HW 1 due now. Wednesday.

Recall: A group G is called cyclic if

$$G = \langle g \rangle = \{ \dots, g^{-2}, g^{-1}, e, g, g^2, \dots \}$$

for some $g \in G$.
(G is generated by 1 element).

For any $g \in G$, $\langle g \rangle \leq G$ is a subgroup

"smallest subgp. of G containing g!!"

$$\langle g \rangle = \bigcap_{\substack{H \leq G \\ g \in H}} H.$$

$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$ order 6.

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ order ∞

Notation: $|\langle g \rangle|$ is the order of g.

Recall Prop 2.4.
Every subgroup of $(\mathbb{Z}, +)$ is cyclic.
i.e. if $H \leq \mathbb{Z}$ then $H = a\mathbb{Z}$ for some $a \in \mathbb{Z}$.

Proof: Let a be smallest positive element of H.
Show $a\mathbb{Z} \subseteq H$ (easy)
and $H \subseteq a\mathbb{Z}$ (less easy)

Given $a, b \in \mathbb{Z}$ let

$$a\mathbb{Z} + b\mathbb{Z} := \{ax + by : x, y \in \mathbb{Z}\}$$

Check: $a\mathbb{Z} + b\mathbb{Z} \leq \mathbb{Z}$

(the subgroup generated by a and b)

Corollary to Prop 2.4:
Let d = smallest pos element of $a\mathbb{Z} + b\mathbb{Z}$.
Then

$$\boxed{a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}}$$

$d = \gcd(a, b)$

Properties:

- $d = ax + by$ for some $x, y \in \mathbb{Z}$.
- $d \mid a$ and $d \mid b$. (common divisor)

Pf: $a, b \in a\mathbb{Z} + b\mathbb{Z} \Rightarrow a, b \in d\mathbb{Z}$. ▨

- if $c \mid a$ and $c \mid b$ then $c \mid d$.

Pf: if $a = ca'$ and $b = cb'$ then

$$d = ax + by = ca'x + cb'y$$
$$= c(a'x + b'y) \Rightarrow c \mid d. \blacksquare$$

Notation:
d is the greatest common divisor of a, b
GCD.

Maps of Groups.

Let C be an infinite cyclic group

$$C = \langle a \rangle = \{ \ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots \}$$

We can define a map (function)

$$\varphi : \mathbb{Z} \to C$$
$$n \longmapsto a^n .$$

Note: • φ is an injection (one-to-one).

Given $m, n \in \mathbb{Z}$ suppose $\varphi(m) = \varphi(n)$.
That is $a^m = a^n$ in C.
If say $m < n$ then multiply by $(a^m)^{-1} = (a^{-1})^m$ to get $e = a^{n-m}$.
Since a has order ∞ this is a Contradiction.
Hence $m = n$.

$$\boxed{\varphi(m) = \varphi(n) \implies m = n}$$

injective

• φ is a surjection (onto)

Given $q \in C$ we have $q = a^n$ for some $n \in \mathbb{Z}$. But then $q = \varphi(n)$.

$$\boxed{\forall g \in C \; \exists n \in \mathbb{Z}, \; \varphi(n) = g}$$

surjective.

- injection + surjection = bijection

$$\mathbb{Z} \leftrightarrow C.$$

But more is true.

- $$\boxed{\varphi(m+n) = a^{m+n} = a^m \cdot a^n = \varphi(m)\varphi(n)}$$

φ is a homomorphism of groups ("same structure")

- bijection + homomorphism = isomorphism

Conclusion:

$\varphi : \mathbb{Z} \to C$ is a group isomorphism and we write

$$\mathbb{Z} \approx C.$$

Up to isomorphism, $\mathbb{Z}$ is the ONLY infinite cyclic group.

Similarly, all finite cyclic groups of the same size are isomorphic.

Let $G = \langle g \rangle$ with $|\langle g \rangle| = |\langle h \rangle| = n$.
$H = \langle h \rangle$

Then the map $\varphi : G \to H$
$g^n \mapsto h^n$
is an isomorphism $G \cong H$.

Cor: There is one cyclic group of each size.
The cyclic group of size n is usually called $\mathbb{Z}/n\mathbb{Z}$ ($\mathbb{Z}$ mod $n\mathbb{Z}$).

Summary: If G is cyclic then
$G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}/n\mathbb{Z}$ for some n.

General Facts: Let S, T be finite sets.

(1) $\exists$ injection $f : S \to T$
$\iff |S| \leq |T|$

(2) $\exists$ surjection $f : S \to T$
$\iff |S| \geq |T|$

(1)+(2) = $\exists$ bijection $f : S \to T$
$\iff |S| = |T|$

Now consider maps $f: X \to X$, $|X| < \infty$ FINITE

By (1) + (2) we have

f is injective $\iff$ f is surjective.

Remark: NOT true for infinite sets.

eg. $f: \mathbb{Z} \to \mathbb{Z}$. injective ✓
$n \longmapsto 2n$. surjective X.

