Document last updated Tue, Sep 23, 2025

Abstract Algebra Notes

Day 3 Tue, 9/23/25

Outline

* Break before 8 pm

- Present HW
- Quiz 2
- Lecture: Ch 4 Cyclic groups
  Ch 5 Permutation groups
- Group activity: problems for next week's HW & quiz

TODO

Fri: TP 3 Overleaf
Next Tue: HW03 Due in class
Study for Quiz 3: Quiz @ start of class

Ch 4 Cyclic groups

Thm 4.1 Criterion for $a^i = a^j$

Let G be a group, and let $a \in G$.

1. If a has infinite order,

$$a^i = a^j \text{ iff } i = j$$

2. If a has finite order n, then:

(i) $\langle a \rangle = \{a, a^2, \ldots, a^{n-1}, e\}$

(ii) $a^i = a^j$ iff n divides $i - j$

Proof 1. If a has infinite order, then $a^n \neq e$ for all $n \in \mathbb{N}$.

$a^i = a^j$ iff $a^{i-j} = e$ iff $i - j = 0$

2. Assume $|a| = n$.

(i) We'll prove $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

We have $\{e, a, a^2, \ldots, a^{n-1}\} \subset \langle a \rangle$ by definition of $\langle a \rangle$.

To prove $\langle a \rangle \subset \{e, a, \ldots, a^{n-1}\}$,

suppose $a^k \in \langle a \rangle$.

There exists q, r such that

$k = qn + r$ with $0 \leq r < n$

(This is called the division algorithm)

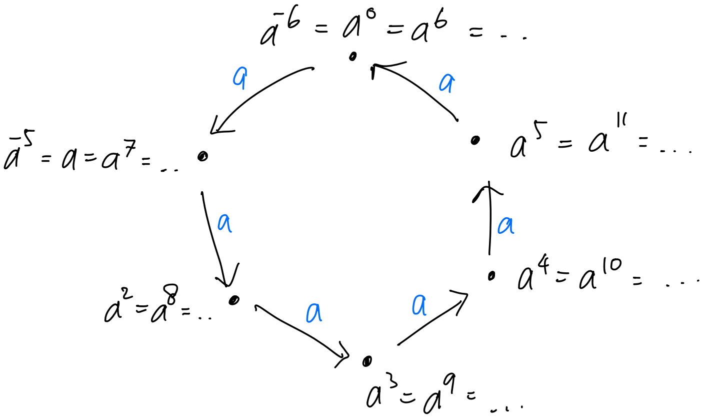
Then $a^k = a^{qn+r} = a^{qn} a^r = (a^n)^q a^r = e\, a^r = a^r$

Since $0 \leq r < n$, this shows $a^k \in \{e, a, \ldots, a^{n-1}\}$.
So $\langle a \rangle \subset \{e, a, \ldots, a^{n-1}\}$.

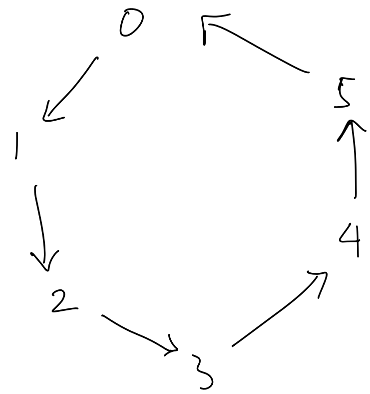
So the two sets are equal.

See proof of (2)(ii) in the book. $\boxtimes$

Cayley graph of $\langle a \rangle$ if $|a| = 6$



Cayley graph of $\mathbb{Z}_6 = \langle 1 \rangle$



Cayley graph of $\langle a \rangle$ if a has infinite order

$$\dots \leftarrow a^2 \xleftarrow{a} a \xleftarrow{a} e \xleftarrow{a} a^{-1} \leftarrow \dots$$

Cayley graph of $\mathbb{Z} = \langle 1 \rangle$

$$\dots 2 \leftarrow 1 \leftarrow 0 \leftarrow -2 \dots$$

Upshot of Thm 4.1: No matter what the group G is, or how the elt a is chosen, multiplication in $\langle a \rangle$ ...

* works the same as addition in $\mathbb{Z}_n$ if $|a| = n$:

  If $i + j \equiv k \bmod n$ then $a^i a^j = a^k$

* works the same as addition in $\mathbb{Z}$ if a has infinite order:

  $a^i a^j = a^{i+j}$ (and no modular arithmetic is done)

Corollary Let $a \in G$ be an elt of order n. Then $|a| = |\langle a \rangle|$

i.e., the order of a group element a is equal to the number of elts in the cyclic subgroup $\langle a \rangle$ generated by a.

Proof Part (2)(ii) of the above theorem says that $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$, so $|\langle a \rangle| = n$.

Corollary Let $a \in G$ be an elt of order n. If $a^k = e$ then n divides k.

