based on Fraleigh

MATH 113 Review Sheet on Group Theory

$* : S \times S \to S$ 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.
$\ldots, c \in S \quad (a*b)*c = a*(b*c)$ 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: $\varphi(e) *' s' = s' *' \varphi(e) = s'$

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

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

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 $\langle G, * \rangle$.

$(a'*a)*x = a'*b$ $\quad y = b*a'$

$x = a'*b$

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 $\left(\text{i.e. } \begin{aligned} x * e &= x \quad \forall x \in G \\ a * a' &= e \quad \forall a \in G. \end{aligned}\right)$

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

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

these tell us that if we want to show a set endowed b. with "$*$" is a group, check associativity, left/right id. and left/right inv.

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

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

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

and also closed

one do not need both sides.

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 "·" 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) (-na) (na)

Law of exponents

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

by associativity.

order: $|G|$.

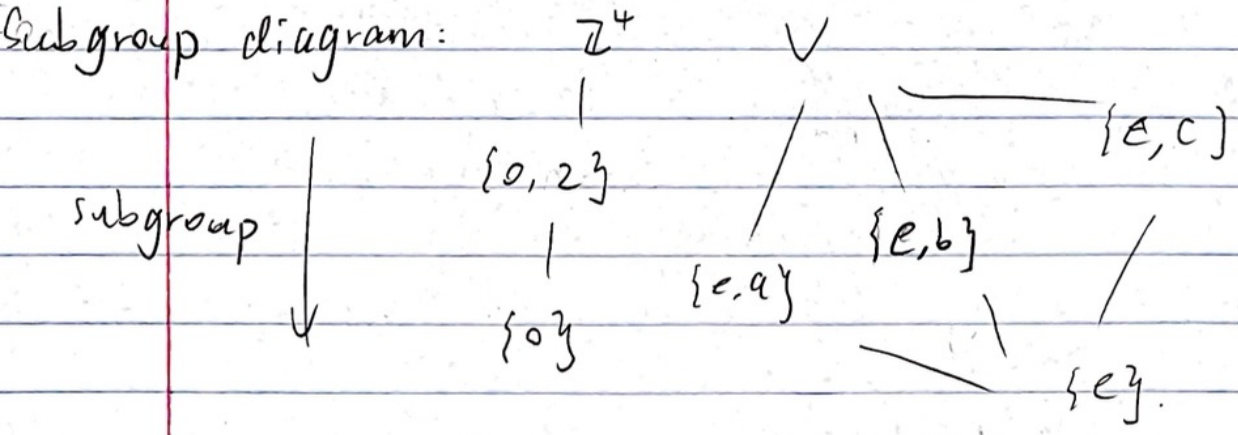
$H \subseteq G$ closed under binary operation of G. If H w/ induced operation from G forms a group, then H is a subgroup of G. $H \leq G$.

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 $0 \le r < m$.

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

Thm: $H \le G$, 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 $b = \text{power-of } c$.

$\in H$

□.

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

Cor. $n\mathbb{Z}$ 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 $\forall\, b \in G$, proved before

$\{b^n \mid n \in \mathbb{Z}\}$ 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 of order n/d).

Thus, $\exists!$ cyclic subgroup of order n/d

$\leq$ cyclic G of order n.

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

$\therefore$ their orders are the same

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

$\therefore$ 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.

$\therefore$ 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.

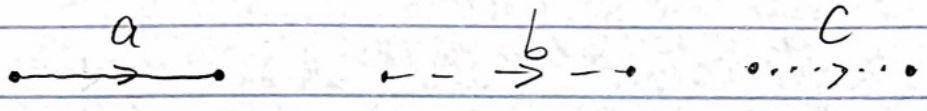
S generates $G \Rightarrow$ superset of S generates G.

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 $ya^{-1} = x$

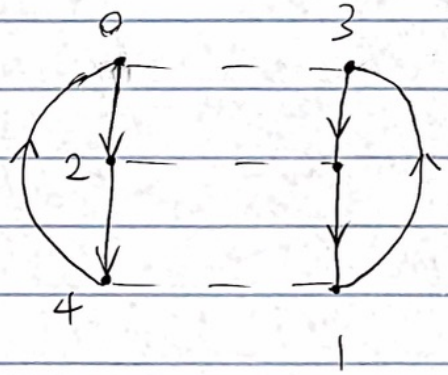
(because we are in a group)

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 groups.

(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: $\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

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

$\rightarrow$ rotate 2.

$\rightarrow$ rotate 1

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.