Food for thought: Let $A, B \in M_n(\mathbb{R})$.
If $AB = I$ then $BA = I$. Why?

Think: A, B are functions $\mathbb{R}^n \to \mathbb{R}^n$.
Suppose $AB = I$.
Then (Claim) B is injective
Proof: If $B\vec{x} = B\vec{y}$ for $\vec{x}, \vec{y} \in \mathbb{R}^n$
Then $AB\vec{x} = AB\vec{y} \Rightarrow \vec{x} = \vec{y}$ ∎

Now note $(I - BA)B = B - B(AB) = B - B = O$
zero matrix.

If $\vec{x} \mapsto B\vec{x}$ were surjective then $\forall \vec{y} \in \mathbb{R}^n$
we can write $\vec{y} = B\vec{x}$ and hence
$(I - BA)\vec{y} = (I - BA)B\vec{x} = O\vec{x} = \vec{0}$.

Hence $(I - BA)\vec{y} = \vec{0}$ for all $\vec{y} \in \mathbb{R}^n$.

In particular, let $\vec{e}_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}$ — ith position.

Then $(I - BA)\vec{e}_i = i$th col of $I - BA = \vec{0}$ $\forall i$.

$\Rightarrow$ $I - BA = O$ matrix

$\Rightarrow$ $BA = I$ ☒ ??

Problem:

We know $B: \mathbb{R}^n \to \mathbb{R}^n$ is injective

We want $B: \mathbb{R}^n \to \mathbb{R}^n$ is surjective.

But $|\mathbb{R}^n| = \infty$ ☹

Wait, we're still OK.

Rank-Nullity Theorem says:

for linear function (matrix) $B: \mathbb{R}^n \to \mathbb{R}^n$ we have

B injective $\iff$ B surjective

(even though $\mathbb{R}^n$ is not finite) //

HW 1 due NOW

HW 2 due Mon Sep 26

Exam 1 Wed Sep 28

Now: Maps.

Let $f: S \to T$ be a function, S, T possibly infinite sets.

actually $g: \text{im}(f) \to S$

(1) $\exists\, g: T \to S \ni g \circ f = id_S$

(say f is "left-invertible")

$\Updownarrow$

$\forall s_1, s_2 \in S,\ f(s_1) = f(s_2) \Rightarrow s_1 = s_2$

(f is "injective")

(2) $\exists\, h: T \to S \ni f \circ h = id_T$

(f is "right-invertible")

$\Updownarrow$

$\forall t \in T\ \exists s \in S \ni f(s) = t$

(f is "surjective")

(1)+(2) f is bijective (inj. + surj.)

$\Updownarrow$

$\exists\, g: T \to S \ni f \circ g = id_T$ and $g \circ f = id_S$

We say f is "invertible"
In this case we also identify $S = T$ via f. So f is really

$$f : S \to S.$$

$f \circ g = g \circ f = id_S$
"two-sided inverse" ///

Notation: Given $f : S \to T$, define

$$\text{image}(f) := \{ t \in T : \exists\, s \in S \ni f(s) = t \}$$

"$f(S)$"
"$\text{im}(f)$"

Thus: f surjective $\iff \text{im}(f) = T$

Add structure ....

Let $(G, *)$, $(H, \#)$ be groups. The map $\varphi : G \to H$ is a homomorphism if

$$\forall\, a, b \in G, \quad \varphi(a * b) = \varphi(a) \# \varphi(b)$$

($a * b$: product in G; $\varphi(a) \# \varphi(b)$: product in H.)

Def: bijection + homomorphism "$G \cong H$"
= isomorphism

(isomorphism $G \to G$) = automorphism

Let $\mathrm{Aut}(G) := \{ f : G \to G \mid f \text{ automorphism} \}$
– a group under $\circ$

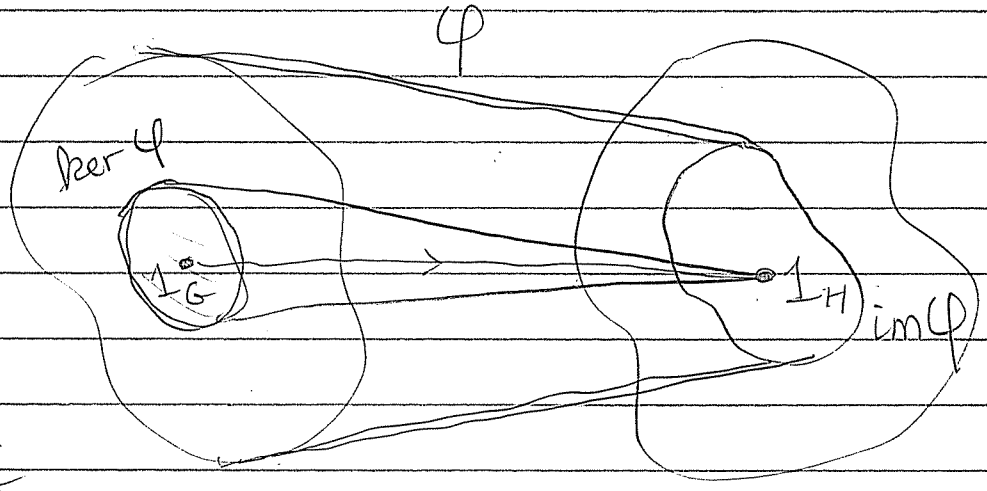
Imagine.... G, $\mathrm{Aut}(G)$, $\mathrm{Aut}(\mathrm{Aut}(G))$, ...
↑ "symmetries of G" ↑ "symmetries of symmetries"

ACK!

