35003 MODERN ALGEBRA

Prof Murray Elder, UTS

Week 3: permutation groups

Lauritzen 2.9

Recall from last week the process of finding a “maximal” proper normal subgroup, quotienting and repeating to decompose a finite group into “easier” pieces, until you cannot find a normal subgroup anymore.

A group that has no proper non-trivial normal subgroups is called *simple*.

One goal of today is to prove the existence of a large family of non-cyclic simple groups called A_n.

THE SYMMETRIC GROUP ON n ELEMENTS

Recall S_3: the set of bijective maps from $M_3 = \{1, 2, 3\}$ to itself.

Elements of S_3 were written as $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

We can generalise to n elements as follows.

Let $M_n = \{1, 2, \ldots, n\}$, and S_n the set of bijective maps from M_n to itself.

Group? (assoc yes because it is a set of maps). Check. Abelian?

THE SYMMETRIC GROUP ON n ELEMENTS

An element of S_n is called a *permutation*, $\sigma \in S_n$.

As for S_3, we can denote a bijective map $\sigma \in S_n$ by
$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Since elements $\sigma, \tau \in S_n$ are maps, we "multiply" right-to-left, so $\sigma\tau$ is the map $x \mapsto \sigma(\tau(x))$ for all $x \in M_n$.

S_3 is isomorphic to the set of isometries of $\mathbb{R}^2$ which preserve a triangle centred at $(0, 0)$.

Question: is this true in general: is S_n isomorphic to isometries of an n-gon?

Definition (2.9.1)

Let $\sigma \in S_n$, then define

$$M_\sigma = \{x \in M_n \mid \sigma(i) \neq i\}$$

Two perms are *disjoint* if $M_\sigma \cap M_\tau = \emptyset$ (they move different elements around).

Proposition (2.9.2)

If $\sigma, \tau \in S_n$ are disjoint, then they commute.

Proof: Show that $\sigma(\tau(x)) = \tau(\sigma(x))$ for all $x \in M_n$.

3 cases: $x \notin M_\sigma \cup M_\tau$, then $\sigma(\tau(x)) = x = \tau(\sigma(x))$.

$x \in M_\sigma$ (so not in M_τ, $\tau(x) = x$), then $\sigma : \sigma(x) \mapsto \sigma(x)$ would mean σ is not injective, so $\sigma(x) \in M_\sigma$ as well, which means τ doesn't move $\sigma(x)$, so

$$\tau(\sigma(x)) = \sigma(x) \quad \text{and} \quad \sigma(\tau(x)) = \sigma(x)$$

last case same. $\square$

CYCLE

Let $\sigma \in S_n$ and $x_1, \ldots, x_k \in M_n$ k distinct elements of M_n.

We call σ a *k-cycle* if

$$\sigma(x_1) = x_2, \sigma(x_2) = x_3, \ldots \sigma(x_k) = x_1$$

and $M_\sigma = \{x_1, \ldots, x_k\}$.

Notation: $(x_1\ x_2\ \ldots x_k)$.

Eg: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$ is written $(1\ 4\ 2) = (4\ 2\ 1)$

1-cycle = e
2-cycle: $(i\ j)$ just swaps i and j, so it has order 2. In general the order of a k-cycle is k for $k \geqslant 2$.

Suppose τ is an arbitrary permutation in S_n.

Start with 1 and "follow it around, until you get back to 1". Write down that k-cycle $(1 \ \dots) = \sigma_1$.

Now start with the next smallest element in $M_n \setminus M_{\sigma_1}$, and repeat. Stop after t steps when $M_n = M_{\sigma_1} \cup \dots M_{\sigma_t}$.

Claim: $\tau = \sigma_1 \cdots \sigma_t$. (Hint: they commute). Prop 2.9.6 in Lauritzen, proof by induction.

Proposition (2.9.5)

If $\sigma \in S_n$ is written as a product of disjoint cycles $\sigma_1 \cdots \sigma_r$, then the order of σ is the lcm of the orders of σ_i.

Proof: Since disjoint cycles commute, $\sigma^n = \sigma_1^n \ldots \sigma_r^n$ ...

Lemma (2.9.8)

If $\tau = (i_1 \dots i_k) \in S_n$ is a k-cycle and $\sigma \in S_n$. Then

$$\sigma \circ (i_1 \dots i_k) \circ \sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k))$$

In words: conjugating τ by σ gives another k-cycle, which is $(\sigma(i_1) \dots \sigma(i_k))$.

Proof: Let $J = \{ (\sigma(i_1) \dots \sigma(i_k)\}$. The RHS moves every element of J, and nothing else. It sends $\sigma(i_p)$ to $\sigma(i_{(p+1) \mod k})$.

The LHS starts with an element $\sigma(i_p)$ in J, sends it via σ^{-1} to i_p in $\{i_1, \dots, i_k\}$, then τ sends i_p to $i_{(p+1) \mod k}$, then σ sends it back into J to $\sigma(i_{(p+1) \mod k})$, so LHS and RHS do the same thing to J.

To finish, LHS does not move $M_n \setminus J$ because it simply hits by σ^{-1}, τ does nothing, then goes back via σ. $\square$

SIMPLE TRANSPOSITION

A simple transposition in S_n is $(i\ i+1)$ for $1 \leqslant i < n$.

We use the notation $s_i = (i\ i+1)$.

Sort 631542

631542 361542 316542 136542 135642
135462 134562 134526 134256 132456
123456.

