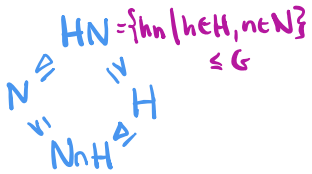
Math 3700 11/15 and 11/17

Today: other isom thms
HW 9
↳ SES
↳ gp extensions
↳ free gps
↳ gp presentations

Isomorphism Thms at Lightning Speed

① Let $\phi: G \to G'$ be a gp hom. Then
$$G/\ker\phi \cong G'$$

② Let $H \leq G$ and $N \trianglelefteq G$. Then



and $HN/N \cong H/N\cap H$.

③ Let $N \trianglelefteq G$. Then

+④ $\{$normal subgps of $G/N\}$ $\longleftrightarrow$ $\{$normal subgps of G containing $N\}$
M/N $\qquad$ $N \leq M \leq G$

and $(G/N)/(M/N) \cong G/M$.

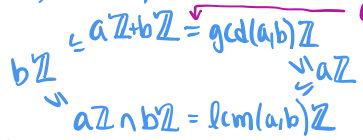
Note: $|G/M| = |G/N| \cdot |M/N|$.

Examples using them

last time

Prove: $\text{lcm}(a,b)\gcd(a,b) = ab$

Let $G = \mathbb{Z}$, $H = a\mathbb{Z}$, $N = b\mathbb{Z}$. Then



so $\gcd\mathbb{Z}/b\mathbb{Z} \cong a\mathbb{Z}/\text{lcm}\mathbb{Z} \Rightarrow \frac{\gcd}{b} = \frac{a}{\text{lcm}}$.

Recall $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$ and $SL_n(\mathbb{R}) = \ker(\det)$
for $\det: GL_n(\mathbb{R}) \to \mathbb{R}^\times$. By 1st iso, $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$
so 3rd iso $\{$subgps of $\mathbb{R}^\times\}$ $\longleftrightarrow$ $\{$subgps of $GL_n(\mathbb{R})$ containing $SL_n(\mathbb{R})\}$

Since all subgps of $\mathbb{R}^\times$ are normal, all subgps of $GL_n(\mathbb{R})$ containing $SL_n(\mathbb{R})$ are normal (!)

Short Exact Sequences of Groups

A **short exact sequence** (SES) of groups is notation

$$e \to N \xrightarrow{i} G \xrightarrow{p} Q \to e$$ ← often 1 or 0 (if Abelian)

which neatly packages a lot of info:

- N, G, Q are groups and i, p are gp homs
- i is injective $1 \to N \xrightarrow{i} G$
- p is surjective $G \xrightarrow{p} Q \to 1$
- $\ker(p) = \text{im}(i)$ $\quad N \xrightarrow{i} G \xrightarrow{p} Q$

What is this telling us?

① we know $\ker(p) \trianglelefteq G$, and by 1st iso
$$G/\ker(p) \cong \text{im}(p)$$
② But p is surjective, so $G/\ker(p) \cong \text{im}(p) = Q$.

(3) By exactness, $\ker(p) = \mathrm{im}(i)$ so $G/\mathrm{im}(i) \cong Q$.

(4) But i is injective, so $N \cong \mathrm{im}(i)$, hence

$$"\ G/N \cong Q\ "$$

↪ quotations b/c it's really $G/i(N) \cong Q$ but $i(N) \cong N$ sooo...

The gp G is called the extension of Q by N.

Sometimes, $G \cong N \times G/N \cong N \times Q$. ♀ not always!

Examples (from HW9 Exc1)

1. $0 \to 2\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{q} \mathbb{Z}/2 \to 0$

$a \mapsto a$

$b \mapsto b \bmod 2$

(i) everything involved is a gp + gp hom

(ii) i is injective since if $a, b \in 2\mathbb{Z}$ are equal in $\mathbb{Z}$, then equal in $2\mathbb{Z}$.

(iii) q is surjective since $0, 1 \in \mathbb{Z}$ map to $[0], [1]$

(iv) $\ker(q) = \mathrm{im}(i)$ ...

