MATH 113 Review Sheet.

$*: S \times S \to S$ binary operations.
$(a, b) \mapsto a * b := *((a, b))$.

$H \subseteq S$, on which $*$ is defined.

H is closed under $*$
$\forall a, b \in H, \quad a * b \in H$

have no ambiguity
$a * b * c * d$
if associative
then the order "braces" DN matter

$*$ restricted to H is called the induced operation of $*$ on H.

$\forall a, b \in S, \quad a * b = b * a$ commutative.
$\dots, c \in S \quad (a * b) * c = a * (b * c)$ associative.
(composition of functions is associative).

$\langle S, * \rangle$ and $\langle S', *' \rangle$
isomorphism between 2 binary algebraic structure

if $x \leftrightarrow x' \wedge y \leftrightarrow y'$ + 1 to 1 correspondence
then $x * y \leftrightarrow x' *' y'$ between elements of S and that of S'.

s.t. $\langle S, * \rangle$ and $\langle S', *' \rangle$ are structurally alike

We customarily use the notion of bijective function to describe the isomorphism relation.

$\varphi : S \to S'$

$x \mapsto x' = \varphi(x)$.

Isomorphism: $\langle S, * \rangle, \langle S', *' \rangle$

isomorphism of S w/ S' is a 1-1 func. φ that maps S onto S' s.t.

$$\varphi(x * y) = \varphi(x) *' \varphi(y), \quad \forall x, y \in S.$$

homomorphism property.

"$S \simeq S'$"

★ To show two binary A.S. are not isomorphic, we may show that the two have some different structural property.

e.g. cardinality of S and S'.

commutativity: $a * b = b * a$ ↘ use homo. property to verify.

$x * x = x \quad \forall x \in S$

$a * x = b$ has one solution in $S \quad \forall a, b \in S$

Def. e: i.d. element $e * s = s * e = s$

$\forall s \in S$.

e uniqueness: $e = e * e' = e'$

$\varphi(e)$ is i.d. (preservation of id under iso.)

$\forall s' \in S$, WTS: $\varphi(e) *' s' = s' *' \varphi(e) = s'$

$$\underset{s' :=}{\varphi(s)} = \varphi(s * e) = \varphi(e * s)$$

$$\underset{s' :=}{\varphi(s)} *' \varphi(e) = \varphi(e) *' \underset{s' :=}{\varphi(s)}$$

φ is an isomorphism of $\langle S, * \rangle$ w/ $\langle S', *' \rangle$

$\Rightarrow \varphi^{-1}$ is an isomorphism of $\langle S', *' \rangle$ w/ $\langle S, * \rangle$

1-1 and onto follows obviously!

$$\varphi(\varphi^{-1}(a' *' b')) = a' *' b'$$

$$\varphi(\varphi^{-1}(a') * \varphi^{-1}(b')) = \varphi(\varphi^{-1}(a')) *' \varphi(\varphi^{-1}(b'))$$

$$= a' *' b'$$

φ is 1-1 gives us the result.

→ and we can then show "$\simeq$" is an equi. relation

Composition of isomorphisms work in the same way.

§4

Groups: $\langle G, * \rangle$ w/ 1) associativity

$$(a*b)*c = a*(b*c)$$

2) $\exists e$ s.t. $e*x = x*e = x$ (id. element)

3) $\forall a \in G$, $\exists a' \in G$ s.t. $a*a' = a'*a = e$ (inv)

(inv. a' of a)

if "$*$" is commutative, then G is abelian.

Left & Right Cancellation:

$a*b = a*c \Rightarrow b=c$, $b*a = c*a \Rightarrow b=c$

$$\Rightarrow \boxed{\begin{array}{c}(a'*a)*b = (a'*a)*c \\ b = c\end{array}}$$

WLOG!

Linear Eq. in a group has a unique sol.

$a*x = b$

$y*a = b$

x, y are unique in $\langle G, * \rangle$.

$(a'*a)*x = a'*b$ ⇒ $y = b*a'$

$x = a'*b$

x, y are unique ∵ e.g. $a * x_1 = a * x_2 = b$

then $x_1 = x_2$

by cancellation!

identity is unique as we have proven in binary op.

inverse is unique bc $\left.\begin{aligned} a'a = aa' = e \\ a''a = aa'' = e \end{aligned}\right\}$

$\Rightarrow aa' = aa'' \Rightarrow a' = a''$

inv of $(a*b)' = b' * a'$ by associativity and the fact that inv is unique.

semigroup: set w/ associative "$*$"

monoid: has identity.

