

35003 MODERN ALGEBRA

Prof Murray Elder, UTS
Week 3: permutation groups

Lauritzen 2.9



SIMPLE

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.

$\mathbb{Z}/p\mathbb{Z}$

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

$N_1, G/N_1$
①

N_1/N_2

$G/N_1, N_2$

THE SYMMETRIC GROUP ON n ELEMENTS

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

$$f(1) = 3$$

$$f(2) = 1$$

$$f(3) = 2$$

S_n bijective maps from $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$

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

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

3/24

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

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

S_n \longrightarrow Subgroup
 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 $M_n = \{1, 2, \dots, n\}$, 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

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

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 $x \in M_n$.

~~$f \circ g : \mathbb{R} \rightarrow \mathbb{R}$~~
 ~~$f(g(x))$~~

THE SYMMETRIC GROUP ON n ELEMENTS

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

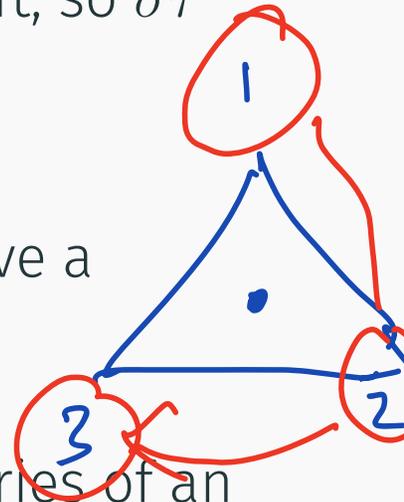
An element of S_n is called a *permutation*, $\sigma \in S_n$.

As for S_3 , we can denote a bijective map $\sigma \in S_n$ by

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

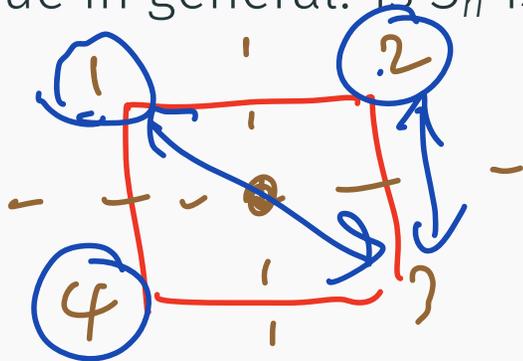
Since elements $\sigma, \tau \in S_n$ are maps, we “multiply” right-to-left, so $\sigma\tau$ is the map $x \mapsto \sigma(\tau(x))$ for all $x \in M_n$.

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?

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



order 8
Dihedral groups.

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

SUPPORT OF σ

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$
$$M_\sigma = \{1, 2, 3\}$$

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).

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

$$\tau \circ \sigma$$
$$\sigma \circ \tau$$

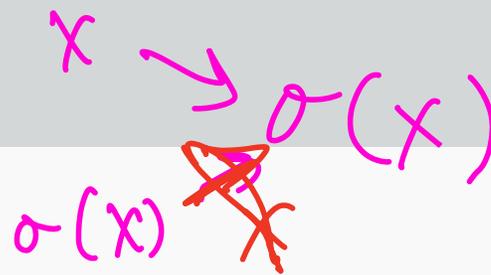
$$M_\tau = \{4, 5\}$$

Proposition (2.9.2)

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

Proof:

SUPPORT OF σ



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 $\sigma(\tau(x)) = x = \tau(\sigma(x))$.

② $x \in M_\sigma$ not in M_τ

$$\sigma(\tau(x)) = \sigma(x)$$

③ $x \in M_\tau$ not in M_σ

~~$\sigma(\sigma(x)) \neq \sigma(x)$~~

If ~~not~~ NOT POSS.