$\because |S_3| = 6$ 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

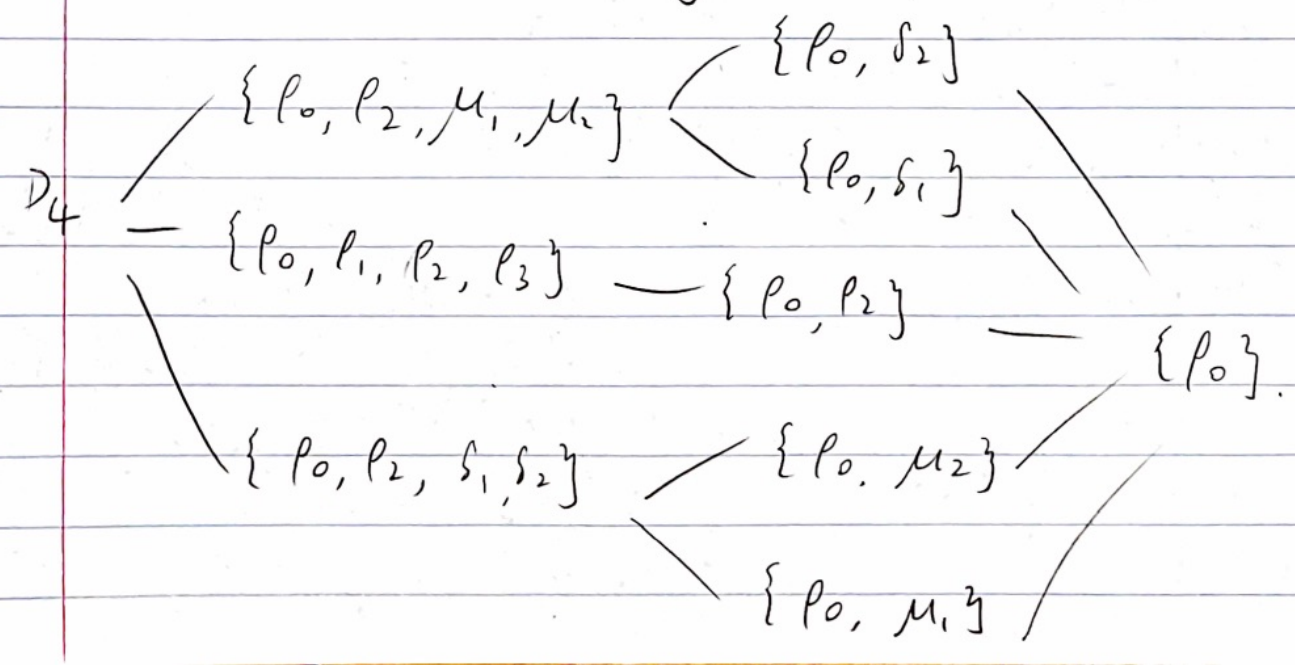
$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

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

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

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

, 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. $\varphi(x) = x'$, $\varphi(y) = y'$

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

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* gives us

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

* — list as $(\cdots)$

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 orbits of an element is an equivalence class.

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

$a \sim a$ ✓.

$a \sim b \Rightarrow b \sim a$ ✓

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

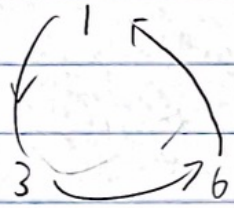
All the equivalence classes in A determined by $\sim$ are the orbits of σ.

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.

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 4 & 1 \end{pmatrix} = (136)(45)\underbrace{(2)}_{\text{omitted}}$$: 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 $(n \geq 2)$, $I = (1,2)(1,2)$, 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: w/ det

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

transposition (interchange 2 elements) ↓ transposition 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 ~.

One could also count the orbits and see σ and $\tau\sigma$ (where τ 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 τ 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.

$\sigma \in S_8$ $\quad \sigma = (1\,2)(4\,5\,7)$
order 2, order 3

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

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 $\text{Lagr} \mid p \Rightarrow |\langle a \rangle| = p$.

$\Rightarrow \langle a \rangle = G$.

$\therefore G$ is cyclic.

G of prime order p is a cyclic group of order p

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

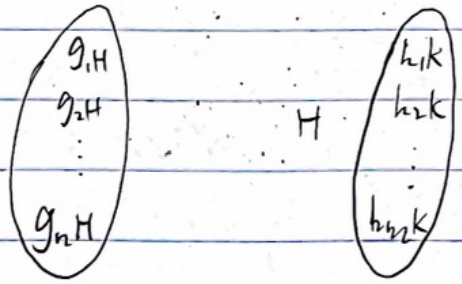
$\simeq \mathbb{Z}_p$.

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:



$g_1h_1K \cdots g_1h_mK$

$\vdots$

$g_nh_1K \cdots g_nh_mK$

all different

§11 Direct products and finitely generated abelian groups.

Make $\prod_{i=1}^{n} G_i$ into a group by a binary operation of multiplication by components.

Thm. Let $G_1, \cdots, G_n$ be groups.

$\forall (a_1, a_2, \cdots, a_n)$ and $(b_1, \cdots, b_n) \in \prod_{i=1}^{n} G_i$.

def. $(a_1 b_1, a_2 b_2, \cdots, a_n b_n)$ = their product. (component-wise)

then the binary operation "$\cdot$" makes $\prod_{i=1}^{n} G_i$ a group, the direct product of the groups G_i's.

Closed by def., associativity easily verified!

identity: $(e_1, e_2, \cdots, e_n)$

inv: $(a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1})$ ✓.

if each G_i has commutative operation. (abelian)

we (may) use the direct sum $\bigoplus_{i=1}^{n} G_i$ notation.

Obviously, the direct product / "sum" of abelian groups

$V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

is again abelian.

And $|\prod_{i=1}^{n} G_i| = \prod_{i=1}^{n} |G_i|$

E.g. $G = H \times K$ where H, K are groups

Let $H' := H \times \{e_K\}$ $\quad K' = \{e_H\} \times K$.