The def. of group can be defined using right/left inv. only $\left(\begin{aligned} &\text{i.e. } x * e = x \quad \forall x \in G \\ &a * a' = e \quad \forall a \in G. \end{aligned}\right)$

Proof: 1. For $a * a = a$, $a = e_G$. (idempotence of e)

Since $a = ae = (aa)a^{-1} = aa^{-1} = e$

2. We show left inverse is also a^{-1}.

$$(a^{-1}a)(a^{-1}a) = a^{-1}ea = a^{-1}a$$

$$\therefore a^{-1}a = e$$

3. left identity is also e.

$$ea = (aa^{-1})a = ae = a$$

Table for Finite Groups:

$*$	e
e	e

$*$	e	a
e	e	a
a	a	e

left $*$ right

$\langle \mathbb{Z}_2, +_2 \rangle$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$\langle \mathbb{Z}_3, +_3 \rangle$

Note that from the "linear equation" theorem, every element of G must appear in each row and col only once.

$\therefore ax = b$ and $ya = b$ have unique solutions.

	b_1	b_2
a	x_1	x_2

"There is only one group of 1/2/3 elements, up to isomorphism."

For finite group of order 4,

we have $\langle \mathbb{Z}_4, +_4 \rangle$ and Klein-4.

$\mathbb{Z}_4$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

V:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Rmk: As you might have noticed already, we follow the convention of using "$\cdot$" for general binary operations, and "$+$" for designated commutative operations.
but we will keep using e as the identity element.

a^{-1}: inverse of a.

$a^0 := e$, $a^{-n} := \underbrace{a^{-1} a^{-1} \cdots a^{-1}}_{n \in \mathbb{Z}^+}$, $a^n = \underbrace{a \cdots a}_{n \in \mathbb{Z}^+}$

add: $(0a)$ $(-n)a$ (na)

Law of exponents

$a^{m+n} = a^m a^n$ hold for $m, n \in \mathbb{Z}$.

by associativity.

order: $|G|$.

$H \subseteq G$ closed under binary operation of G. If H w/ induced operation from G forms a group, then H is a subgroup of G. $H \leq G$.

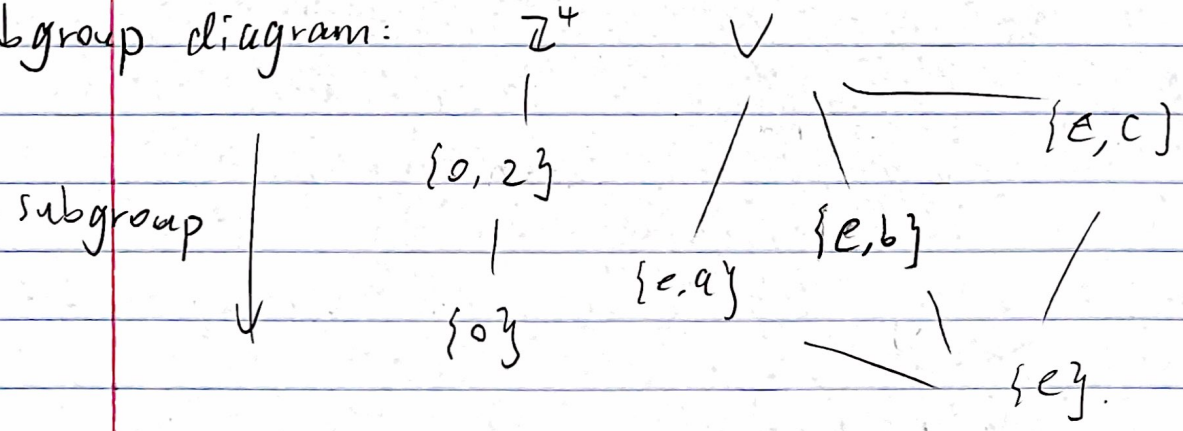
For $H \subsetneq G$, then $H < G$. proper subgroup.

$\{e\}$ and G are subgroups of G.

trivial subgroup

improper subgroup.

Subgroup diagram:



The criterion for subgroup is similar to the criterion for vector subspace. Proof is omitted here.

iff ① H is closed under the binary operation of G.

Rmk. when finding all elements of a finite cyclic group, we only need to list $a^0 = e \sim a^{m-1}$. We will talk about this later.

② $id_G \in H$.

③ $\forall a \in H \Rightarrow a^{-1} \in H$

(for the $\Leftarrow$ direction associativity holds by considering elements in H as elements in G)

cyclic subgroups

for $a \in H$, a^n, a^0, a^{-n} $(n \in \mathbb{Z}^+)$ must all contain in H. (a^0: id., a^{-n}: inv.)