HW 2.3(b)
Compute $\mathrm{Aut}(\mathbb{Z}^+)$.

Def: Given hom. $\varphi : G \to H$, let

$\ker \varphi := \{ g \in G : \varphi(g) = 1_H \}$



Prop 2.5.3. Given $\varphi: G \to H$ hom.

(b) $\varphi(1_G) = 1_H$

Proof: $\varphi(1_G)\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)$.

Multiply by $\varphi(1_G)^{-1}$ to get $\varphi(1_G) = 1_H$ ☒

(c) $\forall a \in G$, $\varphi(a^{-1}) = \varphi(a)^{-1}$

Proof: $\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1_G) = 1_H$.

Multiply by $\varphi(a)^{-1}$ to get $\varphi(a^{-1}) = \varphi(a)^{-1}$ ☒

Important Fact:

Given hom. $\varphi: G \to H$.

$\ker \varphi = \{1_G\} \subseteq G \iff \varphi$ injective.

PAUSE

$\mathbb{R}^n$ is an additive abelian group

Consider matrices $A, B \in M_n(\mathbb{R})$ as (linear) functions $A, B: \mathbb{R}^n \to \mathbb{R}^n$.

(linear) homomorphisms

$AB = I \implies B$ left invertible

$\implies B$ injective

$\implies \ker B = \{\vec{0}\}$

↓

Fact: Dimension Formula (Thm 4.1.6)

$$\dim(\ker B) + \dim(\operatorname{im} B) = \dim(\mathbb{R}^n) = n$$

So $\dim(\ker B) = 0 \Rightarrow \dim(\operatorname{im} B) = n$

$\Rightarrow \operatorname{im} B = \mathbb{R}^n$

$\Rightarrow B$ surjective

$\Rightarrow \exists\ C \in M_n(\mathbb{R}) \ni BC = I$.

Finally,

$$A = AI = A(BC) = (AB)C = IC = C.$$

Hence $BA = I$ ▨

UNPAUSE.

Given hom. $\varphi: G \to H$, we know $\ker\varphi \subseteq G$, $\operatorname{im}\varphi \subseteq H$ by definition

Moreover $\ker\varphi \leq G$ (1), $\operatorname{im}\varphi \leq H$ (2). you do this

Check: (1) Closed because $\varphi(a) = 1_H$ and $\varphi(b) = 1_H \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = 1_H 1_H = 1_H$.

Contains 1_G since $\varphi(1_G) = 1_H$.

Contains inverses since $\varphi(a) = 1_H$

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

eg $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$
is a homomorphism $(\det(AB) = \det(A)\det(B))$

Hence

$\ker(\det) = SL_n(\mathbb{R})$
is a sbgp of $GL_n(\mathbb{R})$ ///

eg The map $z \mapsto z^n$ is a
homomorphism $U(1) \to U(1)$.

$\ker(z \mapsto z^n) = \{z \in U(1) : z^n = 1\}$
$= \langle e^{i\theta} \rangle \leq U(1)$
n-th roots of 1

$U(1)$ = "the circle group"

eg $x \overset{\varphi}{\mapsto} nx$ is a hom $\mathbb{Z} \to \mathbb{Z}$.

$\operatorname{im}\varphi = n\mathbb{Z} \leq \mathbb{Z} = 1\mathbb{Z}$
$\ker\varphi = \{0\} = 0\mathbb{Z} \leq 1\mathbb{Z}$

HW 2 due Monday Sep 26
Exam 1 Wed Sep 28
NO CLASS Mon Oct 3.
NO office Hours tomorrow. ///

Today:
① Some $\mathbb{Z}$
② Some maps.

① Recall Theorem 2.3.3
Let $S \leq \mathbb{Z}^+$ be a subgroup. Then $S = \{0\} (= 0\mathbb{Z})$ or $S = \mathbb{Z}a$ where a is smallest pos element of S.