H', K' are subgroups of G.

✓ closed, i.d. (e_H, e_K), inv. (h^{-1}, e_K).

✓ $H' \cap K' = \{e_G\} = \{e_H\} \times \{e_K\}$

✓ $\forall\, h' \in H',\ k' \in K'$,

$h'k' = (h, e_K)(e_H, k) = (h, k) = (e_H, k)(h, e_K)$

$= k'h'$.

Thm. $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic and thus isomorphic to $\mathbb{Z}_{mn}$ (order mn)

iff $\gcd(m, n) = 1$

$\Leftarrow$: consider cyclic subgroup $\langle (1,1) \rangle$.

bc first $\underset{(m,n)}{\text{lcm}} = mn$ | order of $\langle 1, 1 \rangle$; second in total there are mn elements.

∴ the cyclic subgroup is of order mn and is thus the whole group.

$\Rightarrow$: WTS $\operatorname{lcm}(m,n) = mn$.

We know m and $n \mid \operatorname{lcm}(m,n)$.

Therefore, $\forall\ (a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, $\operatorname{lcm}(m,n)(a,b) = 0$.

since $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic, $\operatorname{lcm}(m,n) = mn$

since $mn(a',b') = 0$ for some (a',b').

Cor. $\bigoplus_{i=1}^{k} \mathbb{Z}_{m_i} \cong \mathbb{Z}_{m_1 m_2 \cdots m_k}$ iff $\gcd(m_i, m_j) = 1$ for all $i \neq j$.

(by induction)

∴ $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \mathbb{Z}_{p_2^{r_2}} \cdots \mathbb{Z}_{p_n^{r_n}}$ (prime factorization)

Changing the order of factors does not change the group structure (isomorphism) because the ordering of the components are changed via an isomorphism

φ: $(\mathbb{Z}^2, \mathbb{Z}^5, \mathbb{Z}^3) \to (\mathbb{Z}^5, \mathbb{Z}^3, \mathbb{Z}^2)$ "renaming is isomorphism"

cyclic subgroup of $\mathbb{Z}$ and thus cyclic

lcm: positive generator of the cyclic group of all common multiples of r_i. $(i = 1 \sim n)$.

Thm: For $(a_1, a_2, \cdots, a_n) \in \prod_{i=1}^{n} G_i$

a_i has finite order r_i in G_i

order of $(a_1, a_2, \cdots, a_n)$ in $\prod_{i=1}^{n} G_i$: lcm

= lcm of the orders of a_i's in G_i's

$a_1^{r_1} = e_1 \cdots a_n^{r_n} = e_n$ $\quad \mathbb{Z} \simeq ?$

$\therefore$ lcm $(r_1 \sim r_n) = ?$ as desired.

For $\prod_{i=1}^{n} G_i$, $\bar{G_i} := \{(e_1, \cdots, a_i, \cdots, e_n) \mid a_i \in G_i\}$

$\simeq G_i$ by $\varphi(e_1, \cdots a_i, \cdots, e_n) = a_i$

Subgroup of $\prod G_i$

$\prod_i G_i$ is called the internal direct product here w.r.t. the $\bar{G_i}$'s, On the other hand, $\prod_i G_i$ is called the external direct product w.r.t. G_i's.

Fundamental Theorem of finitely generated abelian groups.

generated by finite elements: abelian group G is $\simeq$ to a direct product of cyclic group in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

primes $p_1 \sim p_n$ can repeat

$r_1 \sim r_n \in \mathbb{Z}^+$

w/ Betti no. of G, which is ignored if we are considering finite groups.

Proof Omitted.

We can use this to find all abelian groups of a given order. (up to iso)

e.g. order $360 = 2^3 \times 3^2 \times 5$

$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{360}$$

recall $\mathbb{Z}_2 \times \mathbb{Z}_4 \not\simeq \mathbb{Z}_8$ since $\gcd(2,4) = 2 \neq 1$

$\therefore \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

and for the other 2, we replace $\mathbb{Z}_9$ by $\mathbb{Z}_3 \times \mathbb{Z}_3$.

$\therefore$ in total 6. (if we want to get this no. of abelian groups of order $p_1^{r_1} \dots p_n^{r_n}$ up to isomorphism, we need partition function (expressed in the form of generating functions, and has no closed form).

e.g. $p(3) = 3$, $p(2) = 2$, $p(1) = 1$

$\therefore$ $3 \times 2 \times 1 = 6$.

A group G is decomposable if it is isomorphic to two proper non-trivial subgroups. otherwise, we call G indecomposable.

The finite indecomposable abelian groups are exactly the cyclic groups w/ order a power of a prime

all cyclic Groups $\cong \mathbb{Z}_{p^r}$ are finite indecomposable abelian groups

(if not, $\cong \mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$, then order of every element is $\leq j$ $(i \leq j)$ $(i+j = r)$ and thus the group is not cyclic.

For any indecomposable abelian group G, it can only be isomorphic to $\mathbb{Z}_{p^r}$ because otherwise, if the group has two (prime) divisors, then G is decomposable.

Therefore, G must be (at least) cyclic groups of order p^r.

and since $\mathbb{Z}_{p^r}$ is indecomporable as well:

(since $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j} \not\cong \mathbb{Z}_{p^r}$ $(i \le j,\ i+j=r)$ as $\gcd(p^i, p^j) = p^i > 1$.)