(closed under binary operation)

Thm:

$a \in G$, then $H := \{a^n \mid n \in \mathbb{Z}\} \leq G$ is the smallest subgroup of G containing a. (similar to VS as well)

(∵ the three criterions automatically satisfied, ∴ $H \leq G$)

(∵ the existence of element "a" implies all powers of "a" must be contained in any subgroup containing "a")

∴ the smallest.

$\langle a \rangle :=$

Def. $\{a^n \mid n \in \mathbb{Z}\}$ for $a \in G$ is the cyclic subgroup of G generated by a.

$a \in G$ generates G if $\langle a \rangle = G$. a is called a generator.

A group is cyclic if $\exists\, a \in G$ s.t. $G = \langle a \rangle$.

* $\langle \mathbb{Z}, + \rangle$ is a cyclic group, the only generators of which are $\langle 1 \rangle$ and $\langle -1 \rangle$.

$\langle \mathbb{Z}_n, +_n \rangle$ is also cyclic, and $\langle 1 \rangle$ and $\langle n-1 \rangle$ are always generators.

For the set of n-th roots of unity in $\mathbb{C}$, $\langle U_n, \cdot \rangle$ is a cyclic group generated by $\zeta = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$

It is a cyclic subgroup of $\langle U, \cdot \rangle$ of all complex number z w/ norm 1.

§6. Cyclic Groups

* (Order of an element) × order of a group

$\langle a \rangle \leq G$ is a finite group, we say order of a is $|\langle a \rangle|$. If it is an infinite group,

then $\langle a \rangle$ is of infinite order.

Properties of cyclic groups:

1. every cyclic group is abelian.

consider $g_1, g_2 \in \langle a \rangle$.

$\exists$ r.s. s.t. $g_1 = a^r$, $g_2 = a^s$.

$$g_1 g_2 = a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r = g_2 g_1$$

(associativity)

Recall the division algorithm for $\mathbb{Z}$.

for $m \in \mathbb{Z}^+$, $n \in \mathbb{Z}$. $\exists !$ q and $0 \leq r < m$.

s.t. $n = mq + r$.

Thm: $H \leq G$, if G is cyclic, then H is cyclic.

This can be shown by gcd or by the division algorithm.

Following the book, we first prove this thm w/ division algorithm, with this thm, we define gcd w/ generators.

$G = \langle a \rangle$.

Proof If $H = \{e\}$, $H = \langle e \rangle$ is cyclic.
If $H \neq \{e\}$, $a^n \in H$, for some $n \in \mathbb{Z}^+$
(since $n \in \mathbb{Z}^-$ would mean $a^{-n} \in \mathbb{Z}^+$, we only need to consider $\mathbb{Z}^+$).

Let m = smallest positive integer s.t. $a^m \in H$.

Claim: $c = a^m$ generates H

i.e., $H = \langle a^m \rangle = \langle c \rangle$.

$\forall b \in H$, $b = a^n$ $(n \in \mathbb{Z})$.

$n = mq + r$. for $0 \leq r < m$

$a^r = \underbrace{(a^m)^{-q}}_{\in H} \underbrace{a^n}_{\in H} \in H$ $\therefore r = 0$, and $b = \underbrace{\text{power of } c}_{\in H}$.

□.

Cor. Since $n\mathbb{Z}$ $(n \in \mathbb{Z}^+)$ are all cyclic subgroups of $\langle \mathbb{Z}, + \rangle$. ($\forall$ generators from all integers).

$n\mathbb{Z}$ are the only subgroups of $\langle \mathbb{Z}, + \rangle$

Consider

Def $H = \{nr + ms \mid n, m \in \mathbb{Z}\} \leq \langle \mathbb{Z}, + \rangle$.

$\therefore$ H must be cyclic w/ generator d, which we restrict to positive here.

First, $d \mid r, s$ since $r, s \in H$.

and $d = nr + ms$ for some n and m.

$\gcd(r,s) \mid r, s \Rightarrow \gcd(r,s) \mid nr + ms \Rightarrow \gcd(r,s) \mid d$.

since $d \mid r, s$, $d = \gcd(r,s)$, which proves Bezout's identity that we are familiar with.

* It is possible to describe all the cyclic groups up to isomorphisms.

$G = \langle a \rangle$, if $|G| = \infty$, then $G \simeq \langle \mathbb{Z}, + \rangle$

$|G| < \infty$, then $G \simeq \langle \mathbb{Z}_n, +_n \rangle$.

