Document last updated: Mon, Sep 30 2024

Abstract Algebra Notes

Week 4 Wed, Sep 25 2024

Symmetric group (Sec 5.1)

Notation: $[n] := \{1, 2, \ldots, n\}$

The $\underline{\text{symmetric}}$ $\underline{\text{group}}$ on $\underbrace{n \text{ letters}}$, denoted S_n,

for convenience, the letters are $1, 2, \ldots, n$

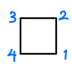
is the set of $\underbrace{\text{permutations}}$ on $[n]$ under function composition.

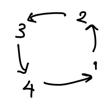
bijections from $[n]$ to itself

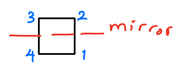
> Motivation: Every finite group is "the same" as a subgroup of S_n (Cayley's Thm Sec 9.1)

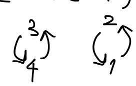
Ex: Symmetry $(\triangle) = D_3$ is S_3

Ex: Symmetry $(\square) = D_4$ is a subgroup of S_4 when viewed as follows:

- Initial State: 

- $90°$ CC Rotation can be viewed as permutation $\overset{\text{rho}}{\rho} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = (1\ 2\ 3\ 4)$ $=$ 

- Exercise: Check that the other rotations are ρ^2 and ρ^3 and Id
- Vertical flip (reflection across a horizontal mirror) 

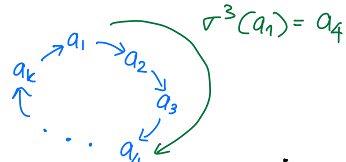
can be viewed as permutation $\overset{\text{phi}}{\phi} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = (1\ 2)(3\ 4)$
$=$ 

- Exercise: The other reflections are $(14)(23)$, (24), and (13)
- Check: These eight permutations form a group.

Ex: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ can be viewed as the cyclic group $\langle \sigma \rangle$ generated by $\sigma = (1\,2\,6)(4\,5)$ or $\sigma = \underbrace{(1\,3\,2\,6\,4\,5)}_{\text{a } 6\text{-cycle}}$

Prop A k-cycle in S_n has order k.

Proof Let $\overset{\text{sigma}}{\sigma} = (a_1 a_2 \cdots a_k)$ be a k-cycle



For $i \in [k-1]$, we have $\sigma^i(a_1) = a_{i+1} \neq a_1$ so $\sigma^i \neq Id$

But $\sigma^k(a_1) = a_1$, $\sigma^k(a_2) = a_2, \ldots,$ $\sigma^k(a_k) = a_k$, so $\sigma^k = Id$.

Therefore, $|\sigma| = k$ $\square$

Prop The inverse of a k-cycle $\sigma = (a_1 a_2 \cdots a_k)$ is the (opposite) k-cycle $(a_k \cdots a_2 a_1)$

Ex $\sigma = (1\,2\,6\,5)$ $\quad \pi = (1\,5\,6\,2)$ $\quad \sigma\pi = Id$

$$\begin{tikzcd} 1 \arrow[r] & 2 \arrow[d] \\ 5 \arrow[u] & 6 \arrow[l] \end{tikzcd} \qquad \begin{tikzcd} 1 \arrow[d] & 2 \arrow[l] \\ 5 \arrow[r] & 6 \arrow[u] \end{tikzcd}$$

Prop Disjoint cycles commute (so the order of the disjoint cycles doesn't matter)

Ex $(1\,4\,5\,6)(2\,3\,7) = (2\,3\,7)(1\,4\,5\,6)$

Thm Every $\sigma \in S$ is the product of disjoint cycles.

Ex Elements of S_3: Id, (12), (23), (13), (123), (132)

$(1)(2)(3)$, $(12)(3)$, $(1)(23)$, $(13)(2)$, (123), (132)

Ex The elts of S_4, by cycle type:

cycle type	Types	permutations	count
$(1,1,1,1)$		$Id = (1)(2)(3)(4)$	1
$(2,1,1)$	2-cycles or "transpositions"	$(12), (13), \ldots, (34)$	6
$(3,1)$	3-cycles	$(123), \ldots, (243)$	8
(4)	4-cycles	$(1234), \ldots, (1432)$	6
$(2,2)$	$(2,2)$-cycles	$(12)(34)$, $(13)(24)$, $(14)(23)$	3
			+
			$24 = 4!$

Prop The order of σ is the least common multiple of the cycle lengths.

Proof Write $\sigma = \overset{\text{tau}}{\tau_1} \tau_2 \cdots \tau_m$ as disjoint cycles $\tau_1, \tau_2, \dots, \tau_m$.