If $q(a) = 0$ then $a = 2k$ for some $k \in \mathbb{Z}$, i.e. $a \in 2\mathbb{Z}$, so $\ker(q) \subseteq \mathrm{im}(i)$.

If $a \in \mathrm{im}(i)$ then $a = 2k$ for some $k \in \mathbb{Z}$ so $q(a) = q(2k) = 0$, hence $\mathrm{im}(i) \subseteq \ker(q)$. □

Note $\mathbb{Z} \not\cong 2\mathbb{Z} \times \mathbb{Z}/2$ e.g. the RHS has non-id elmt $(0,1)$ of finite order

but we can understand elmts of $\mathbb{Z}$ as "$2\mathbb{Z}$ part" plus "1 or 0".

2. $0 \to \mathbb{Z}/2 \xrightarrow{i} \mathbb{Z}/2 \times \mathbb{Z}/2 \xrightarrow{\pi_2} \mathbb{Z}/2 \to 0$

$a \mapsto (a, 0)$

$(a, b) \mapsto b$

(ii) i is injective since if $(a,0) = (a',0)$ then $a = a'$.

(iii) π_2 is surjective since for any $b \in \mathbb{Z}/2$, $\pi_2(0, b) = b$.

(iv) $\mathrm{im}(i) = \ker(\pi_2)$:

$$\ker(\pi_2) = \{(a,b) \mid 0 = q(a,b) = b\}$$
$$= \{(a,0) \mid a \in \mathbb{Z}/2\}$$

and $\mathrm{im}(i) = \{(a,0) \mid a \in \mathbb{Z}/2\}$, so they're equal.

Note $\mathbb{Z}/2 \times \mathbb{Z}/2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ duh...

Idea: A SES $e \to N \to G \to Q \to e$ is "split" if $G \cong N \times Q$". Otherwise, non-split.

Claim $e \to N \xrightarrow{i} N \times Q \xrightarrow{p} Q \to e$ is a SES

$n \mapsto (n, e)$

$(n, g) \mapsto g$

(iv) $\mathrm{im}(i) = \ker(p)$

($\subseteq$) Suppose $(n,g) \in \mathrm{im}(i)$. Then $g = e$, so $p(n,g) = p(n,e) = e \in Q$ so $(n,g) \in \ker(p)$.

($\supseteq$) Suppose $(n,g) \in \ker(p)$, so $p(n,g) = e$. This means $g = e$ so $(n,g) = (n,e) = i(n) \in \mathrm{im}(i)$.

□

Defn A SES $e \to N \underset{r}{\overset{i}{\rightleftarrows}} G \xrightarrow{p} Q \to e$ is **split** if $\exists r: G \to N$ s.t. $r \circ i = id_N$

↑ "retraction"

Q. Why is this the same as "$G \cong N \times Q$"? ↖ or "G is split extension"

A. Exc 2(2)

Prop - A SES splits iff $\exists \alpha: G \xrightarrow{\cong} N \times Q$ s.t. TFDC:

$$\begin{array}{ccccccccc} e & \to & N & \xrightarrow{i} & G & \xrightarrow{p} & Q & \to & e \\ \| & & \| & ① & \downarrow \alpha & ② & \| & & \| \\ e & \to & N & \xrightarrow[i_N]{} & N \times Q & \xrightarrow[\pi_2]{} & Q & \to & e \end{array}$$

① $\alpha(i(n)) = i_N(n) = (n, e)$

② $p(g) = \pi_2(\alpha(g)) \Rightarrow \alpha(g) = (?, p(g))$

Proof: ($\Leftarrow$) Suppose $\exists \alpha: G \xrightarrow{\cong} N \times Q$ which commutes appropriately. Define $r: G \to N$ by

$$r: G \xrightarrow{\alpha} N \times Q \xrightarrow{\pi_1} N$$
$$g \mapsto \alpha(g)$$
$$(n, q) \mapsto n$$

i.e. $r = \pi_1 \circ \alpha$

Then r is a gp hom since both α and π_1 are, and $r \circ i(n) = \pi_1 \circ \alpha(i(n)) = \pi_1(n, e) = n$.