Now let $a, b \in \mathbb{Z}$ and consider

$$\langle a,b \rangle = \bigcap_{\substack{H \leq \mathbb{Z} \\ \{a,b\} \subseteq H}} H \leq \mathbb{Z}$$

↑ HW 2.3

Claim: $\langle a,b \rangle = \mathbb{Z}a + \mathbb{Z}b = \{ra + sb \mid r,s \in \mathbb{Z}\}$
Proof: $\mathbb{Z}a + \mathbb{Z}b$ is a subgp. $\mathbb{Z} \Rightarrow \langle a,b \rangle \subseteq \mathbb{Z}a + \mathbb{Z}b$.
Conversely, note $\{a,b\} \subseteq \langle a,b \rangle$. Since $\langle a,b \rangle$ is closed, $\mathbb{Z}a + \mathbb{Z}b \subseteq \langle a,b \rangle$

Corollary: for $a, b \in \mathbb{Z}$ not both zero, we have

$$\langle a, b \rangle = \langle d \rangle$$
$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d. \quad (d > 0).$$

Notation: $d = \gcd(a, b)$

↑ greatest common divisor.

Facts: (a) $d \mid a$ & $d \mid b$.

(b) $e \mid a$ & $e \mid b \Rightarrow e \mid d$.

(c) $\exists\, r, s \in \mathbb{Z} \ni d = ra + sb$.

Notation: If $\gcd(a, b) = 1$, say a, b are coprime.

Corollary:

a, b coprime $\iff \exists\, r, s \in \mathbb{Z} \ni ra + sb = 1$

Proof: If $\gcd(a, b) = 1$ then $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}1 = \mathbb{Z}$.

Then $1 \in \mathbb{Z} \Rightarrow 1 = ra + sb$.

Conversely, sp. $ra + sb = 1$ then

$1 \in \mathbb{Z}a + \mathbb{Z}b \Rightarrow \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z} \Rightarrow \gcd(a, b) = 1$ ∎

↓

Corollary (Euclid's Lemma).
Let $p, a, b \in \mathbb{Z}$ with p prime.
If $p \mid ab$ then $p \mid a$ OR $p \mid b$.

Proof: Suppose $p \mid ab$ and $p \nmid a$.
What is $d = \gcd(p, a)$? Well $d \mid p$.
$\Rightarrow d = 1$ or p. But $p \nmid a$. Hence $d = 1$.
Then $\exists\, r, s \in \mathbb{Z} \ni ra + sp = 1$.
Multiply by b to get

$$rab + spb = b.$$

$p \mid rab$ & $p \mid spb \Longrightarrow p \mid b$. ▨

PAUSE (Euclid $\rightsquigarrow$ Unique Factorization)
Chapter 12 !!

for now...

What about $\mathbb{Z}a \cap \mathbb{Z}b$?

Fact: $\mathbb{Z}a \cap \mathbb{Z}b \leq \mathbb{Z}$
↖ HW 2.3

Cor: $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$ $(m > 0)$.

What is m?

(a) $a|m$ & $b|m$

Proof: $m \in \mathbb{Z}m \Rightarrow m \in \mathbb{Z}a \cap \mathbb{Z}b$ ∎

(b) $a|n$ & $b|n \Rightarrow m|n$. (hence $m \leq n$)

Proof: $a|n$ & $b|n \Rightarrow n \in \mathbb{Z}a \cap \mathbb{Z}b$

$\Rightarrow n \in \mathbb{Z}m \Rightarrow m|n$ ∎

Notation: $m = \operatorname{lcm}(a,b)$

↑

least common multiple.

($a, b > 0$)

↓

Cor: Let $d = \gcd(a,b)$, $m = \operatorname{lcm}(a,b)$

Then $ab = dm$.

Proof: Note $ab/d = a(b/d) = b(a/d) = N$

is an integer with $a|N$ & $b|N$.

Hence $m|N$ i.e. $\exists\, k \in \mathbb{Z} \ni mk = ab/d$

$\Rightarrow dmk = ab \Rightarrow dm \mid ab$.

Next, write $d = ra + sb$, so $dm = ram + sbm$.

Say $m = aa'$, $m = bb'$. Then

$dm = mabb' + sbaa' = ab(mb' + sa')$

$\Rightarrow ab \mid dm$.

$dm \mid ab$ & $ab \mid dm \Rightarrow ab = dm$ ∎

(& $a, b, d, m > 0$)

(2) More Maps

Two Equivalent concepts:

(i) S = a set.

A partition Π of S is a decomp. of S as a disjoint union

$$S = S_1 \cup S_2 \cup \cdots \cup S_k$$

where $S_i \cap S_j = \emptyset \quad \forall i \neq j$.

eg $\mathbb{Z} = (\mathbb{Z}2) \cup (1+\mathbb{Z}2)$
even odd.

eg $\mathbb{Z} = (0+\mathbb{Z}3) \cup (1+\mathbb{Z}3) \cup (2+\mathbb{Z}3)$
rem 0 rem 1 rem 2.

$$2+\mathbb{Z}3 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$
all have rem 2 (mod 3).

(ii) S = a set

A relation $R \subseteq S^2$ (written $x \sim y$ for $(x,y) \in R$) is called an equivalence if
- $x \sim y$ & $y \sim z \Rightarrow x \sim z$ (trans.)
- $x \sim y \Rightarrow y \sim x$ (Symm.)
- $\forall x, \ x \sim x$ (refl.)