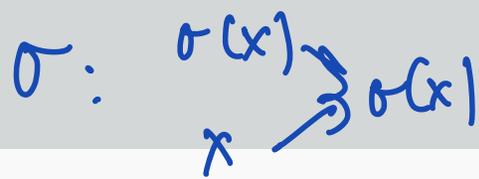
σ bijectm, $\sigma(x) \neq \sigma(x)$

$\sigma(x) \in M_\sigma \therefore \sigma(x) \notin M_\tau$

$$\tau(\sigma(x))$$

$$= \sigma(x)$$

SUPPORT OF σ



$$M_\tau \cap M_\sigma = \emptyset$$

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

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

last case same.

If $\sigma(x) \in M_\tau$ then $\sigma(x) \notin M_\sigma$ \square

~~$$\text{so } \sigma(\sigma(x)) = \sigma(x)$$~~

$$\tau(\sigma(x)) = \sigma(x)$$

not possible unless two elts \rightarrow same

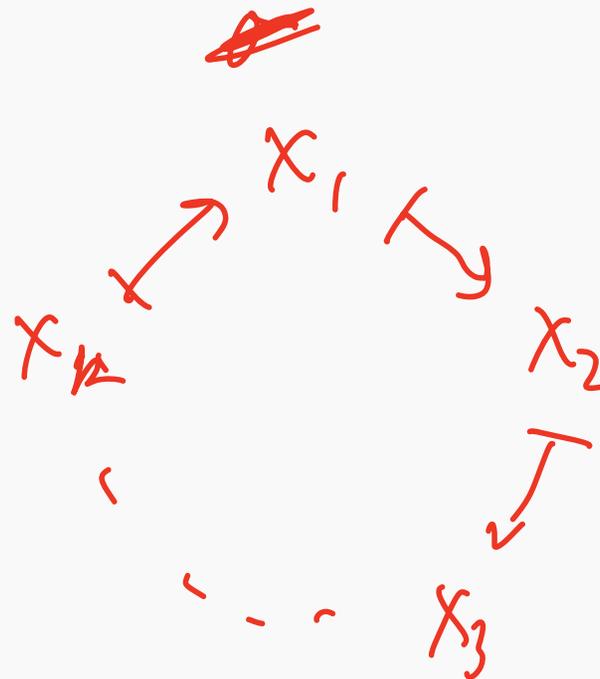
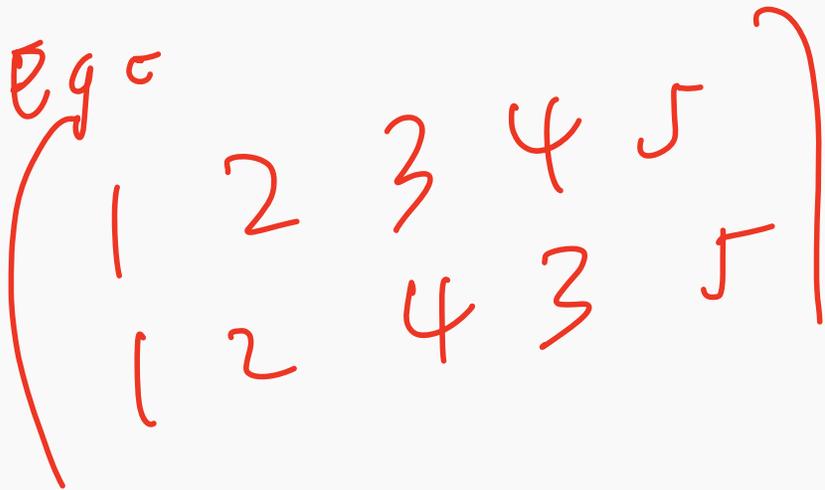
CYCLE

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

We call σ a k -cycle if

$$\sigma(\underline{x_1}) = \underline{x_2}, \sigma(x_2) = x_3, \dots, \sigma(x_k) = x_1$$

and M_σ = $\{x_1, \dots, x_k\}$.