First Lemma: cyclic infinite order group $\Leftrightarrow \forall m \in \mathbb{Z}^+$, $a^m \neq e$.

$\Rightarrow$ $\exists a^m = e$ means repetitions beyond $a^0, a^1 \ldots a^{m-1}$ are all the elements distinct (one can use division algo. to prove this)

$\Leftarrow$: no 2 powers of a can be the same.

$\therefore$ infinite order.

infinite order cyclic group $\sim \langle \mathbb{Z}, + \rangle$.

when $i \neq j$.
since no $a^n = a^j$

$\varphi(a^i) = i$ well-defined: 1-1 and onto $\mathbb{Z}$.

$\varphi(a^i a^j) = \varphi(a^{i+j}) = i+j = \varphi(a^i) + \varphi(a^j)$

$\therefore \varphi$ is an isomorphism of cyclic/infinite-order G w/ $\langle \mathbb{Z}, + \rangle$.

finite order cyclic group $\sim (\mathbb{Z}_n, +_n)$.

Choose the smallest n s.t. $a^n = e$.

then $e = a^0 \sim a^{n-1}$ are all elements distinct by division algorithm and "smallest".

$\therefore \psi : G \to \mathbb{Z}_n$ by $\psi(a^i) = i$ for $i = 0 \sim n-1$ is well-defined, 1-1, and onto $\mathbb{Z}_n$.

$\because a^n = e$, $a^i a^j = a^k$ as $i +_n j = k$.

$\therefore \psi(a^i a^j) = i +_n j = \psi(a^i) +_n \psi(a^j)$.

$= \langle a \rangle$

Thm. G be cyclic w/ n elements, generated by a.

Let $b = a^s \in G$. then [i] b generates a cyclic subgroup $H \leq G$ containing $n/\gcd(n,s)$ elements. Also,

[ii] $\langle a^s \rangle = \langle a^t \rangle$ iff $\gcd(s,n) = \gcd(t,n)$.

Proof. b generates $H \leq G$, since $\forall\, b \in G$, $\{b^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.

WTS: $\frac{n}{\gcd(n,s)}$ is the smallest power of $a^s = b$ to let it be e.

consider $(a^s)^m = e$ iff $n \mid sm$

$\therefore$ smallest power $m = n/\gcd(n,s)$.

— — — — —

Consider $\mathbb{Z}_n$ for ease of discussion.

if $d \mid n$, then $\langle d \rangle$ is of order n/d.

and contains all m s.t. $\gcd(m,n) = d$.

(these m also generate a cyclic group).

Thus, ∃! cyclic subgroup of order n/d

$\leq$ cyclic G of order n.

$\langle a^s \rangle = \langle a^t \rangle \Rightarrow \gcd(s,n) = \gcd(t,n)$

∴ their orders are the same

$\langle a^s \rangle = \langle a^t \rangle \Leftarrow \gcd(s,n) = \gcd(t,n)$

∴ there is only one cyclic subgroup of order n/d.

Cor. from (i) when $\gcd(n,r)=1$., given $\langle a \rangle = G$

the subgroup is the group itself. because the order is the same.

∴ all other generators are $\langle a^r \rangle$, where

$\gcd(n,r)=1$.

§7. Generating sets and Cayley Digraphs.

For $S = \{a, b, \ldots\}$ finite or infinite

Consider the subgroup generated by elements in this

closed (products still are products)

since $e = a^0 = b^0 = \cdots$ (identity of the same type)

$(a^2 b^4 a^{-3} b^2 a^5)^{-1} = a^{-5} b^{-2} a^3 b^{-4} a^{-2}$ (inverse)

$\therefore$ the finite products of powers of elements in S form a subgroup of G.

The elements of S are the generators of this subgroup. If S is finite, and generates G: finitely generated.

e.g. for $V = \{a, b, c, e\}$, $\{a,b\}$ $\{a,c\}$ $\{b,c\}$ $\{a,b,c\}$ are all generating sets of V.

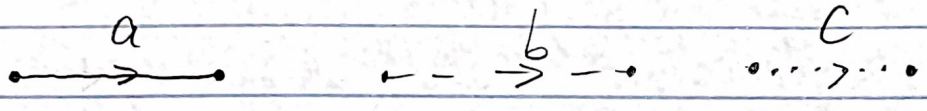
S generates $G \Rightarrow$ superset of S generates G.

Similar to VS: arbitrary intersection of some / open sets subgroups $H_i \leq G$ is again a subgroup of G.

check closure, identity, inverse condition

(directed graph)

Cayley Digraphs:



different lines to represent the right-multiplication by the generator.