Then $\sigma^k = (\tau_1 \tau_2 \cdots \tau_m)^k$

$= \tau_1^k \tau_2^k \cdots \tau_m^k$ because disjoint cycles commute

$\tau_i^k = \mathrm{Id}$ iff k is a multiple of the length of τ_i.

So $|\sigma|$ is the smallest positive integer which is a multiple of every cycle length. $\square$

Def A 2-cycle is also called a <u>transposition</u>.

Prop Every cycle is a product of transpositions.

Ex $(12345) = (12)(23)(34)(45)$
$(12345) = (15)(14)(13)(12)$
$(12345) = (15)(23)(14)(12)(23)(12)$

Proof Let $\sigma = (a_1 a_2 \dots a_k)$ be a k-cycle

Then $\sigma = (a_1 a_2)(a_2 a_3)(a_3 a_4) \cdots (a_{k-1} a_k)$

Since every $\sigma \in S_n$ is a product of cycles, every $\sigma \in S_n$ can be written as a product of transpositions

Note This product is not unique, as the example shows

Thm S_n is generated by transpositions

Thm Let $\sigma \in S_n$. Then either

* every expression of σ as a product of 2-cycles has an even number of 2-cycles
  (in this case, σ is called an <u>even</u> permutation)

OR

* every expression of σ as a product of 2-cycles has an odd number of 2-cycles
  (σ is called an <u>odd</u> permutation)

Whether σ is even or odd depends on the cycle type.

Ex $(12345) = (12)(23)(34)(45)$ is an even permutation

Ex The elts of S_4, by cycle type:

	cycle type	Types	permutations	count
Even	$(1,1,1,1)$		$Id = (1)(2)(3)(4)$	1
odd	$(2,1,1)$	2-cycles or "transpositions"	$(12), (13), \ldots, (34)$	6
Even	$(3,1)$	3-cycles	$(123), \ldots, (243)$	8
odd	(4)	4-cycles	$(1234), \ldots, (1432)$	6
Even	$(2,2)$	(2,2)-cycles	$(12)(34), (13)(24), (14)(23)$	3
			+	$24 = 4!$

Thm The set $A_n := \{\text{even permutations in } S_n\}$ is a subgroup of S_n.

(**Def** A_n is called the alternating group on $[n]$

Pf
- Id can be written as the product of 0 transpositions, so it's an even permutation.
- Closure: The product of two even permutations is also even.
- Inverse: If $\sigma \in A_n$ then σ can be written as a product $\sigma_1 \sigma_2 \cdots \sigma_r$ of transpositions where r is even.

  Then $\sigma^{-1} = \sigma_r \sigma_{r-1} \cdots \sigma_2 \sigma_1$

  so σ^{-1} is also in A_n.

Prop The number of even permutations in S_n $(n \geq 2)$ is equal to the number of odd permutations, so $|A_n| = \frac{n!}{2}$

Proof Let $B_n = \{\text{odd permutations in } S_n\}$

We will give a bijection from A_n to B_n.

Let $f: A_n \longrightarrow B_n$

$f(\sigma) = (12)\sigma$

To prove that f is injective, let $f(\sigma) = f(\pi)$.
sigma pi

Then $(12)\sigma = (12)\pi$

Multiply on the left by (12):

$(12)(12)\sigma = (12)(12)\pi$

$\sigma = \pi$.

To prove that f is surjective, let $\overset{\text{omega}}{\omega} \in B_n$.

Then ω can be expressed as $\omega = \omega_1 \cdots \omega_r$ where the ω_i are transpositions and r is odd.

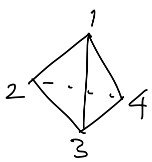
Then $(12)\omega$ is an even permutation and we have

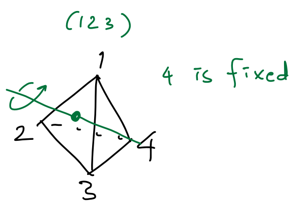
$f((12)\omega) = \omega$, as needed. $\square$

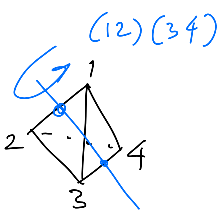
<u>Ex</u> A_4 has 12 elts

		count
Id	Id	1
3-cycles	Six of them	6
(2,2)-cycles	$(12)(34)$, $(13)(24)$, $(14)(23)$	3
		+

<u>Prop</u> The twelve rotations of a regular tetahedron can be described as elts of A_4.