Prop 2.7.4. Let S = a set. Then

a partition Π of S $\longleftrightarrow$ an equivalence $\sim$ on S

Proof: Given Π, define $\sim$ by saying $x \sim y \iff x, y$ in the same part of Π. Check $\sim$ is an equivalence.

Conversely, let $\sim$ be an equivalence and for $x \in S$ define

$$C_x := \{ y \in S : x \sim y \} \subseteq S$$

the "equivalence class of x"

Claim: The equiv classes partition S.

Note. $x \sim x \Rightarrow x \in C_x$. Thus

$$S = \bigcup_{x \in S} C_x \quad (S \text{ is covered})$$

But this union is NOT disjoint.

Can we make it disjoint?

Key Point: If $C_x \cap C_y \neq \emptyset$ then $C_x = C_y$.

symmetry.
$z \sim x$ $z \sim y$

Suppose $z \in C_x \cap C_y$ i.e. $x \sim z$ & $y \sim z$.
Then for any $a \in C_x$ we have
$a \sim x$ & $x \sim z \Rightarrow a \sim z$.
Then $a \sim z$ & $z \sim y \Rightarrow a \sim y$, i.e. $a \in C_y$.
Conclusion: $C_x \subseteq C_y$.
Similarly, $C_y \subseteq C_x$. Hence $C_x = C_y$ ///.

So we can remove duplicates from $\bigcup_{x \in S} C_x$ to get

$$S = \bigcup \text{distinct} \sim \text{classes}$$

↑ disjoint!

Sometimes we like to choose a (arbitrarily) class rep from each class.
Let X = class reps. Then

$$S = \bigsqcup_{x \in X} C_x \quad \text{disjoint.}$$

Notation & Sometimes we say
X = a transversal for $\sim$

HW 2 due Mon Sep 26

Exam 1 Wed Sep 28

I'm gone Thurs Sep 29 → Tues Oct 3

So... NO CLASS Mon Oct 3.

Recall: Some $\mathbb{Z}$

Given $a, b \in \mathbb{Z}$ we have

$$\langle a \rangle \wedge \langle b \rangle = \langle m \rangle$$

where $m > 0$ is $\text{lcm}(a, b)$.

Note:

$\langle a \rangle \cup \langle b \rangle \leq \mathbb{Z}$ is NOT a subgroup so we must define

$$\langle a, b \rangle = \langle \langle a \rangle \cup \langle b \rangle \rangle = \bigcap_{\substack{H \leq \mathbb{Z} \\ \langle a \rangle \cup \langle b \rangle \subseteq H}} H \leq \mathbb{Z}$$

↑ HW 2.3.

Then $\langle a, b \rangle = \langle d \rangle$

where $d > 0$ is $\gcd(a, b)$.

For general group G with subgroups $H, K \leq G$ we define

$$H \wedge K := H \cap K \leq G.$$

$$H \vee K := \langle H \cup K \rangle \leq G.$$

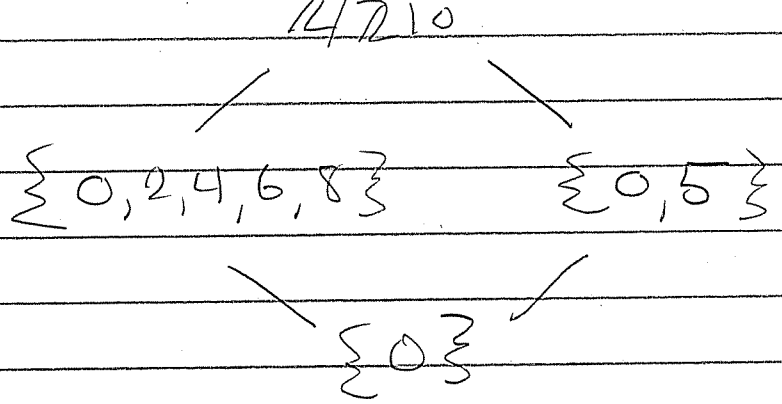
↳ smallest group containing $H \cup K$.

The set of subgps of G together with $(\wedge, \vee, \leq)$

$\wedge$: meet, $\vee$: join, $\leq$: subgroup (partial order)

is called a "Lattice".

eg. The subgroup lattice of $\mathbb{Z}/\mathbb{Z}10$.



Recall: Given a set S we have

partitions of S	$\longleftrightarrow$	Equivalence Relations $\sim$ on S

Let $\sim$ be an equivalence on S. i.e. $\forall x,y,z \in S$

- $x \sim y$ & $y \sim z \Rightarrow x \sim z$ (trans.)
- $x \sim y$ & $y \sim x$ (symm.)
- $x \sim x$ (reflex.)

For $x \in S$ define $C_x := \{ y \in S : x \sim y \}$

(Alternative: Say $C_x = [x]$)

the equivalence class of x.

Since $x \in C_x$, have $S = \bigcup_{x \in S} C_x$

Fact (Lemma 2.7.6.)