Proof Since $a^k = e = a^0$, the above theorem tells us n divides $k - 0$. $\blacksquare$

Thm 4.2 Let $a \in G$ be an elt of order n.
Let k be a positive integer. Then we have:

1. $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

(Extra) 2. $|a^k| = \dfrac{n}{\gcd(n,k)}$

Ex Suppose $|a| = 30$

$\gcd(30, 17) = 1$, so $\langle a^{17} \rangle = \langle a^1 \rangle = \{e, a, a^2, \dots, a^{29}\}$

and $|a^{17}| = \frac{30}{1} = 30$

$\gcd(30, 18) = 6$, so $\langle a^{18} \rangle = \langle a^6 \rangle = \{e, a^6, a^{12}, a^{18}, a^{24}\}$

and $|a^{18}| = |a^6| = \frac{30}{6} = 5$

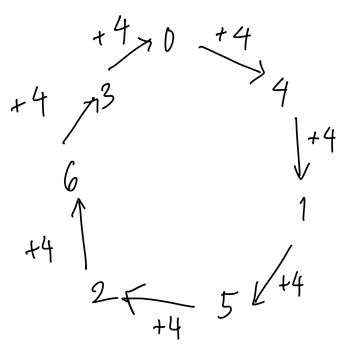
Cor An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff $\gcd(n,k) = 1$

Ex $\mathbb{Z}_7 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle$

$\mathbb{Z}_9 = \langle 1 \rangle = \langle 2 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 8 \rangle$

Cayley graph for $\mathbb{Z}_7$

$S = \{4\}$



Thm 43 <u>Thm</u> (1) Every subgroup of a cyclic group is cyclic.

(2) Suppose $|\langle a\rangle| = n$.

(i) The order of any subgroup of $\langle a\rangle$ is a divisor of n.

(ii) For each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k : $\langle a^{\frac{n}{k}}\rangle$

<u>Proof of (1):</u> (Extra)

Let $G = \langle x\rangle$ be a cyclic group w/ generator x.

Suppose H is a subgroup of G.

Case 1: H is the trivial subgroup $\{e\}$.

Then $H = \langle e\rangle$ is cyclic

Case 2: H is non trivial.

- So H contains some elt g not the identity.
- Then $g = x^n$ for some $n \in \mathbb{Z}_{\neq 0}$
- Since a subgroup is closed under taking inverses, $g^{-1} = x^{-n}$ must also be in H.
- Since either n or $-n$ is positive, H must contain some positive power of x.
- Let m be the smallest positive integer such that $x^m \in H$. (Such an m exists by the Principle of Well-ordering.)

- <u>Claim</u> $H = \langle x^m \rangle$

<u>Proof of claim</u>

- Since $x^m \in H$, we know $\langle x^m \rangle \leq H$ since by def $\langle x^m \rangle$ is the smallest subgroup of H containing x^m

- Next, we will prove $H \leq \langle x^m \rangle$:

Let $h \in H$. Since $H \leq G = \langle x \rangle$, we have $h = x^k$ for some $k \in \mathbb{Z}$

- By the division algorithm, there are $q, r \in \mathbb{Z}$ with $0 \leq r < m$ such that $k = mq + r$.
- Thus $h = x^k = x^{mq+r} = x^{mq} x^r$
- Multiply $x^k = x^{mq} x^r$ on the left by x^{-mq}:

$$x^{-mq} x^k = x^r$$

- So $x^r = x^{-mq} x^k = (x^m)^{-q} x^k$ is in H,

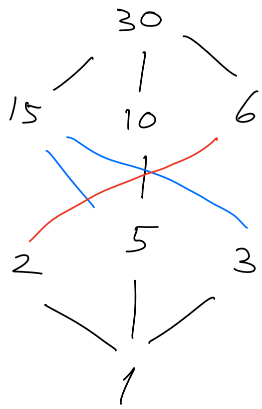
since $x^k = h \in H$ (by assumption) and $x^m \in H$ (by).

- We said earlier that m is the smallest positive integer such that $x^m \in H$.
- Since $0 \leq r < m$, we must have $r = 0$.
- Thus $k = mq$, and $h = x^k = x^{mq} = (x^m)^q \in \langle x^m \rangle$.
- This proves $H \leq \langle x^m \rangle$.

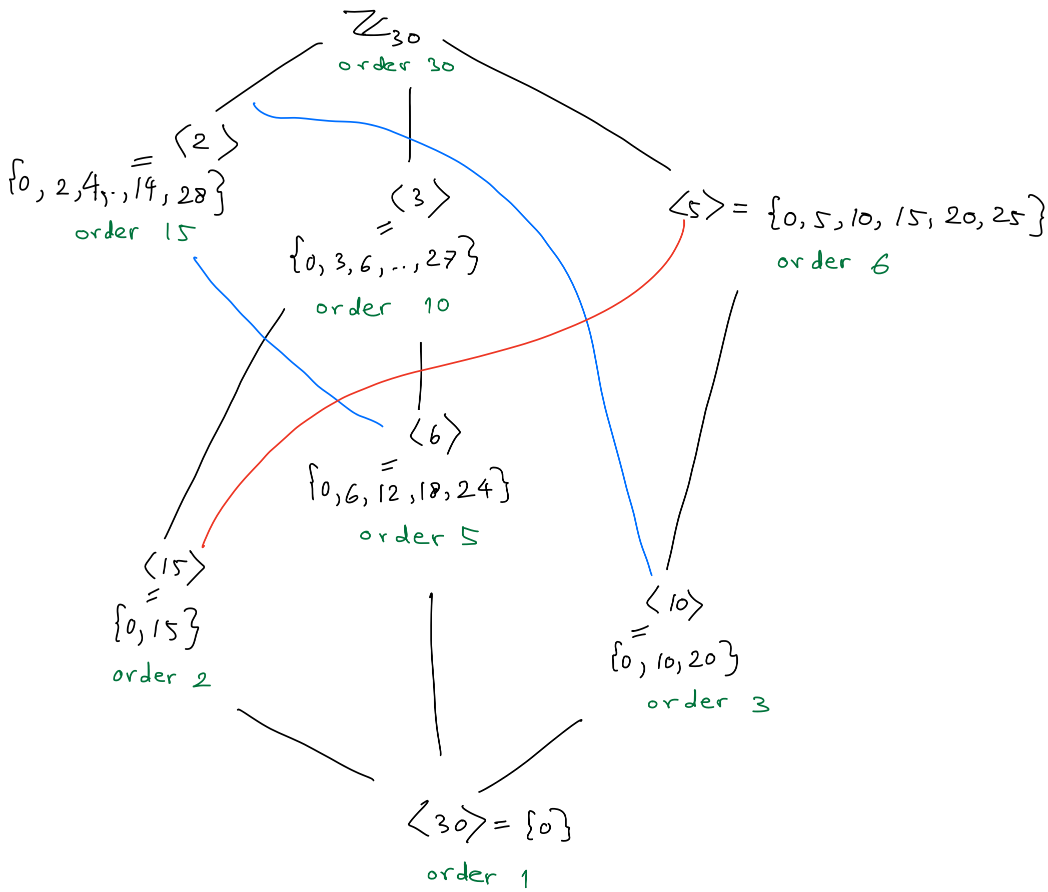
— the end of proof —

Cor For each positive divisor k of n, the set $\langle \frac{n}{k} \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k. These are the only subgroups of $\mathbb{Z}_n$.

Ex Lattice of divisors of 30:



Subgroup lattice for $\mathbb{Z}_{30}$:



Ch 5 Permutation groups

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 "isomorphic to" a subgroup of S_n (Cayley's Thm)

Notation: α in S_n can be written in two line notation

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \end{bmatrix}$$

Ex $\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$, $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} \in S_5$

\gamma \sigma

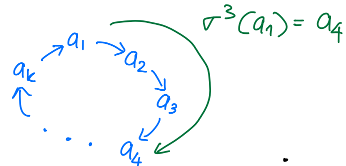
Read from right to left, like function composition:

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

$\underline{\text{Fact}}$ $|S_n| = n!$

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 $\sigma^i \neq \mathrm{Id}$

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

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 $\sigma = (1\,2\,6\,5)$ $\quad \pi = (1\,5\,6\,2)$ $\quad \sigma\pi = \mathrm{Id}$

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

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
$(1,1,1,1)$		$\mathrm{Id} = (1)(2)(3)(4)$	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 $\tau_1, \tau_2, \ldots, \tau_m$.

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 transposition.

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 $\sigma = (a_1 a_2 \ldots a_k)$ 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 $B_n = \{\text{odd permutations in } S_n\}$ (Extra)

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.

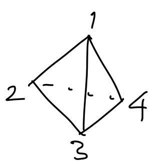
Then $(12)\omega$ is an even permutation and we have

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

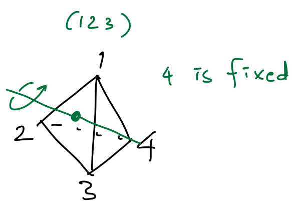
<u>Ex</u> A_4 has 12 elts

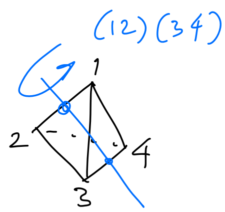
		count
Id	Id	1
3-cycles	Six of them	6
(2,2)-cycles	$(12)(34)$, $(13)(24)$, $(14)(23)$	3 +

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



(Extra)





<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.

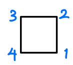
Additional examples

Ex: $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ can be viewed as the cyclic group $\langle \sigma \rangle$

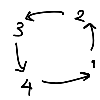
generated by $\sigma = (126)(45)$ or $\sigma = \underbrace{(132645)}_{\text{a 6-cycle}}$

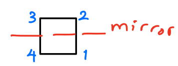
Ex: Symmetry$(\triangle) = D_3$ is S_3

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

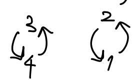
- Initial state: 

- 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 $\overset{\text{phi}}{\phi} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = (1\ 2)(34)$

  $=$ 

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