All cyclic groups of order p^r are cyclic and noncabelian.

$\therefore$ We proved both directions.

Thm. $m \mid |G|$, where G is a finite abelian group G, then G has a subgroup of order m.

$(p_i)^{r_i - s_i}$ generates a cyclic subgroup of $\mathbb{Z}_{(p_i)^{r_i}}$ of order $(p_i)^{s_i}$

$\therefore \langle (p_1)^{r_1-s_1} \rangle \times \langle (p_2)^{r_2-s_2} \rangle \times \cdots \times \langle (p_n)^{r_n-s_n} \rangle$

w/ order $= m$

is our desired cyclic subgroup of G. $\{e, s_1, s_2, \ldots, s_n\}$

(is itself a group under the induced operation of G).

Thm m is square free, then every abelian group of order m is cyclic

$$G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_n} \quad (p_i \neq p_j)$$
$$\cong \mathbb{Z}_{p_1 p_2 \cdots p_n} \text{ (cyclic)}$$

since $p_1 \sim p_n$ are pairwise coprime.

---

§ 13. Group Homomorphism:

$\varphi: G \to G'$ satisfying the homomorphism property

$\ast \quad \ast'$

$$\varphi(a \ast b) = \varphi(a) \ast' \varphi(b)$$

$\forall\, a, b \in G$.

structure preserving map w.r.t. "$\ast$" and "$\ast'$"

Trivial Homomorphism: $\forall\, g \in G$, $\varphi(g) = e'$

always true for G': $e' = e'e'$ is what we get from the homomorphism

exists for all G and G'.

homo.

$\varphi : G \to G'$

Homomorphism preserves identity and inverses
(recall these are shown to be true in isomorphism, but it turns out that the homomorphism properties suffices :)

① $\varphi(e)\varphi(e) = \varphi(ee) = \varphi(e)$

since the only idempotent element of G' is e'

$\varphi(e) = e'$

② $\varphi(a)\varphi(a)^{-1} = e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$

left cancellation

$\Rightarrow \varphi(a)^{-1} = \varphi(a^{-1})$

Also, $H \leq G \Rightarrow \varphi(H) \leq G'$

$\forall\ \varphi(a), \varphi(b) \in \varphi(H)$.

$\varphi(ab) = \varphi(a)\varphi(b) \in \varphi(H)$ closed.

$e' = \varphi(e)$ id. of $\varphi(H)$

$\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H)$ inv.

subgroup of G'

***

(From this we know $\varphi(G)$ is a subgroup of G'.)

And $K' \leq G' \Rightarrow \varphi^{-1}(K') \leq G$.

We can prove this similar to above.

**: yet showing $H \leq G \Leftrightarrow$ ($\forall a \in H, b \in H$, $ab^{-1} \in H$.) and ($H \neq \emptyset$ or $e_G \in H$)

$\Rightarrow$ obvious (i.d.)

$\Leftarrow$: let $a = e_G$, then $b \in H$ (inv.)

$\Rightarrow b^{-1} \in H$

$\forall a, b \in \varphi^{-1}(K')$ then $a \in H$, $b^{-1} \in H \Rightarrow b^{-1} \in H$

gives $a(b^{-1})^{-1} = ab \in H$ (closed)

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

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

$\in K' \quad \in K'$

$\in K'$

$ab^{-1} \in \varphi^{-1}(K')$

For group homomorphism $\varphi: G \to G'$

given G is abelian and φ is onto G', then

G' must be abelian.

$\forall\, a', b' \in G'$, $a'b' = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba)$

$= \varphi(b)\varphi(a) = b'a'$.

* "When φ is onto, φ gives group structure of G to G'."

Kernel: $\ker(\varphi) = \varphi^{-1}(\{e'\})$ for $\varphi: G \to G'$.

Since $\{e'\} \leq G'$, $\varphi^{-1}(\{e'\})$ is necessarily a subgroup of G.

Some important examples of group homo.

i) $\varphi: S_n \to \mathbb{Z}_2$ given by $\varphi(e) = \begin{cases} 0 & \text{even permutation} \\ 1 & \text{odd permutation} \end{cases}$

$\ker\varphi = A_n$

ii) evaluation homo. def. $\mathrm{Map}(X, G) = \{f : X \to G\}$

This set of functions from X to G has a natural group structure induced from $\langle G, \cdot \rangle$

$\wedge$

$*$

$\forall x \in X$, $(f * g)(x) := f(x) \cdot g(x)$

closed associative id. inv. ✓.

For any $c \in X$, we may define the evaluation map

$ev_c : Map(X, G) \to G$ given by $f \mapsto f(c)$

$ev_c(f) \cdot ev_c(g) = f(c) \cdot g(c) = (f * g)(c)$

$= ev_c(f * g)$

$\ker(ev_c) = \{ f : X \to G \mid f(c) = e \}$

(the f s.t. $ev_c(f) = e$)

iii.) The left-multiplication transformation

$\varphi : \mathbb{R}^n \to \mathbb{R}^m$ given by $M(\varphi) \cdot \mathbb{R}^n = \mathbb{R}^m$

where $\mathbb{R}^n$, $\mathbb{R}^m$ are seen as abelian groups under addition.