If $C_x \cap C_y \neq \emptyset$ then $C_x = C_y$. ///

Corollary: The classes C_x partition S.

Choose (arbitrarily) a class rep from each $\sim$-class. Say $X = \{\text{class reps}\}$

Then $S = \coprod_{x \in X} C_x$ ← disjoint union!

Notation:

- X is a "transversal" for $\sim$
- $S/\sim$ = the set of $\sim$-classes
  "Say S mod $\sim$"
- $S/\sim$ and X are not EQUAL, but

$S/\sim \Leftrightarrow X$
class $\Leftrightarrow$ class rep. } natural bijection

eg Given $n \in \mathbb{Z}$ define a relation $\equiv_n$ on $\mathbb{Z}$ by

$$a \equiv_n b \iff n \mid a-b.$$

(Say "$a = b \bmod n$" for $a \equiv_n b$).

Claim: $\equiv_n$ is an equivalence

Proof:

Transitive. Suppose $a \equiv_n b$ and $b \equiv_n c$.
i.e. $\exists\, k, l \in \mathbb{Z} \ni a-b = nk$ & $b-c = nl$.
Then $a-c = (a-b)+(b-c) = nk+nl = n(k+l)$
$\Rightarrow a \equiv_n c$.

Symmetric. Suppose $a \equiv_n b$ i.e. $\exists\, k \in \mathbb{Z}$
$\ni a-b = nk$. Then $b-a = n(-k)$
$\Rightarrow b \equiv_n a$.

Reflexive. For all $a \in \mathbb{Z}$ we have
$a-a = n0 \Rightarrow a \equiv_n a$ ▨

Notation:

- $\equiv_n$ is called "congruence modulo n"
- $\forall\, a \in \mathbb{Z}$ let

$$[a] = \{b \in \mathbb{Z} : a = b \bmod n\}$$
$$= \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$$
$$= "a + \mathbb{Z}n"$$

The congruence class of $a \pmod n$.

Hence

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [n-1]$$

partition

$$\mathbb{Z}/\equiv_n = \{[0], [1], \ldots, [n-1]\}$$

Another name: $\mathbb{Z}/\equiv_n = \mathbb{Z}/n\mathbb{Z}$.

A transversal? $\{0, 1, 2, \ldots, n-1\}$.

$\{0, 1, \ldots, n-1\} \hookrightarrow \{[0], [1], \ldots, [n-1]\}$

class reps $\neq$ classes

General Story: Consider subgroup $H \leq G$.
Define a relation $\equiv_H$ on G by

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

"congruent mod H"

Check that $\equiv_H$ is an equivalence.

Classes are called cosets.

↓

$$[a] = \{ b \in H : \exists h \in H,\ a^{-1}b = h \}$$
$$= \{ b \in H : \exists h \in H,\ b = ah \}.$$
$$= \{ ah : h \in H \}$$
$$= aH$$

the (left) coset gen. by a.

Cor 2.8.3: The left cosets of H partition G.

Notation: Let

G/H = the set of left H-cosets.

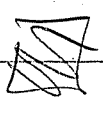
Theorem (Lagrange's Theorem):

For $|G| < \infty$ $\quad |G/H| = |G|/|H|$

i.e. (size of G) = (size of H)(# H-cosets).

Proof: Since the cosets partition G, we only need to show all cosets have the same size. Given any $a \in G$ we define a map $H \to aH$ by $h \mapsto ah$. It is invertible ($h \mapsto a^{-1}h$) hence bijective. Thus for any $a, b \in G$, we have

$$|aH| = |H| = |bH|$$



Notation: # H-cosets is called

$$[G:H] = |G/H|$$

the index of H in G.

Lagrange: $|G| = |H|\,[G:H]$ ///

eg for $\mathbb{Z}n \leq \mathbb{Z}$

congruence mod n $\Longleftrightarrow$ congruence mod $\mathbb{Z}n$.

$\mathbb{Z}/\equiv_n \;\longleftrightarrow\; \mathbb{Z}/\mathbb{Z}n$

cosets of $\mathbb{Z}n$.

Coset of $a \in \mathbb{Z}$ is "$a\mathbb{Z}n$"?

"$a + \mathbb{Z}n$". additive

Index: $[\mathbb{Z}:\mathbb{Z}n] = n$

Lagrange: $|\mathbb{Z}| = |\mathbb{Z}n| \cdot [\mathbb{Z}:\mathbb{Z}n]$

$\infty = \infty \cdot n$? OK

=

Next Idea: The ~~set~~ G/H

might have more structure...

group?, space?, manifold?, etc.

HW 2 due NOW
Exam 1 Wednesday
NO O.H. Thurs
No Class Monday.

Today: HW 2 solutions
& Review.

Def: A group is a set G with a map $G \times G \to G$ written as $(a,b) \mapsto ab$ satisfying

(1) $\forall a,b \in G$, $a(bc) = (ab)c$.
(2) $\exists e \in G$, $\forall a \in G$, $ae = ea = a$.
(3) $\forall a \in G$, $\exists b \in G$, $ab = ba = e$

Problem 2: Let (3') $\forall a \in G \; \exists b \in G$, $ab = e$.
(right inverses exist)
Prove that (1)+(2)+(3) $\Longleftrightarrow$ (1)+(2)+(3')
i.e. (3) $\Longleftrightarrow$ (3') in the presence of (1)+(2).

Proof: Assume (1)+(2) throughout.
If (3) then clearly (3'). Conversely, suppose (3') holds. Claim: Then (3) holds.
To see this let $a \in G$. By (3') $\exists b, c \in G$ $\ni$ $ab = e$ and $bc = e$. But then

$$a = ae = a(bc) = (ab)c = ec = c.$$

Hence $ab = ba = e$, and (3) holds ∎

(Axioms are somewhat flexible).

Let $\varphi: G \to H$.

Set Properties

φ is injective (1:1) $\iff (\forall a,b \in G,\ \varphi(a)=\varphi(b) \Rightarrow a=b)$

φ is surjective (onto) $\iff (\forall h \in H\ \exists g \in G,\ \varphi(g)=h)$.

injection + surjection = bijection

(bijection: $G \to G$) = "permutation"

Group Property

φ is homomorphism $\iff \varphi(ab) = \varphi(a)\varphi(b)\ \forall a,b \in G.$

(ab in G; $\varphi(a)\varphi(b)$ in H)

hom. + bij. = isomorphism.

hom. + perm. = automorphism.

Problem 4

Consider hom $\varphi: \mathbb{Z} \to G$.

If $\varphi(1) = g \in G$, What is $\varphi(n)$?

$\varphi(n) = \varphi(\overbrace{1+1+\cdots+1}^{n \text{ times}})$

$= \varphi(1)\varphi(1)\cdots\varphi(1)$

$= g g \cdots g$

$= g^n$ for $n \in \mathbb{Z}$, $n \geq 1$.

$\varphi(0) = ?$

[Recall : hom. $\varphi: G \to H$.
$\Rightarrow \varphi(1_G) = 1_H$ and $\varphi(a)^{-1} = \varphi(a^{-1})$ $\forall a \in G$]

So $\varphi(0) = \underset{\downarrow}{e} \in G$

$\varphi(-n) = (g^n)^{-1} = (g^{-1})^n$ $\forall n \in \mathbb{Z}$, $n \geq 1$

Hence $\boxed{\varphi(n) = g^n \ \forall n \in \mathbb{Z}}$

[φ is determined by $\varphi(1)$.
since $\mathbb{Z}$ is "generated" by 1]

$\Rightarrow \operatorname{im}\varphi = \{ g^n : n \in \mathbb{Z} \} = \langle g \rangle \leq G$.

$\ker\varphi = \{ n \in \mathbb{Z} : g^n = e \}$.

Suppose $|\langle g \rangle| = a < \infty$

So $g^n = e \iff a \mid n \iff n \in a\mathbb{Z}$

So $\ker\varphi = a\mathbb{Z} \leq \mathbb{Z}$

What if $|\langle g \rangle| = \infty$. $= 0\mathbb{Z}$.

Then $g^n = e \iff n = 0$, so $\ker \varphi = \{0\}$.

Summary: $\operatorname{im} \varphi = \langle g \rangle \leq G$

$$\ker \varphi = \begin{cases} |\langle g \rangle| \mathbb{Z} & \text{if } |\langle g \rangle| < \infty \\ 0\mathbb{Z} & \text{else.} \end{cases}$$

(Idea: $0\mathbb{Z} = \infty\mathbb{Z}$ ... ?)

Now consider hom $\varphi : \mathbb{Z} \to \mathbb{Z}$.

Determined by $\varphi(1) = n \in \mathbb{Z}$.

[i.e. $\operatorname{Hom}(\mathbb{Z}, \mathbb{Z}) \hookrightarrow \mathbb{Z}$]

For which n is φ an automorphism?

Need surjective, i.e. $\operatorname{im} \varphi = n\mathbb{Z} = \mathbb{Z}$.

$n\mathbb{Z} = \mathbb{Z} \implies n = +1$ or -1.

↑ the generators of $\mathbb{Z}$

In either case, $\ker \varphi = \{0\}$.

Summary: $\mathbb{Z}$ has exactly 2 automorphs.

$\varphi_1(1) := 1$ and $\varphi_2(1) := -1$.