$xa = y$

or $ya^{-1} = x$

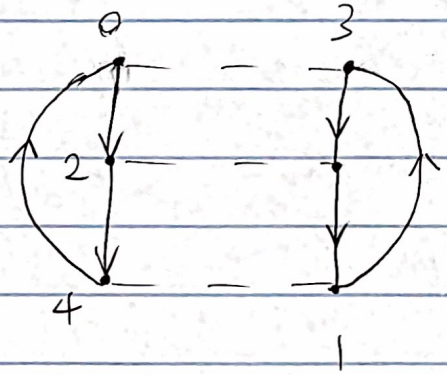
(because we are in a group)

if $a = a^{-1}$

then $xa = y$, $ya = x$

thus ">" is omitted.

For $\mathbb{Z}_6$ w/ $S = \{2, 3\}$



Cayley Digraph: Each node g has exactly one edge of each type starting at g. $(ga, gb, \dots)$

and ending at g $(ga^{-1}, gb^{-1}, \dots)$

The digraph is connected: because $gx = h$, and x can be expressed as a finite product of generators $a, b, \ldots$

(thus we follow the sequence of a's and b's to find the path connecting g and h).

At most one edge can connect a node and another (because solution is unique).

If $gq = h$ and $gr = h$, then $\forall u \in G$,

$ug = ug^{-1}h = ur$

q, r both lead from g to h.

$\Downarrow$

starting from any u, led to the same v under the same seqs.

We may show:

Every digraph w/ these four properties is a Cayley digraph for some group.

(because of symmetry, we can select any node as the identity e).

§8. Groups of Permutations:

Def. A permutation of a set A is a func. $\varphi: A \to A$ that is bijective.

"$\circ$" is a binary operation on the collection of all permutations of a set A.

Since the composition of two permutations (bijective functions) is still bijective (permutation)

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

To further show that S_A, the set of all permutations on A, is a group under "$\circ$", permutation multiplication

We check associativity, identity, and inverse.

func. comp. is associative.

id permutation: $\iota(a) = a. \quad \forall a \in A.$

inverse: bijective func. has a unique inverse.

We may take $A = \{1, 2, \cdots, n\}$ as the prototype for a finite set B of n element.

Then we can construct a bijection f between A and B. And then for

$$\begin{pmatrix} 1 & 2 & 3 \\ ? & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} f(1) & f(2) & f(3) \\ f(3) & f(2) & f(1) \end{pmatrix}.$$

$$\sigma \xrightarrow{\varphi} \tau := \varphi(\sigma)$$

s.t. $\tau(f(a)) = f(\sigma(a))$.

1-1 and onto

isomorphic w/ the prototype.

S_n: symmetric group on n letters

(all permutations of $[n] := \{1, 2, \cdots, n\}$).

$|S_n| = n!$

S_3: $\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\rightarrow$ rotate 1

$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\rightarrow$ rotate 2.

fix 1 and flip

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$*$

$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$*$

fix 2 and flip

fix 3 and flip.

$$\mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$*$

If we draw the group table for $\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3$, then

We can see that the group is not abelian.

In fact, groups of order ≤ 5 are all non-abelian.

$\therefore |S_3| = 6$ has minimum order for any non-abelian group.

n-th dihedral group D_n: the group of symmetries of regular n-gon.

$D_3 = S_3$ in particular.

$|D_n| = 2n$. because  e.g. "1" "2" "3" can take

$= 3$

: n) positions, and whether the order of the vertices are CCW or CW gives us $2n$ elements.