$\ker \varphi = \text{null } \varphi$

iv) Determinant:

$\det : GL(n, \mathbb{R}) \to \mathbb{R}^* := \mathbb{R} \setminus \{0\}$.

$A \mapsto \det(A)$

A: under matrix multiplication

$\det(A)$: under multiplication on real number (nonzero).

$\ker(\det) = SL(n, \mathbb{R})$.

v) Modulo map $\varphi: \mathbb{Z} \to \mathbb{Z}_n$ $\quad \ker\varphi = n\mathbb{Z}$

$m \mapsto r_m$

vi) Inclusion / Projection of direct products:

$i: G_j \to G_1 \times G_2 \times \cdots \times G_j \times \cdots \times G_n$

$g_j \mapsto e_1 \times e_2 \times \cdots \times g_j \times \cdots \times e_n$ $\quad \ker(i) = \{e_j\}$

$j: G_1 \times \cdots \times G_j \times \cdots \times G_n \to G_j$ $\quad \ker(j) = \{g_1 \times \cdots \times e_j \times \cdots \times g_n\}$

$g_1 \times \cdots \times g_j \times \cdots \times g_n \mapsto g_j.$

For a group homomorphism $\varphi: G \to G'$, it is injective iff $\ker\varphi = \{e_G\}$.

$\Rightarrow$: $\varphi(e_G) = e_{G'}$, and must be the only element.

$\Leftarrow$: $\varphi(g_1) = \varphi(g_2)$ for $\forall\, g_1, g_2 \in G$

then $\varphi(g_1 g_2^{-1}) = \varphi(g_1)(\varphi(g_2)^{-1}) = e_{G'}$.

$\therefore g_1 g_2^{-1} \in \ker\varphi$

$= e_G \quad \Rightarrow g_1 = g_2$

Rmk: to show $\varphi: G \to G'$ is an isomorphism,

first show φ is a homomorphism
then show $\ker\varphi = \{e\}$.
last show φ is onto

Def. $N \leq G$ is called a normal subgroup if any left coset of N is the same as the corresponding right coset of N.

$$gN = Ng \quad \text{for all } g$$

denoted by $N \trianglelefteq G$

Thm: $H \leq G$ is a normal subgroup of G: equivalent conditions:

(a) $g^{-1}hg \in H \quad \forall g \in G, h \in H$. / $g^{-1}Hg \subseteq H \quad \forall g \in G$

(b) $g^{-1}Hg = H \quad \forall g \in G$ ($\Leftrightarrow$ of course, switching g and g^{-1} does not matter)

(c) $Hg = gH \quad \forall g \in G$

(a) $\Rightarrow$ (b): to show $H \subseteq g^{-1}Hg$. $\forall g$
consider $h \in H$, $= gHg^{-1}$

$\forall g$, $g^{-1}hg \in H \Rightarrow h \in gHg^{-1}$, as desired

(b) $\Rightarrow$ (c). fix G, $\forall h \in H$, first show $hg \in gH$
and then the other direction. $gh \in Hg$.

$\forall h_1$

(c) $\Rightarrow$ (a): $h_1 g = g h_2$

$g^{-1} h_1 g = h_2 \in H$.

* Note that any subgroup of an abelian group is obviously a normal subgroup.

For any group homomorphism $\varphi: G \to G'$, $\ker \varphi \trianglelefteq G$.

$\forall g \in G$, $h \in \ker \varphi$, WTS: $g^{-1} h g \in \ker \varphi$.

$$\varphi(g^{-1} h g) = \varphi(g^{-1}) \varphi(h) \varphi(g)$$
$$= \varphi(g^{-1}) \varphi(g) = \varphi(g^{-1} g) = e_{G'}$$

§14. Factor groups.

$H \trianglelefteq G$, left coset $S = \{g \cdot H \mid g \in G\}$

define $*$ on S by $(g_1 H) * (g_2 H) = (g_1 g_2) H$.

We can show that $*$ is well-defined, and further show that $\langle S, * \rangle$ forms a group.

$g_1 H = g_1' H$, $g_2 H = g_2' H$.

$(g_1 H) * (g_2 H) = (g_1 g_2) H$

$(g_1' H) * (g_2' H) = (g_1' g_2') H$.

WTS: $(g_1 g_2) H = (g_1' g_2') H$

$\Rightarrow (g_1 g_2)^{-1} (g_1' g_2') \in H$

one can also show
$g_1' g_2' \in (g_1, g_2) H$

($\sim_L$ equivalence relation)

iff

$(g_1' g_2')^{-1} (g_1, g_2) \in H$

$g_2'^{-1} g_1'^{-1} g_1 g_2 = g_2'^{-1} g_2 \; g_2^{-1} (g_1'^{-1} g_1) g_2 \in H.$

$\in H$ $\in H$ $\in H$ $\in H$

$\because g_1 H = g_1' H$

$g_2 H = g_2' H$ since $H \trianglelefteq G$, $g_2^{-1} h g_2 \in H$

if we let H be normal
the operation "$*$" can always be well-defined.

$\langle S, * \rangle$ is a group

✓ associativity $((g_1 H) * (g_2 H)) * g_3 H$

✓ identity eH.