$Aut(\mathbb{Z}) = \{\varphi_1, \varphi_2\}$

Group table

$\circ$	φ_1	φ_2
φ_1	φ_1	φ_2
φ_2	φ_2	φ_1

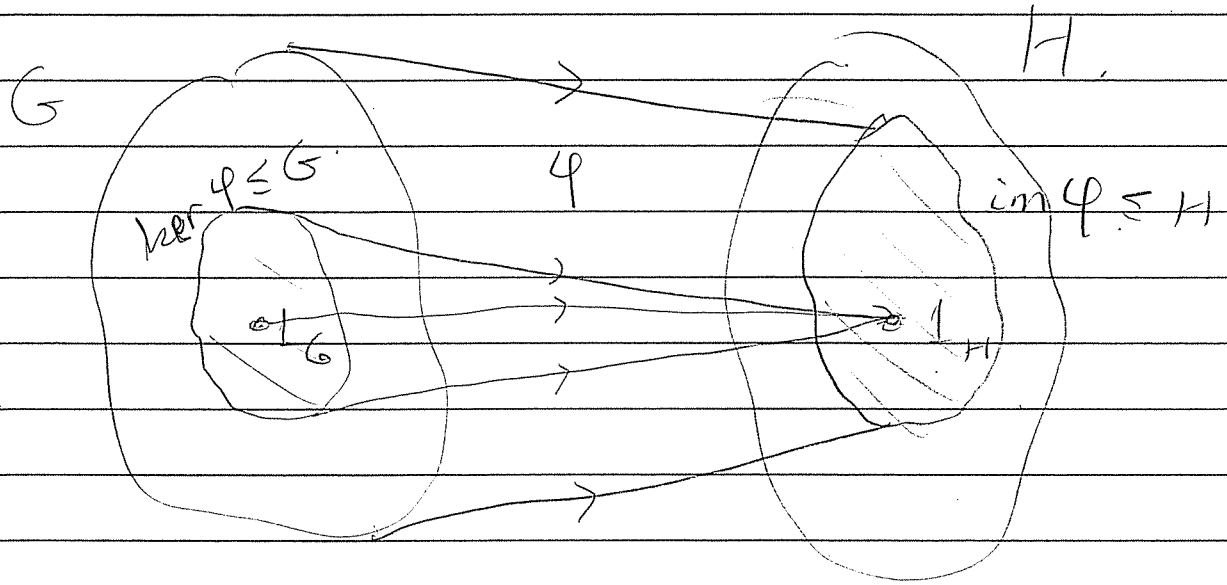
Def: $H \subseteq G$ is a subgroup if

1. $\forall a, b \in H$, $ab \in H$.
2. $e \in H$
3. $\forall a \in H$, $a^{-1} \in H$.

We write $H \leq G$.

Fact $\varphi: G \xrightarrow{\text{hom.}} H$

$\ker \varphi$ $\quad$ $\text{im}\, \varphi$



Be able to prove.

Example: Define a map $\phi : G \to Aut(G)$, where $\phi(g) = \phi_g$ is the map $\phi_g : G \to G$ defined by $\phi_g(h) = ghg^{-1}$ $\forall h \in G$.

Claim: $\forall g \in G$, $\phi_g : G \to G$ is automorph

Proof: HW 1.4.

Hence indeed $\phi : G \to Aut(G)$

Claim: ϕ is a hom.

Proof: We must show $\forall g, h \in G$ that

$$\phi_{gh} = \phi_g \circ \phi_h.$$

Indeed, $\forall a \in G$ we have.

$$\begin{aligned} \phi_g(\phi_h(a)) &= \phi_g(hah^{-1}) \\ &= g(hah^{-1})g^{-1} \\ &= (gh)a(hg)^{-1} \\ &= \phi_{gh}(a) \end{aligned}$$

Image has a special name

$\operatorname{im}\phi = Inn(G) \leq Aut(G)$

"inner automorphisms of G".

$\ker\Phi = ? = \{ g \in G : \Phi_g = id \}$

$= \{ g \in G : \Phi_g(h) = h \ \forall\, h \in G \}$

$= \{ g \in G : ghg^{-1} = h \ \forall\, h \in G \}$

$= \{ g \in G : gh = hg \ \forall\, h \in G \}$

$= Z(G)$

the center of G.

Cor: $Z(G) \leq G$

normal.

In particular, $Z(G) \trianglelefteq G$

Recall: An Equivalence Relation $\sim$ satisfies

(1) $x \sim y$ & $y \sim z \Rightarrow x \sim z$

(2) $x \sim y \Rightarrow y \sim x$

(3) $x \sim x \ \forall\, x$

"conjugacy relation"

Problem 8: Say $a \sim b$ if $\exists\, g \in G$, $a = gbg^{-1}$

Prove $\sim$ is an equivalence.

(1) Suppose $a \sim b$ and $b \sim c$ i.e. $\exists\, g, h \in H$, $a = gbg^{-1}$ and $b = hch^{-1}$. But then $a = gbg^{-1} = g(hch^{-1})g^{-1} = (gh)c(gh)^{-1}$

Hence $a \sim c$ as desired. ✓

(2) Sp. $a \sim b$ i.e. $\exists\, g \in G$, $a = gbg^{-1}$

But then $b = (g^{-1})a(g^{-1})^{-1}$. Hence $b \sim a$.

(3) $a = eae^{-1} \Rightarrow a \sim a \ \forall\, a \in G$

$\sim$-classes are called conjugacy classes