D_4 : octic group

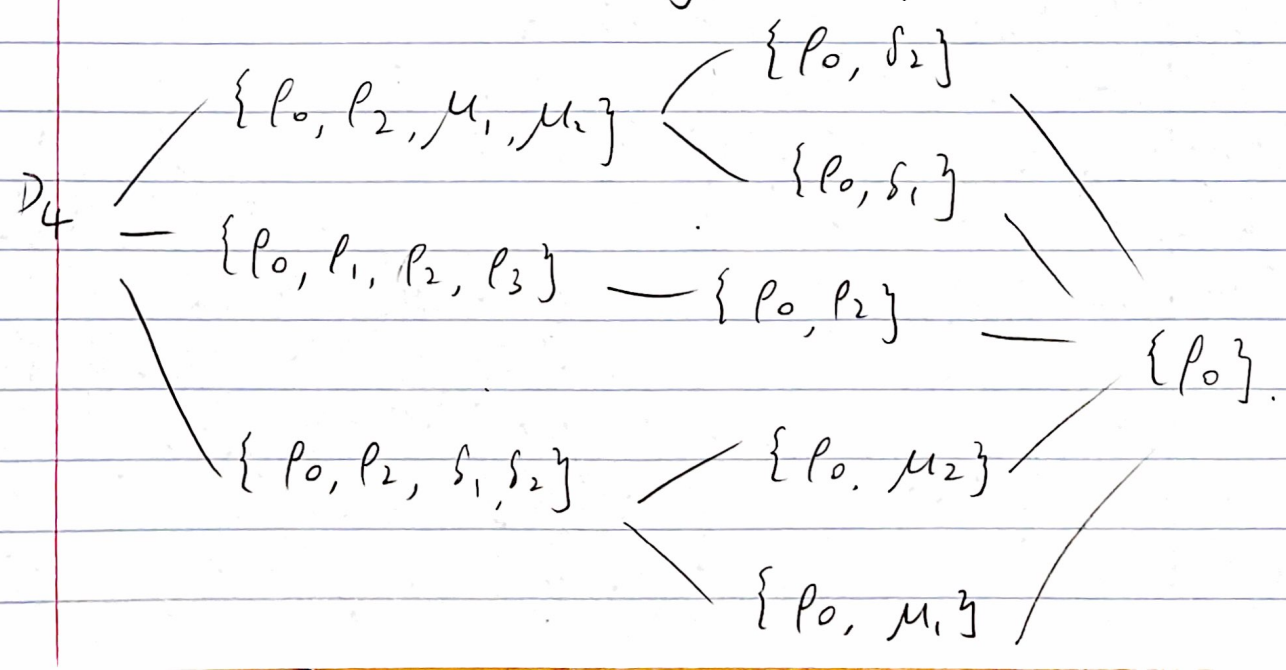
$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \qquad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

, diagonal flip.



(finite/infinite)

Cayley's thm: every group $\simeq$ some group consisting of permutations under "$\circ$"

Lemma: For G and G' be groups and let $\varphi: G \to G'$ be 1-1 s.t. $\varphi(xy) = \varphi(x)\varphi(y)$.

$\forall x, y \in G$. Then $\varphi(G)$ is a subgroup of G' and φ is an isomorphism of G w/ $\varphi(G)$.

Proof: $\varphi(G)$ is a subgroup $\Rightarrow$ φ is a 1-1 and onto $\varphi(G)$ (thus isomorphism)

Closed: $\forall x', y' \in \varphi(G)$, $x, y \in G$ s.t. $\varphi(x) = x'$, $\varphi(y) = y'$

(injective)

$\varphi(xy) = \varphi(x)\varphi(y) = x'y' \in \varphi(G)$.

identity: $e'\varphi(e) = \varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$

$\Rightarrow e' = \varphi(e) \in \varphi(G)$.

inverse: $x' \in \varphi(G)$. $x' = \varphi(x)$

$e' = \varphi(e) = \varphi(x)\varphi(x^{-1}) = x'\varphi(x^{-1})$.

Cayley's Thm Proof: ↓ subgroup of S_G.

We want essentially $G \simeq S \leq S_G$

it suffices to define $\varphi(xy) = \varphi(x)\varphi(y)$ $\boxed{\forall x, y \in G}$

Define left-multiplication map $\lambda_x : G \to G$.

$$\lambda_x(g) = xg.$$

$\forall g \in G$.

λ_x is 1-1 and onto, quite clearly.

$\forall b \in G$, $\exists!\ a = x^{-1}b$ s.t. $\lambda_x(a) = b$.

the fact that λ_x is a permutation * — list as $(\cdots)$ gives us

the $\varphi : G \to S_G$ needed by $\varphi(x) = \lambda_x$ $(x \in G)$

φ 1-1: $\varphi(x) = \varphi(y) \Leftrightarrow \lambda_x = \lambda_y \Rightarrow \lambda_x(e) = \lambda_y(e)$

$\Rightarrow xe = ye \Rightarrow x = y$.

$\varphi(x)\varphi(y) = \varphi(xy) \Rightarrow \lambda_{xy} = \lambda_x \lambda_y$

$\forall g \quad \lambda_{xy}(g) = (xy)g$

and $(\lambda_x \lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg)$

Associativity $\Rightarrow \lambda_{xy} = \lambda_x \lambda_y$.