<u>Remark</u> Many molecules w/ chemical formulas of the form AB_4, such as methane (CH_4) and carbon tetrachloride (CCI_4), have A_4 as their rotational symmetry group.

Motivation: Lagrange's Thm (order of a subgroup divides the order of the group)

Cosets (Sec 6.1) & Lagrange's Thm (Sec 6.2)

Warm-up: Given a subgroup H of a group, we can define an equivalence relation $\sim_L$ on G as follows:

$$x \sim_L y \quad \text{iff} \quad x^{-1}y \in H$$

(L stands for "left")

Ex: If $H = \{e\}$, then $x \sim_L y$ iff $x^{-1}y = e$ iff $x = y$,

So each equivalence class has exactly one elt.

If $H = G$, then $x \sim_L y$ for all $x, y \in G$,

so there is exactly one equivalence class, and it contains all elts of G.

In general, for a subgroup H, what are the equivalence classes corresponding to this equivalence relation $\sim_L$?

Answer: Given $g \in G$, the class $[g]_{\sim_L}$ containing g is

$$[g]_{\sim_L} = \{x \in G : g \sim_L x\}$$

$$= \{x \in G : g^{-1}x \in H\}$$

$= \{x \in G : g^{-1}x = h \text{ for some } h \in H\}$

$= \boxed{\{x \in G : x = gh \text{ for some } h \in H\}}$

A natural way to denote this equivalence class is gH

<u>Def</u> Let G be a group, H a subgroup, $g \in G$.

The <u>left coset</u> of H in G <u>containing g</u> (or <u>with representative g</u>) is

$$gH \overset{\text{def}}{=} \{gh : h \in H\}$$

Similarly, the <u>right coset of H containing g</u> is

$$Hg \overset{\text{def}}{=} \{hg : h \in H\}$$

<u>Note</u>: If G is abelian, $gH = Hg$.

<u>Thm</u> Let G be a group, H a subgroup. The left cosets of H in G partition G.

<u>Pf</u> The left cosets are equivalence classes for $\sim_L$,

$gH = [g]_{\sim_L}$. $\square$

<u>Note</u> $eH = H$ is the only coset which is a group

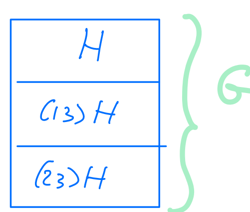
<u>Ex</u> $G = S_3$, $H = \langle (12) \rangle = \{ \mathrm{Id}, (12)\}$

<u>Left cosets of H in G:</u>

① $H = \{e, (12)\}$ $= eH = (12)H$

② $(13)H = \{(13), \underset{(123)}{\overset{(13)(12)}{\shortparallel}}\}$ $= (123)H$

③ $(23)H = \{(23), \underset{(132)}{\overset{(23)(12)}{\shortparallel}}\}$ $= (132)H$



Right cosets of H in G (different!)

① $H = \{e, (12)\}$ $= eH = (12)H$

② $H(13) = \{(13), (132)\}$ $= H(132)$

③ $H(23) = \{(23), (123)\}$ $= H(123)$

H	
$H(13)$	G
$H(23)$	

<u>Ex</u> $G = S_3$, $K = \langle (123) \rangle = \{e, (123), (132)\} = A_3 = \{\text{even permutations on } [n]\}$

Left cosets of K in G:

① $K = \{e, (123), (132)\}$ $= (123)K = (132)K$

② $(12)K = \{(12), \underset{(12)(123)}{\underset{\parallel}{(23)}}, \underset{(12)(132)}{\underset{\parallel}{(13)}}\} = (23)K = (13)K$

	K	
e	(123)	(132)
(12)	(23)	(13)

$(12)K$

Right cosets of K in G (the same!)

① $K = \{e, (123), (132)\}$ $= K(123) = K(132)$

② $K(12) = \{(12), (23), (13)\} = K(23) = K(13)$

	K	
e	(123)	(132)
(12)	(23)	(13)

$K(12)$

<u>Ex</u> $G = \mathbb{Z}$, $H = 4\mathbb{Z} = \{4k : k \in \mathbb{Z}\}$

Left (also right) cosets of H in G:

① $4\mathbb{Z}$ H $\ldots -8 \ -4 \ 0 \ 4 \ 8 \ \ldots$

② $1 + 4\mathbb{Z}$ $1+H$ $\ldots -7 \ -3 \ 1 \ 5 \ 9 \ \ldots$

③ $2 + 4\mathbb{Z}$ $2+H$ $\ldots -6 \ -2 \ 2 \ 6 \ 10 \ \ldots$

④ $3 + 4\mathbb{Z}$ $3+H$ $\ldots -5 \ -1 \ 3 \ 7 \ 11 \ \ldots$

All integers appear in my infinite array

Lemma (Book Lemma 6.3) Extra notes

Let G be a group, H a subgroup, and $a, b \in G$.
Then the following conditions are equivalent.