✓ inverse: $(gH)^{-1} = g^{-1} H$.

we denote $\langle S, * \rangle$ by G/H.

the factor / quotient group of G by H.

Actually $(aH)(bH) = (ab)H$ is well defined also only if $H \trianglelefteq G$. (WTS: $aH \subseteq Ha$ and the other direction)

$\mathbb{Z}/n\mathbb{Z}$: residue class modulo n.

For any representative $x \sim_L a$ (i.e. $x \in aH$)

$(xH)(a^{-1}H) = (xa^{-1})H$

$(aH)(a^{-1}H) = eH$

$\therefore xa^{-1} \in H$. so that the two are well-defined.

$\therefore x \in Ha \Rightarrow aH \subseteq Ha$. (same for $\supseteq$).

Under the well-defined operation of left-coset multiplication (given $H \trianglelefteq G$),

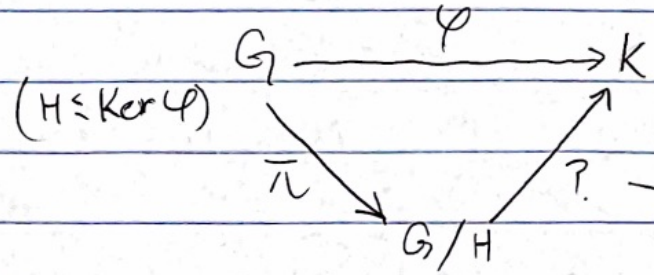
$\pi: G \to G/H$

$g \mapsto gH$ is a natural surjective homomorphism, with $\ker \pi = H$.

$\pi(g_1 g_2) = (g_1 g_2)H = g_1 H \cdot g_2 H = \pi(g_1)\pi(g_2)$ ✓.

$\ker \pi = \pi^{-1}(H) = \{$all elements $\in H\} = H$.

If we set the $H \trianglelefteq G$ to be a subgroup of $\ker \varphi$, where $\varphi: G \to K$ is a group homomorphism.



— we would get a group homo. $\tilde{\varphi}$.

It is easy to show the homo. property.

$\tilde{\varphi} : gH \mapsto \varphi(g) \quad \forall g \in G.$

$\tilde{\varphi}(g_1 H g_2 H) = \tilde{\varphi}(g_1 g_2 H)$

$= \varphi(g_1 g_2)$

$\tilde{\varphi}(g_1 H)\,\tilde{\varphi}(g_2 H) = \varphi(g_1)\varphi(g_2)$) $\because \varphi$ is a group homomorphism.

But before we need to check $\tilde{\varphi}$ is well-defined.

Consider $\tilde{\varphi}(g_1 H)$, $\tilde{\varphi}(g_2 H)$, where $g_1^{-1} g_2 \in H$

$\tilde{\varphi}(g_1 H) = \varphi(g_1)$, $\tilde{\varphi}(g_2 H) = \varphi(g_2)$

WTS: $\varphi(g_1) = \varphi(g_2)$

$\varphi(g_1^{-1} g_2) = (\varphi(g_1))^{-1} \varphi(g_2)$ { $\because \varphi$ is homo. }

$= e$ { $\because H \le \ker \varphi$ }

$\therefore \varphi(g_1) = \varphi(g_2)$ ✓.

— — — — — — — —

Rmk. If we set $H = \ker \varphi$, then

when $\varphi(g) = \tilde{\varphi}(gH) = e_K$.

$\therefore g \in \ker \varphi = H$, and thus $\ker \tilde{\varphi} = H$, the identity in G/H.

Thus, $\tilde{\varphi} : G/H \longrightarrow \varphi(G)$ { image of φ }

is an isomorphism bc both injective and surjective

This is sometimes called the first isomorphism thm, and the φ we have is usually a surjective group homomorphism (meaning that we know the image).

Examples: for the surjective group homomorphism

1) $\varphi: S_n \to \mathbb{Z}_2$ w/ $\ker \varphi = A_n$

$S_n / A_n \cong \mathbb{Z}_2$.

for the surjective evaluation homo.

2) $ev_x : Map(X, G) \to G$

$Map(X, G) / \{f: X \to G \mid f(x) = e\} \cong G$.

3) (Recall in linear maps, we also have

$V / \text{null } T \cong \text{range } T$)

quotient space

4) Determinant: $\det : GL(n, \mathbb{R}) \to \mathbb{R}^*$ surjective.

$\ker \det = SL(n, \mathbb{R})$

$GL(n, \mathbb{R}) / SL(n, \mathbb{R}) \cong \mathbb{R}^*$

5) For projection homomorphism:

$p_j : G_1 \times \cdots \times G_j \times \cdots \times G_n \to G_j$

$\ker p_j = G_1 \times \cdots \times \{e_j\} \times \cdots \times G_n$.

$G_1 \times \cdots \times G_j \times \cdots \times G_n / G_1 \times \cdots \times \{e_j\} \times \cdots \times G_n \simeq G_j$.

An isomorphism from G to G is called an automorphism.

$\mathrm{Aut}(G) := \{$ the set of all automorphisms φ on $G\}$

Recall S_G is the group of all permutations (bijections) on G.

Since closed, identity, and inverse can all be checked,

$\mathrm{Aut}(G) \leq S_G$.

called the automorphism group of G.