Rmk. similarly one can take $\rho_x(g) = gx$ (right-multiplication map) and let the one-to-one map be $\mu(x) = \rho_{x^{-1}}$

Def: $\varphi(x) = \lambda_x$ is called the left regular representation
$\mu(x) = \rho_{x^{-1}}$ right regular representation

Because of the preservation of structure under isomorphism $\varphi(x) = \lambda_x$.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$\longmapsto$

λ_e	λ_a	λ_b	
λ_e	λ_e	λ_a	λ_b
λ_a	λ_a	λ_b	λ_e
λ_b	λ_b	λ_e	λ_a

Rmk: from the proof, we see why any group is $\cong$ to a group of permutations. The rows / cols representing left/right multiplication are permutations themselves of the elements of G.

and what are doing is constructing a map 1-1 from $x \mapsto \lambda_x$, the left-multiplication permutation.

An implication of this thm: counterexample for conjectures in group theory could always be found in some group of permutations.

§9. Orbits, cycles, and A_n.

$\mathcal{O}_{a,\sigma} = \{\sigma^n(a) \mid n \in \mathbb{Z}\}$ is the orbit of a under $\sigma \in S_A$.

The orbit of an element is an equivalence class.

say $a \sim b$ if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$

$a \sim a$ ✓.

$a \sim b \Rightarrow b \sim a$ ✓

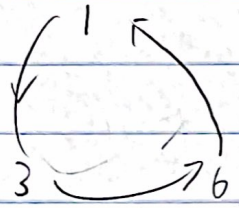
$a \sim b$, $b \sim c \Rightarrow a \sim c$ ✓.

All the equivalence classes in A determined by $\sim$ are the orbits of σ.

The orbits of ι_A are the singleton subsets of A.

Now we restrict to finite S_n.

Each equivalence class gives a circle of elements

e.g. 

(because the order is finite, $\sigma^m(a) = a$, for some $1 \le m \le n$.)

which corresponds to

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

$\sigma \in S_n$ **Cycle** if σ has at most one orbit with more than 1 element. Length = max length among the orbits

Thm Every permutation is a product of disjoint cycles.

For $B_1, B_2, \dots, B_r$ orbits of σ.

$$\mu_i(x) := \begin{cases} \sigma(x) & x \in B_i \\ x & x \notin B_i \end{cases}$$

thus defining a cycle permutation corresponding to orbits.

$\sigma = \mu_1 \mu_2 \dots \mu_r$ as a result.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 4 & 1 \end{pmatrix} = (136)(45)(2)$$ omitted : does not change.

And all of the cycles are disjoint

(Note that multiplications of disjoint cycles are commutative)

The orbits of a permutation are unique, so the representation of a permutation as a product of disjoint cycles (excluding the identity permutation) is unique (up to the order of the factors).

Any cycle is a product of transpositions (cycles of length 2)

$(a_1, a_2, \cdots, a_n) = (a_1, a_n) \cdots (a_1, a_2)$

$\Rightarrow$ Any permutation of a finite set with size ≥ 2 is a product of transpositions.

S_n $(n \geq 2)$, $L = (1,2)(1,2)$, e.g.

Thm. The no. of transpositions used to represent a fixed permutation must be always even / odd.

No permutation can be expressed as a product of both even and odd no. of transpositions.

Classical Proof: $\begin{matrix}1\\2\\3\\\vdots\\n\end{matrix}$ $\simeq$ the rows of I_n

w/ det

transposition ↓ transposition

(interchange 2 elements) interchange 2 rows (changing the sgn of the det)

$\therefore$ for $\sigma \in S_n$, we have $\overline{\sigma}$ corresp. for rows of I_n

the matrix with rows after the permutation $\overline{\sigma}$ have
det 1 iff even transp.
-1 iff odd $\sim$.

One could also count the orbits and see σ and $\overline{\tau}\sigma$ (where $\overline{\tau}$ is a transposition in S_n) differ by 1.
See §9 of the book.

Def.

even permutation — even # of transp.
odd — odd # of transp.

Alternating groups: $|\text{even permutations of } S_n|$

$(n \geq 2)$ $= |\text{odd permutations of } S_n| = n!/2$.

even odd

To show A_n and B_n have the same size, we construct a bijection between these two sets.

Let τ be a fixed transposition in S_n. $(n \geq 2)$
(e.g. $\tau = (1,2)$).

$\lambda_\tau : A_n \to B_n$ is given by the left-multiplication

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

$\sigma \in A_n$, $\tau\sigma \in B_n$

even $+1$ = odd

1-1: $\tau\sigma = \tau\mu \Rightarrow \sigma = \mu$

onto: $\tau = \tau^{-1} = (1,2)$ e.g.

then $\tau^{-1}\rho \in A_n$ if $\rho \in B_n$

and $\lambda_\tau(\tau^{-1}\rho) = \rho$.