CYCLE

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

We call σ a k -cycle if

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

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

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

Eg from beginning $= (6 \ 2) \circ (3 \ 4)$

CYCLE

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

We call σ a k -cycle if

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

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

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

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

CYCLE

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

We call σ a k -cycle if

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

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

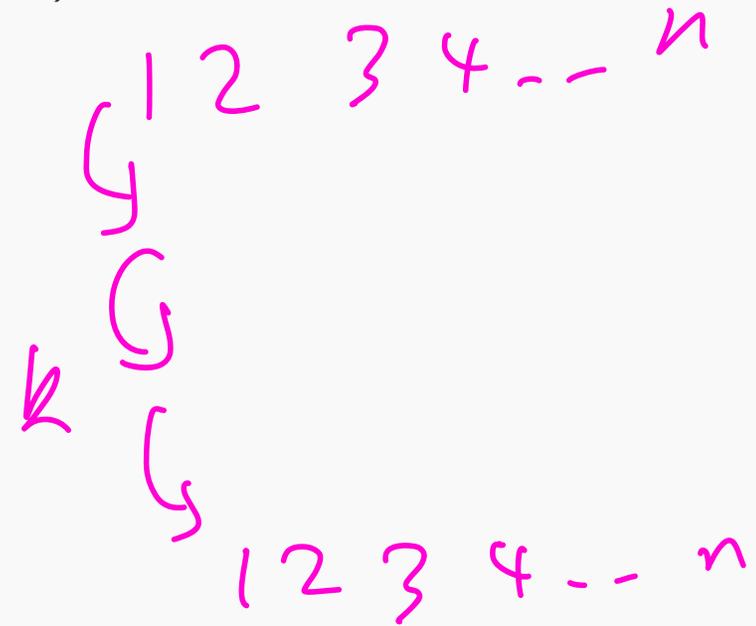
Notation: $(x_1 x_2 \dots x_k)$.

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

1-cycle = e (1)

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 $k \geq 2$.

transposition



CYCLE NOTATION

Suppose τ is an arbitrary permutation in S_n .

CYCLE NOTATION

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 $(1 \dots) = \sigma_1$.

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

CYCLE NOTATION

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 $M_n = M_{\sigma_1} \cup \dots \cup M_{\sigma_t}$.

Claim: $\tau = \sigma_1 \cdots \sigma_t$. (Hint: they commute).

CYCLE NOTATION

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 $(1 \dots) = \sigma_1$.

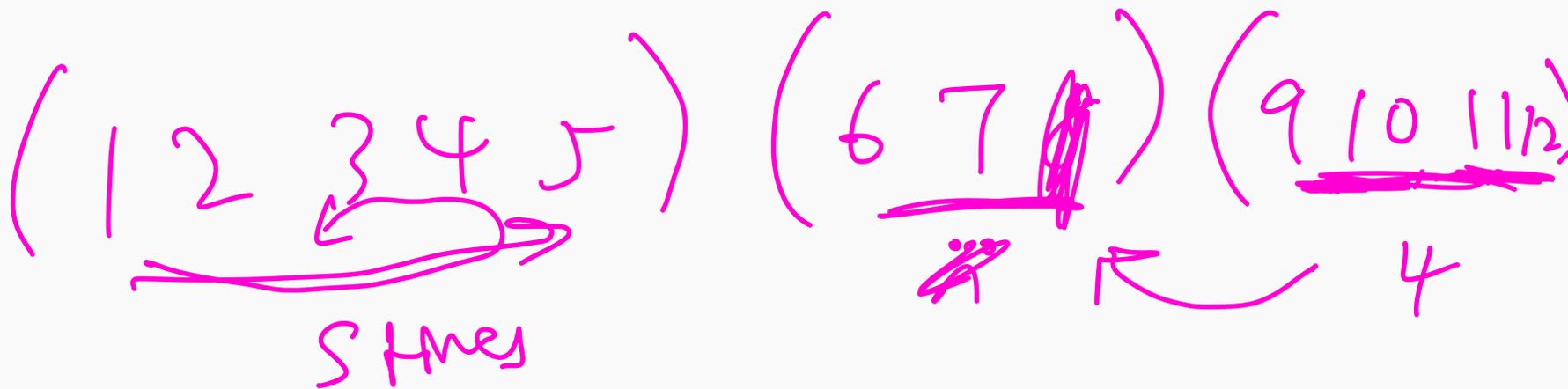
Now start with the next smallest element in $M_n \setminus M_{\sigma_1}$, and repeat. Stop after t steps when $M_n = M_{\sigma_1} \cup \dots \cup M_{\sigma_t}$.