For G, $\forall g \in G$, $i_g : G \to G$ given by $x \mapsto gxg^{-1}$ is an automorphism of G.

injective ✓

$i_g(x) = i_g(y) \Rightarrow x = y$ by cancellation law.

surjective ✓

$i_g(g^{-1}xg) = x$

$$(i_g)(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1})$$
$$= i_g(x) \cdot i_g(y).$$

* These automorphisms $i_g \in Aut(G)$ are called the inner automorphisms of G by g.

$Inn(G)$ = the set of all inner automorphisms of G.
$\trianglelefteq Aut(G)$

Closed: $(i_h \circ i_g)(x) = i_h(gxg^{-1}) = (hg)x(g^{-1}h^{-1})$
$= (hg)x(hg)^{-1}$
$= (i_{hg})(x)$.
$\therefore \in Inn(G)$

identity: the identity automorphism (id_G) is the identity inner automorphism (i_e).

inverse: $(i_{g^{-1}})(gxg^{-1}) = x$.
$\in Inn(G)$.

(note that $H \trianglelefteq G$ iff H is invariant under all automorphisms of G)
↑ inner

$\forall g, \quad gHg^{-1} = H$

Def $Out(G) := Aut(G) / Inn(G)$

(outermorphism group.

$\varphi: G \to Inn(G)$ is a surjective group homo.
$g \mapsto i_g$

surjective by def. $\varphi(g_1 g_2) = (g_1 g_2)(\cdot)(g_1 g_2)^{-1}$

$= g_1 (g_2(\cdot) g_2^{-1}) g_1^{-1}$

$= i_{g_1}(i_{g_2}(\cdot))$

$= \varphi(g_1)\varphi(g_2)$.

$\ker \varphi = \{ g \in G \mid i_g = id_G \}$

$= \{ g \in G \mid gxg^{-1} = x, \forall x \in G \}$

$:= Z(G)$, center of G. | (it is clearly abelian, and when G is abelian $G = Z(G)$, which is not useful)

$G / Z(G) \simeq Inn(G)$.

§15. More on Factor Groups

e.g. Disproof of the converse of Lagrange's thm

A_4 w/ order 12 has no subgroup of order 6

$\frac{12}{6} = 2$

We can prove that index 2 subgroups must be normal.

for $H < G$ w/ $|G:H| = 2$,

take $g \in G - H$, then H has left cosets $\{H, gH\}$

and right cosets $\{H, Hg\}$.

$H \cup gH = H \cup Hg = G \Rightarrow gH = Hg$

$\Rightarrow H \lhd G$.

If we have $|H| = 6$ s.t. $H \lhd A_4$,

then $A_4/H \cong \mathbb{Z}_2$ (the only group of order 2 up to iso)

$\therefore \forall \sigma \in A_4, \ \sigma H \cdot \sigma H = \sigma^2 H = H$.

$\therefore \sigma^2 \in H, \ \forall \sigma \in A_4$

e.g. since $\sigma_1 = (1,2,3) \in A_4, \ \sigma_1^2 = (1,3,2) \in H$

$\sigma_2 = (2,3,1), \Rightarrow \sigma_2^2 = (1,2,3) \in H \cdots$ etc,

and we can show all 8 "3 cycles" in A_4 are in H.

$\therefore |H| \geq 8$, contradiction

$\mathbb{Z}_4 \times \mathbb{Z}_6$ abelian $\Rightarrow$ $\mathbb{Z}_4 \times \mathbb{Z}_6 / H$ abelian (bc we are using representatives from $\mathbb{Z}_4 \times \mathbb{Z}_6$ in calculation)

e.g. $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(2,3)\rangle \simeq ?$

---

sometimes we check if one $\mathbb{Z}_m$ collapses: $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,1)\rangle = \mathbb{Z}_4$, e.g. ($\because \mathbb{Z}_6$ collapses)

For questions of this type in general, first find order $= \frac{4 \times 6}{2} = 12 = 2^2 \times 3$.

$\therefore$ the factor group $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ or $\mathbb{Z}_4 \times \mathbb{Z}_3$

*** What does isomorphism mean?

iso. $\Rightarrow$ the number of elements of a certain order is the same for isomorphic groups, and this is what we usually check in such problems.

For $\langle(2,3)\rangle + (1,0)$
$+ (2,0)$
$+ (3,0)$
$+ (0,0)$ smallest power that returns

$\therefore$ order of $(1,0) + \langle(2,3)\rangle$ is 4

$\therefore \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \simeq \mathbb{Z}_{12}$

e.g. $\mathbb{Z} \times \mathbb{Z}/\langle(1,1)\rangle \simeq \mathbb{Z}$ by drawing the affine subsets on the integer coordinate system.

We restate the techniques we used:

*

For the collapse argument we have on the sidebar above, we have the thm:

$G = H \times K$, $\begin{cases} \bar{H} = \{(h,e) \mid h \in H\} \trianglelefteq G. \\ G/\bar{H} \cong K \\ G/\bar{K} \cong H. \end{cases}$

proof: $\pi_2 : H \times K \to K$ by $\pi_2(h,k) = k$, (surjective)

$\ker \pi_2 = e = \bar{H} \trianglelefteq G$,

and the other 2 claims follow by the isomorphism theorem.

*

A factor group of a cyclic group is cyclic.

$G = \langle a \rangle$, then for $N \trianglelefteq G$, WTS: $\langle aN \rangle = G/N$.

the powers of a gives all elements in G and thus all elements in G/N.

Simple groups:

a nontrivial group that has no proper nontrivial subgroups.

The alternating group A_n is simple for $n \geq 5$

(see the exercise in the book for proof)

Def. A maximal normal subgroup of a group G is a normal subgroup $M \neq G$ s.t. there is no proper normal subgroup $N \trianglelefteq G$ such that $M \subsetneq N$.

Lemma: For group homo. $\varphi: G \to G'$

$N \trianglelefteq G \Rightarrow \varphi(N) \trianglelefteq \varphi(G)$

$N' \trianglelefteq \varphi(G) \Rightarrow \varphi^{-1}(N') \trianglelefteq G$

easy to prove: we already have this for regular subgroups, and use group homo. we can show that "normal" is preserved.

Prop. M is a maximal normal subgroup of G iff G/M is simple.

$\Rightarrow$: consider $\pi: G \to G/M$ canonical homo. $g \mapsto gM$ (surjective)

π^{-1} of any proper nontrivial normal subgroup of G/M is a proper normal subgroup of G.

$N' \neq eM$

since $eM \in N'$, $M \subsetneq \pi^{-1}(N')$ $\quad \pi^{-1}(N') \trianglelefteq G$.

$\therefore \pi^{-1}(N') = G$ bc M is maximal.

consider nontrivial $N' \trianglelefteq G/M$. $\pi^{-1}(N') \trianglelefteq G$ because φ is surjective

$\{eM\} \subsetneq N' \Rightarrow M \subsetneq \pi^{-1}(N')$

since M is maximal, no such $\pi^{-1}(N')$ exists

$\Rightarrow$ no such N' exists

$\Rightarrow$ G/M is simple.

$\Leftarrow$: Let G/M be simple

If $N \trianglelefteq G$ w/ $M \subsetneq N$.

$\pi(N)$ is normal in G/M

with $\pi(N) \neq G/M$ and $\pi(N) \neq \{eM\}$,

showing that no such normal subgroup

$\pi(N)$ by G/M is simple

$\Rightarrow$ no such N exists under our assumption

$\Rightarrow M$ is maximal

✓ Last topic: commutator subgroup

idea: for a nonabelian G, we want to create an abelianized version of G by letting all elements a, b in it having $ab = ba$.

An element $aba^{-1}b^{-1}$ in a group we call it the commutator of the group.

what we want is to replace every commutator of G by e.

First we can prove that the commutators generate normal subgroup C of G. (called the commutator subgroup, although the commutators themselves do not form a group!)

WTS: subgroup generated is normal in G.

$e = eee^{-1}e^{-1}$ is a commutator

$(aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$ is a commutator. $\Rightarrow$

So that it is okay to say the integral powers of commutators, and all elements in the generated subgroup are finite integral powers of commutators.

WTS: for finite product of commutators x,

$$g^{-1}xg \in C \quad \text{for all } g \in G.$$

we insert $e = gg^{-1}$ between every adjacent pair of

commutators, then it suffices to show

$g^{-1}(cdc^{-1}d^{-1})g \in C$ for $cdc^{-1}d^{-1}$ commutator.

$$g^{-1}(cdc^{-1}d^{-1})g = (g^{-1}cdc^{-1})(e)(d^{-1}g)$$
$$= (g^{-1}cdc^{-1})(gd^{-1}dg^{-1})(d^{-1}g)$$
$$= [(g^{-1}c)d(c^{-1}g)d^{-1}](dg^{-1}d^{-1}g)$$
$$\in C.$$

showing that $C \trianglelefteq G$.

---

second, we may treat this commutator subgroup C as the "identity" & consider the factor group of G modulo a normal subgroup N containing C, since the commutators are now seen as

Second, if we consider the factor group of G modulo N, where $N \trianglelefteq G$ and $C \leq N$, then G/N is abelian.

This is bc G/N has N as its identity. Therefore, w.r.t. G/N, elements in N (and thus all elements in C) become identity representatives.

Since

(if we take $C=N$, then G/C is abelian)

the usual case

Rigorously, if $C \leq N$, then

$$(aN)(bN) = abN = ab(b^{-1}a^{-1}ba)N$$

$$= baN$$

$$= (bN)(aN).$$

~~The other direction G/N abelian $\Rightarrow C \leq N$~~

under $N \trianglelefteq G$

Rigorously: $\forall a, b \in G$

$$(a^{-1}N)(b^{-1}N) = (b^{-1}N)(a^{-1}N)$$

$$\Leftrightarrow \quad a^{-1}b^{-1}N = b^{-1}a^{-1}N$$

$$\Leftrightarrow \quad aba^{-1}b^{-1} \in N.$$

$$\Leftrightarrow \quad C \leq N$$

so that the claim is true in both directions:

$$G/N \text{ abelian} \Leftrightarrow C \leq N$$

(given $N \trianglelefteq G$).

We may use this as a criterion to check which subgroup is the commutator subgroup.

e.g. C in $S_3 = A_3$. (example 15.21)