1. $aH = bH$
2. $Ha^{-1} = Hb^{-1}$
3. $aH \subset bH$
4. $b \in aH$
5. $a^{-1}b \in H$

Proof We prove 1 implies 2

Suppose $aH = bH$

First we will show $Ha^{-1} \subset Hb^{-1}$.

Let $x \in Ha^{-1}$! (Goal: show $x \in Hb^{-1}$)

Since $aH = bH$, we have $a = ae = bh_b$ for some $h_b \in H$.

Then $x = h_a a^{-1}$ for some $h_a \in H$ (since $x \in Ha^{-1}$)

$$= h_a (h_b^{-1} b^{-1}) \quad (\text{since } a = bh_b)$$

$$= (h_a h_b^{-1}) b^{-1}$$

$$\in Hb^{-1} \quad (\text{since } h_a h_b^{-1} \in H)$$

So $Ha^{-1} \subset Hb^{-1}$.

Exercise: prove that $Hb^{-1} \subset Ha^{-1}$ to finish the proof that 1 implies 2

---

① implies ③ by definition.

We prove that ③ implies ①:

Suppose $aH \subset bH$. (We need to show $bH \subset aH$.)

Let $x \in bH$. (Goal: show $x \in aH$.)

Since $aH \subset bH$, we have $a = ae = bh_1$ for some $h_1 \in H$.

So $ah_1^{-1} = b$

Then $x = bh_2$ for some $h_2 \in H$ (since $x \in bH$)

$= ah_1^{-1}h_2$ since $b = ah_1^{-1}$

$= a(h_1^{-1}h_2)$

$\in aH$ (since $h_1^{-1}h_2 \in H$)

We prove that ⑤ implies ④:

$a^{-1}b \in H$ $\quad$ $b \in aH$

Suppose $a^{-1}b \in H$.

Then $a^{-1}b = h$ for some $h \in H$

So $b = ah$, implying $b \in aH$.

Exercise: prove the rest. □

Def Let G be a group, H a subgroup.
The *index* of H in G, denoted $[G:H]$
is the number of left cosets of H in G.

Thm (Book Thm 6.8)
The number of left cosets of H in G is the same as the number of right cosets of H in G.

So $[G:H]$ is also the number of right cosets of H in G.

Proof
Define a map $f: \{\text{left cosets}\} \longrightarrow \{\text{right cosets}\}$
by $f: gH \longmapsto Hg^{-1}$
and we'll prove that it's a bijection.

* We need to check that this map is well-defined
(that is, we need to check that
$g_1H = g_2H$ implies $f(g_1H) = f(g_2H)$)
By Lemma 6.3, if $g_1H = g_2H$ then $Hg_1^{-1} = Hg_2^{-1}$ so $f(g_1H) = f(g_2H)$.

* To show that f is injective, suppose $f(g_1H) = f(g_2H)$.
Then $Hg_1^{-1} = Hg_2^{-1}$. By Lemma 6.3, we have $g_1H = g_2H$.

* The map is surjective since $f(g^{-1}H) = Hg$ $\square$

<u>Prop</u> (Book Prop 6.9)

Let G be a group, H a subgroup, $g \in G$. Then $|gH| = |H|$

<u>Proof</u>

Define a map $f: H \longrightarrow gH$

by $f: h \longmapsto gh$

and we'll prove that it's a bijection.

* To show that f is injective, suppose $f(h_1) = f(h_2)$.

Then $gh_1 = gh_2$. Multiplying by g^{-1} on the left gives us $h_1 = h_2$.

* The map is surjective since every elt of gH is of the form gh for some $h \in H$, and $gh = f(h)$. $\square$

By a similar argument, prove $|Hg| = |H|$

<u>Thm</u> (Lagrange) (Thm 6.10)

Let G be a finite group, H a subgroup.

Then $\frac{|G|}{|H|} = [G:H]$.

In particular, $|H|$ divides $|G|$.

<u>Pf</u> The group G is partitioned into $[G:H]$ distinct left cosets. Each left coset has $|H|$ elts. Hence $|G| = [G:H] \cdot H$ $\square$