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

CYCLE NOTATION

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 .



20

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, $\sigma^n = \sigma_1^n \cdots \sigma_r^n \dots$

A USEFUL LEMMA

Lemma (2.9.8)

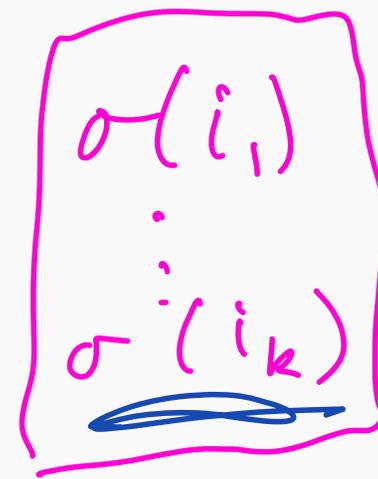
If $\tau = (i_1 \dots i_k) \in S_n$ is a k -cycle and $\sigma \in S_n$. Then

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

τ
~~1 2 3~~
 τ^{-1}
}
cycle

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

If $x \in M_n$ is not one of



that τ does not move it.

then $\sigma^{-1}(x)$ is not one of i_1, \dots, i_k

$$\tau(\sigma^{-1}(x)) = \sigma^{-1}(x)$$

so LHS

$$\therefore \sigma(\tau(\sigma^{-1}(x))) = \sigma(\sigma^{-1}(x)) = x \quad 10/24$$

A USEFUL LEMMA

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 $\sigma(i_{(p+1) \bmod k})$.

A USEFUL LEMMA

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 $\sigma(i_{(p+1) \bmod k})$.

If $x = \sigma(i_p)$ ie $x \in J$,

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 $i_{(p+1) \bmod k}$, then σ sends it back into J to $\sigma(i_{(p+1) \bmod k})$, so LHS and RHS do the same thing to J .



A USEFUL LEMMA

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 $\sigma(i_{(p+1) \bmod k})$.

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 $i_{(p+1) \bmod k}$, then σ sends it back into J to $\sigma(i_{(p+1) \bmod k})$, 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 . □

SIMPLE TRANSPOSITION

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

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

COMP SCI CONNECTION: BUBBLE SORT

Sort 631542



3 6 1 5 4 2

3 1 6 5 4 3



1 2 3 4 5 6

COMP SCI CONNECTION: BUBBLE SORT

Sort 631542

$\begin{array}{ccccc} \overset{\curvearrowright}{6}31542 & \overset{\curvearrowright}{3}61542 & \overset{\curvearrowright}{3}16542 & 136542 & 135642 \\ \underline{6}31542 & \underline{3}61542 & \underline{3}16542 & 136542 & 135642 \\ 135462 & 134562 & 134526 & \underline{134256} & \underline{132456} \\ \underline{123456} & & & & \end{array}$

The process of switching neighbors corresponds to the simple transpositions

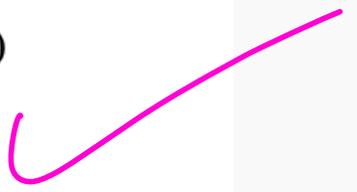
$(12)(23)(12)(34)(45)(34)(56)(45)(34)(23),$

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

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

$$\begin{pmatrix} 1 & 2 & \dots & 6 \\ 6 & 3 & \dots & 2 \end{pmatrix} \underbrace{(12)(23) \dots (23)}_{\text{pink arrow}} = \begin{pmatrix} 1 & 2 & 3 & \dots & 6 \\ 1 & 2 & 3 & \dots & 6 \end{pmatrix} e$$

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.

INVERSIONS

Definition (Inversion, 2.9.10)

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

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

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

1,2	3,4
1,3	3,5
2,3	4,5

$$i=1, j=2$$

$$\begin{aligned} \therefore (1, 2) & \text{ inv. of } \sigma \\ \sigma(i) &= 3 \\ \sigma(j) &= 2 \end{aligned}$$

INVERSIONS

Definition (Inversion, 2.9.10)

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

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

INVERSIONS

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 $\sigma(i) > \sigma(i+1)$.

have at least
one
inversion
 $(i, i+1)$

INVERSIONS

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 $1 \mapsto 1, 2 \mapsto 2, \dots$ but eventually some $i \mapsto \sigma(i) \neq i$, then $\sigma(i) > i$ since the numbers $1, \dots, i-1$ have already been used.

Then maybe $i+1 \mapsto \sigma(i+1)$ ^{maybe} $> \sigma(i)$ 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.

$$s_i = (i \ i+1)$$

Lemma (2.9.13)

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

Proof:

HOW TO COUNT INVERSIONS

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 $i \xrightarrow{s_i} i+1 \xrightarrow{\sigma} \sigma(i+1)$ and send $i+1 \xrightarrow{s_i} i \xrightarrow{\sigma} \sigma(i) < \sigma(i+1)$, so $(i, i+1)$ is an inversion for σs_i .

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

HOW TO COUNT INVERSIONS

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 $\varphi: I_\sigma \rightarrow I_\sigma \setminus \{(i, i+1)\}$ 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 $i+1$)

HOW TO COUNT INVERSIONS

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 .

why

So if we can prove $\varphi: I_\sigma \rightarrow I_{\sigma s_i} \setminus \{(i, i+1)\}$ 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

+ even # inversions
- odd # inv.

Define sgn(σ) = $(-1)^{n(\sigma)}$.

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

SIGN OF A PERMUTATION

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

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

Proposition (2.9.16)

$$\text{sgn}: S_n \rightarrow \{\pm 1\}$$

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. □

SIGN OF A PERMUTATION

$$\text{sgn}(\sigma \cdot \tau) = \text{sgn}(\sigma) \cdot \text{sgn}(\tau)$$

$$\text{sgn}(\tau)$$

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

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

Proposition (2.9.16)

$$\text{sgn}: S_n \rightarrow \{\pm 1\}$$

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?

all even perms

$$S_n / \ker \cong \mathbb{Z}/2\mathbb{Z}$$

ALTERNATING GROUP

(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:

$$\text{Index } [S_n : \underline{A_n}] = 2$$

$$\boxed{(12) A_n}$$

ALTERNATING GROUP

(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

ALTERNATING GROUP

(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 ?

~~Then~~
Then

$$\frac{n!}{2}$$

$$\begin{aligned} |S_n| &= n! \\ &= |A_n| \cdot 2 \end{aligned}$$

EASY FACT ABOUT CYCLES

Prop 2.9.17: the sgn of a r -cycle $(x_1 \dots x_r)$ is $(-1)^{r-1}$
so for example a transposition is odd, and a 3-cycle is even.

Proof:

Ex

ALTERNATING GROUP IS SIMPLE FOR $n \geq 5$

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

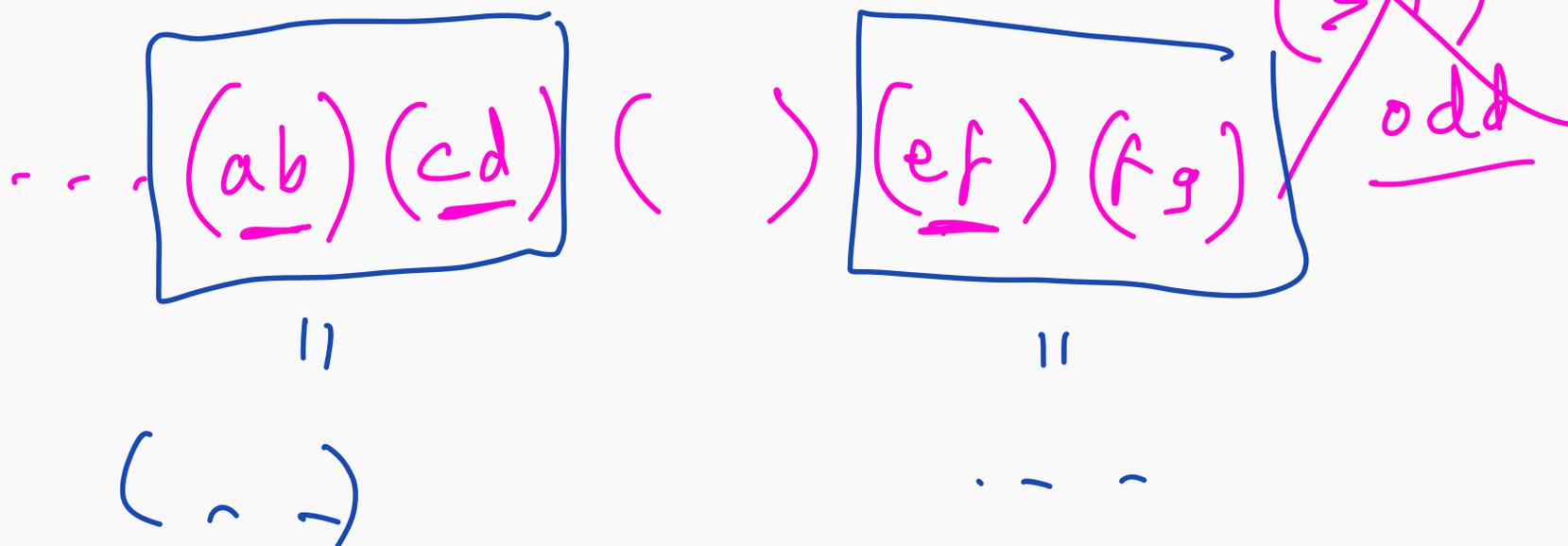
A_n is simple for $n \geq 5$

Strategy:

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

even perms.

even



ALTERNATING GROUP IS SIMPLE FOR $n \geq 5$

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

A_n is simple for $n \geq 5$

Strategy:

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

easy.

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)

$$\sigma: \begin{matrix} \dots & i_1 & \dots & i_2 & \dots & i_3 \\ & 1 & & 2 & & 3 \end{matrix}$$

Lemma

$$\sigma (i_1 i_2 i_3) \sigma^{-1} = (\sigma(i_1) \sigma(i_2) \sigma(i_3))$$

ALTERNATING GROUP IS SIMPLE FOR $n \geq 5$

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

A_n is simple for $n \geq 5$

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

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,

$$\underline{(a\ b)(c\ d)} = \underline{(a\ d\ c)(a\ b\ c)}$$

LHS/RHS
a ↗
b ↘
c ↗

and

$$\underline{(a\ b)(b\ c)} = (a\ b\ c)$$

$$\begin{aligned} & \cancel{= (b\ a)(b\ c)} \\ & = \cancel{(b\ a)(c\ b)} \end{aligned}$$

SUDOKU STRIKES AGAIN

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.

SUDOKU STRIKES AGAIN

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 $G = \{g_1, \dots, g_n\}$. 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 .

SUDOKU STRIKES AGAIN

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 $G = \{g_1, \dots, g_n\}$. 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