$\therefore |A_n| = |B_n|$

Note:

closed: even permutation · even permutation = even permutation

odd odd odd

odd/even even/odd even

$|A_n|$: $n \geq 2$ $(1,2) \in S_n$ and ι is thus even

$= (1,2)(1,2)$

inv: If σ is even, then σ^{-1} is even/odd.
odd

(since $\sigma = \sigma_1 \sigma_2 \sigma_3$, then $\sigma^{-1} = \sigma_3^{-1} \sigma_2^{-1} \sigma_1^{-1}$)

$\therefore$ no. of transp. are the same.

> if σ can be expressed even/odd
> $\Rightarrow$ must be ~

We now have: closed, $\exists$ id, and inverse.

$\therefore$ A_n is a subgroup of order $n!/2$ of S_n.
($n \geq 2$)

Def. alternating group A_n on n letters consisting of even permutations.

Rmk from HW: the order of a permutation is the lcm of the cycle permutation it is divided into.

order 2, order 3

$\sigma \in S_8$ $\sigma = (1\,2)(4\,5\,7)$

$\text{lcm}(2,3) = 6$

order of σ

§10

Cosets and Lagrange Theorem.

order of a subgroup $\leq$ finite group divides the whole group

How? We use the notion of cosets.

$\sim_L$ and $\sim_R$ on G are defined as follows, given a subgroup $H \leq G$ (G can be either finite or infinite).

$a \sim_L b$ if $a^{-1}b \in H$

$a \sim_R b$ if $ab^{-1} \in H$.

Equivalence relation: $a \sim_L a$ $\because (a^{-1})a = e \in H$.

$a \sim_L b$

then $a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1}$

$= b^{-1}a \in H$

$\therefore b \sim_L a$.

$a \sim_L b$ and $b \sim_L c$

$\Rightarrow a^{-1}b \in H \wedge b^{-1}c \in H$

$\Rightarrow a^{-1}c \in H$. ✓

same for $\sim_R$.

Consider the set of x's in the same class as a

i.e., $a \sim_L x$

$a^{-1}x \in H$

$x = ah$ for some $h \in H$

(thus denoted by aH)

for $\sim_R$, it would be "Ha" instead

aH and Ha are not necessarily the same,

but for abelian group G, $aH = Ha$ obviously.

aH : left coset of H containing a

Ha right

and the partition of G into left and right cosets are the same.

Eg. Consider $n\mathbb{Z} < \mathbb{Z}$ the (left) cosets of $n\mathbb{Z}$ under "$+$" are the residue classes of $\mathbb{Z}$ mod n.

For $a \in \mathbb{Z}$, consider "$a + n\mathbb{Z}$"

(Since $\langle \mathbb{Z}, + \rangle$ is abelian, the left and right cosets are the same, and are called the cosets mod $n\mathbb{Z}$).

Lagrange theorem

$H \leq G$. every left and right coset have the same "number" of elements as H.

For fixed g, we show $\varphi_g : H \to gH$ is bijective.

which is quite obvious

onto ✓. 1-1: $g(h_1) = g(h_2) \Rightarrow h_1 = h_2$

by cancelation law

$\forall g \in G, |gH| = |H| = |Hg|$

This leads directly to the Lagrange theorem.

$H \leq G$ w/ $|G| < \infty$, then $|H| \mid |G|$.

set $m = |H|$, $n = |G|$.

the no. of left cosets $r < \infty$, since $n < \infty$.

∵ every left cosets have m element

$n = m \cdot r \Rightarrow m \mid n$.

Cor: *** Every group of prime order is cyclic.

$|G| = p$, let $a \neq e_G$.

$\langle a \rangle$ has order ≥ 2, yet $\text{ord}\,|\, p \Rightarrow |\langle a \rangle| = p$.

$\Rightarrow \langle a \rangle = G$

$\therefore G$ is cyclic.

G of prime order p is a cyclic group of order p $\simeq \mathbb{Z}_p$.

$\therefore$ there is one group structure, up to isomorphism of a given prime order p.

Cor 2: the order of an element of a finite group divides the order of the whole group.

Def. $H \leq G$, # of left cosets of H in G is the index $(G:H)$ of H in G.

Thm. Suppose $K \leq H \leq G$, and $(H:K), (G:H) < \infty$, then $(G:K) = (G:H)(H:K) < \infty$.

Proof: