $h = 1$, so for all g we have g conjugate to itself.
- **Symmetry:** If g_1 is conjugate to g_2 by $g_1 = hg_2h^{-1}$, then g_2 is conjugate to g_1 by $g_2 = h^{-1}g_1(h^{-1})^{-1}$.
- **Transitivity:** If g_1 is conjugate to g_2 by $g_1 = hg_2h_1^{-1}$ and g_2 is conjugate to g_3 by $g_2 = h_2g_3h_2^{-1}$, then g_1 is conjugate to g_3 by

$$g_1 = h_1h_2g_3h_2^{-1}h_1^{-1} = h_1h_2g_3(h_1h_2)^{-1}. \qquad \square$$

Conjugacy classes in S_n

Exercise

Show that conjugacy classes in S_n consist of elements which have the same "cycle structure." For example, all elements of the form $(ab)(cd)$ (with a, b, c, d distinct) are in the same conjugacy class.

- Let $t = (ij)$ be a transposition, and σ be an arbitrary permutation. Then $t = t^{-1}$ and we have that $t\sigma t$ (which is conjugate to σ) swaps i and j in the cycle structure of σ.
- Then we can repeatedly use transpositions to swap elements in the cycle structure of σ, which proves the claim.

As a corollary:

Corollary

All transpositions are in the same conjugacy class of S_n.

Let $n \geq 5$.

- Suppose that N is a normal subgroup of S_n and suppose that $a \neq e \in N$ so that $N \neq \{e\}$. We will prove that $N = A_n$ or $N = S_n$ by proving that $A_n \subseteq N$. Note that the entire conjugacy class of a is contained in N.
- To attain our aforementioned goal it suffices to find a 3-cycle in N, since then, as all 3-cycles are in the same conjugacy class, all 3-cycles are in N. But we also know that the 3-cycles generate A_n, implying $A_n \subseteq N$ by the closure of N as a subgroup.
- WLOG we can write $a = (123\ldots k)b$ where k is the length of the longest cycle of a (by permuting the numbers in cycle notation of a to get a cycle of the form $(123\ldots k)$) for some permutation b which fixes $1, 2, \ldots, k$. Now we distinguish two cases based on the length k of the largest cycle of a.

1. If $k \geq 3$, then by permuting elements in the cycle notation of a, we know that the element $a' = b^{-1}(1(k-1)k(k-2)\dots 32)$ exists in N. Then by closure, we also have that

$$aa' = (123\dots k)bb^{-1}(1(k-1)k(k-2)\dots 32) = (1k(k-1)),$$

   which is a 3-cycle, as desired.

2. Else, $k \leq 2$, so a is the product of transpositions on disjoint elements. If a is a transposition itself, then if $a = (xy)$, permuting cycle notation gives $a' = (xz) \in N$, so by closure $aa' = (xzy) \in N$, which is a 3-cycle, as desired. Otherwise, there are at least two transpositions in a. WLOG let $a = (12)(34)c$ for some c which fixes $1, 2, 3, 4$ and is also a product of disjoint transpositions (in particular, $c^2 = e$) by permuting elements in the cycle notation of a. Now, as $n \geq 5$, the following two subcases are the only possible:
   a. a has a fixed point. WLOG let this fixed point be 5. Then taking $a' = c(32)(54)$ gives by closure

   $$aa' = (12)(34)cc(32)(54) = (12453) \in N,$$

      so we can revert back to the original case of the longest cycle having length larger than 2.
   b. Else, a has at least one other cycle. WLOG let this cycle be (56). Then if $c = (56)d$, taking $a' = d(32)(54)(16)$ gives by closure

   $$aa' = (12)(34)(56)dd(32)(54)(16) = (153)(246) \in N.$$

      Again, we can revert back to the original case of the longest cycle having length larger than 2.

Normal Subgroups of S_n

Based on our above work, we know that if N is a nontrivial normal subgroup of S_n, then $A_n \subseteq N$. However, this means that $\#(N) \geq \frac{\#(S_n)}{2}$. Recalling Lagrange's theorem on the sizes of subgroups, this means that $\#(N) = \#(A_n)$ or $\#(N) = \#(S_n)$, implying the first of the two theorems:

Theorem

For $n \geq 5$, the only normal subgroups of S_n are $\{e\}, A_n$, and S_n.

Normal Subgroups of A_n

We can follow a similar solution path to prove that A_n is simple for $n \geq 5$, i.e. it has no normal subgroups other than the trivial $\{e\}$ and itself. Here is an outline of the proof:

- As before, let N be a normal subgroup of A_n and let $a \neq e \in N$ so that $N \neq \{e\}$.
- Prove that all 3-cycles are in the same conjugacy class in A_n; this requires a bit more work due to the fact that we cannot use a single transposition to conjugate the three cycle. The condition $n \geq 5$ is needed to we have enough space to “add on a dummy transposition.” To illustrate this, we have that (xyz)
- Prove that we must have some 3-cycle in A_n, so that all 3-cycles are in A_n.
- Use the fact that the 3-cycles generate A_n to conclude.

Now, we fill in the details of the above proof:

Lemma

All 3-cycles are in the same conjugacy class.

- First, we prove that $c = (xyz)$ is conjugate to its own inverse. Since $n \geq 5$, let a, b be elements distinct from x, y, z. Note that

$$c = ((ab)(yz))(xzy)((ab)(yz))^{-1}$$

is of the form $ac^{-1}a^{-1}$, so c is conjugate to c^{-1}.

- Now, we show that (xyz) is conjugate to (ayz), which will complete the proof (since then we can swap out elements of the 3-cycle one at a time, which allows us to get from any 3-cycle to any other through a series of conjugations). But we have that

$$(xyz) = ((ax)(yz))(azy)((ax)(yz))^{-1},$$

and $(azy) = (ayz)^{-1}$ are conjugates, so (xyz) is conjugate to (ayz), as desired.

Lemma

Some 3 cycle exists in A_n.

- Here, basically the exact same proof as we gave for S_n works, where we take $a \neq e \in A_n$ and take cases based on the size k of the largest cycle in a. Write $a = (123 \ldots k)b$ where b fixes $1, 2, \ldots, k$.
- We can verify in a similar manner to the case of S_n that the conjugacy classes in A_n are created by applying an even number of transpositions on elements in the cycle structure, rather than any number of transpositions.
- When $k \geq 3$, we can find another element a' in the conjugacy class of a such that aa' is a 3-cycle.
- When $k \leq 2$, we can find another element a' in the conjugacy class of a such that the maximum cycle length of aa' is larger than 2, and revert to the previous case.

Now, since at least one 3-cycle is in N, all of them must be in N; as the 3-cycles generate A_n, then $N = A_n$, as desired. Therefore, we have proven the second theorem:

Theorem

For $n \geq 5$, the A_n is simple.

Other topics of interest

- Analyze where our proofs above fail when $n \leq 4$, and find a nontrivial normal subgroup of A_4.
- Learn more about quotient groups G/N, where N is a normal subgroup of G.
- Attend Eric's lecture, which is immediately after this!

Acknowledgements

- Some portions of this talk were based on content covered in David Speyer's advanced seminar on Galois Theory at PROMYS 2021.

- Thank you for listening!