The process of switching neighbors corresponds to the simple transpositions

$$(12)(23)(12)(34)(45)(34)(56)(45)(34)(23),$$

where the numbers refer to the positions in the sequence. In the language of permutations and S_6 you may express the first step of the bubble sort as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix} (12) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 4 & 2 \end{pmatrix}.$$

In total we have proved that

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix} (12)(23)(12)(34)(45)(34)(56)(45)(34)(23)$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

and therefore that

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix} = (23)(34)(45)(56)(34)(45)(34)(12)(23)(12).$$

You should check this by evaluating the permutations on the left and right hand side on 1, 2, 3, 4, 5 and 6.

Definition (Inversion, 2.9.10)

Let $\sigma \in S_n$. A pair (i, j) with $1 \leqslant i < j \leqslant n$ is called an *inversion* of σ if $\sigma(i) > \sigma(j)$.

Let $I_\sigma = \{(i, j) \mid 1 \leqslant i < j \leqslant n, \sigma(i) > \sigma(j)\}$ and $n(\sigma) = |I_\sigma|$.

Ex: number of inversions in $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix}$ which we just wrote as a product of simple transpositions.

Claim: (prop 2.9.12 but I think its pretty obvious) σ is the identity if and only if $n(\sigma) = 0$ (nothing is out of order).

If not identity then there is some $i < n$ where $\sigma(i) > \sigma(i+1)$.

"Proof:" if not id, suppose $1 \mapsto 1, 2 \mapsto 2, \ldots$ but eventually some $i \mapsto \sigma(i) \neq i$, then $\sigma(i) > i$ since the numbers $1, \ldots, i-1$ have already been used.

Then maybe $i+1 \mapsto \sigma(i+1) > \sigma(i)$ and so on, but all numbers greater than i cannot map to numbers greater than $\sigma(i)$ since there is a gap $[i, \sigma(i)]$ in the range of the function.

Lemma (2.9.13)

$$n(\sigma s_i) = \begin{cases} n(\sigma)+1 & \sigma(i) < \sigma(i+1) \\ n(\sigma)-1 & \sigma(i) > \sigma(i+1) \end{cases}$$

Proof: Assume $\sigma(i) < \sigma(i+1)$. Then applying s_i followed by σ will send $i \mapsto i+1 \mapsto \sigma(i+1)$ and send $i+1 \mapsto i \mapsto \sigma(i) < \sigma(i+1)$, so $(i, i+1)$ is an inversion for σs_i.

So if we can prove $\varphi\colon I_\sigma \to I_{\sigma s_i} \setminus \{(i, i+1)\}$ is a bijection then we have our count increasing by 1 for this case.

Claim: defining $\varphi((k,l)) = (s_i(k), s_i(l))$ does it (Check this on all pairs (k,l) – only issue is when one of these is i or $i+1$)

Trick to do $\sigma(i) > \sigma(i+1)$: look at σs_i. We have $(\sigma s_i)(i) < (\sigma s_i)(i+1)$ so from the previous case,

$$n((\sigma s_i)s_i) = n((\sigma s_i)) + 1$$

Proposition (2.9.14)

σ is a prod of $n(\sigma)$ simple transpositions,

and this is the minimum number of simple transpositions needed to write σ as a product of simple transpositions.

SIGN OF A PERMUTATION

Define $\operatorname{sgn}(\sigma) = (-1)^{n(\sigma)}$.

Say a permutation is *even* if $\operatorname{sgn} = 1$, and odd if $\operatorname{sgn} = -1$.

Proposition (2.9.16)

$$sgn : S_n \to \{\pm 1\}$$

is a group homomorphism to the multiplicative group of order 2.

Proof: since perms are products of simple perms, prove for $\sigma \in S_n$ and τ a simple perm in S_n.

Use the $n(\sigma) \pm 1$ lemma. □

What is the kernel?

(remember last week we said ker is a good way to obtain interesting groups)

Define A_n to be the kernel of the sgn map which is the set of all even permutations in S_n.

Two reasons why A_n is a normal subgroup:

1. kernels are normal subgroups
2. its a subgroup and has index 2

Lagrange: what is the size of A_n?

EASY FACT ABOUT CYCLES

Prop 2.9.17: the sgn of a r-cycle $(x_1 \ \ldots x_r)$ is $(-1)^{r-1}$

so for example a transposition is odd, and a 3-cycle is even.

Proof:

Theorem (2.9.19 (Result due to Galois, age 20-21?))

A_n is simple for $n \geqslant 5$

Strategy:

1. every perm in A_n is the product of 3-cycles (lemma 2.9.18)

2. given a 3-cycle $\tau \in A_n$, there is a perm $\sigma \in A_n$ so that $\sigma\tau\sigma^{-1} = (123)$
   (so we can translate an arb 3-cycle to a specific one, and backwards, so as soon as you have one 3-cycle in a normal subgroup, you have (123) and then you end up with every 3-cycle and thus the whole of A_n)

3. A non-trivial normal subgroup must contain a 3-cycle.

Lemma (2.9.18)

Every perm in A_n is the product of 3-cycles.

This follows from observing that for $a, b, c, d \in M_n$ all distinct,

$$(a\ b)(c\ d) = (a\ d\ c)(a\ b\ c)$$

and

$$(a\ b)(b\ c) = (a\ b\ c)$$

Recall the lemma that every $g \in G$ acts (by left multiplication) as a bijection from G to G.

Theorem (Cayley's theorem)

Every group is a subgroup of a permutation group.

Let's think about this just for finite groups for now: if $|G| = n$, let $G = \{g_1, \ldots, g_n\}$. Then g_i acts a permutations on the set M_n by $g_i : j \mapsto k$ where $g_k = g_i g_j$, so g_i is identified with an element of S_n.

Check: closed, identity, inverse.

Thus G is a subgroup of S_n.

NEXT:

Reading: Lauritzen 2.1–2.9.

Exercises up to 2.11.50

Practice test (on Canvas)

Next week:

- no zoom lecture wednesday
- in class test 12noon-1:20pm CB10.02.420