($\Rightarrow$) Suppose $\exists r: G \to N$ s.t. $r \circ i = id_N$. Define $\alpha: G \to N \times Q$ by

$$\alpha(g) = (r(g), p(g)).$$

Note that α is a gp hom since r and g are, and TFDC:

$$\begin{array}{ccc} g & \longmapsto & p(g) \\ G & \to & Q \\ \alpha \downarrow & & \| \\ N \times Q & \to & Q \\ (r(g), p(g)) & \mapsto & p(g) \end{array}$$

$$\begin{array}{ccc} n & \longmapsto & i(n) \\ N & \to & G \\ \| & & \downarrow \alpha \\ n & N \to N \times Q & (\alpha(i(n)) \| p(i(n))) \\ & \searrow \quad \nearrow & \\ & (n, e) & \bigstar \end{array}$$

$\bigstar$ $r(i(n)) = (r \circ i)(n) = n$ and $p(i(n)) = e$ since $\operatorname{im}(i) = \ker(q)$.

Remains to show α is bijective.

(injective). Suppose $\alpha(g) = e$, so $r(g) = e = p(g)$. This means $g \in \ker(p) = \operatorname{im}(i)$, so $g = i(n)$ for some $n \in N$. But then $e = r(g) = r(i(n)) = n$, so $n = e$. Hence $g = i(e) = e$.

(surjective). Let $(n, q) \in N \times Q$. WTS $\exists g$ s.t. $(n, q) = \alpha(g) = (r(g), p(g))$

ASIDE

Know

- Since p is surjective, $\exists \hat{g} \in G$ s.t. $p(\hat{g}) = q$, but probably not $r(\hat{g}) = n$.
- $\alpha(i(n)) = (r(i(n)), p(i(n))) = (n, e)$

Idea: combine them

- $\alpha(i(n)\hat{g}) = \alpha(i(n))\alpha(\hat{g}) = (n, e) \cdot (r(\hat{g}), q) = (n r(\hat{g}), q)$ almost...
- $\alpha(i(n)\hat{g}\, i(r(\hat{g})^{-1})) = \alpha(i(n))\alpha(\hat{g})\alpha(i(r(\hat{g})^{-1}))$
  $= (n, e) \cdot (n\hat{g}, q) \cdot (r(\hat{g})^{-1}, e)$
  $= (n\, r(\hat{g}) r(\hat{g})^{-1}, eqe) = (n, q).$

Set $g = i(n)\cdot\hat{g}\cdot i(r(\hat{g})^{-1})$. Then $\alpha(i(n)\,\hat{g}\,i(r(\hat{g})^{-1})) = (n,q)$ by above. □

UPSHOT: Split extensions are when $G \cong N \times Q$ in a nice way. These always exist + are nice, but sometimes more interesting things happen.

Ex. two extensions of $\mathbb{Z}/2$ by $\mathbb{Z}/3$

Split: $0 \to \mathbb{Z}/3 \to \mathbb{Z}/6 \to \mathbb{Z}/2 \to 0$
$\mathbb{Z}/6 \cong \mathbb{Z}/3 \times \mathbb{Z}/2$

non-split: $0 \to \mathbb{Z}/3 \xrightarrow{i} S_3 \xrightarrow{p} \mathbb{Z}/2 \to 0$
b/c $S_3 \not\cong \mathbb{Z}/6$

$0 \mapsto e$
$1 \mapsto (123)$
$2 \mapsto (123)^2 = (132)$

What is p? $S_3/i(\mathbb{Z}/3) = \{e\langle(123)\rangle, (12)\langle(123)\rangle\}$
$\cong \downarrow$ $\quad\downarrow\quad\downarrow$
$\mathbb{Z}/2 \quad 0 \quad 1$

So $p: S_3 \to \mathbb{Z}/2$ from univ. prop.
$S_3/i(\mathbb{Z}/3) \cong$
$e, (123), (132) \mapsto 0$
$(12), (13), (23) \mapsto 1$

Note $\mathbb{Z}/3 \cong A_3$ so similar argument shows $0 \to A_3 \hookrightarrow S_3 \to \mathbb{Z}/2 \to 0$ is non-split exact.

Special examples: Group Presentations ← special kind of f.g. group

One of the ways we describe groups is using **generators** and **relations**

e.g. $\mathbb{Z}/n \cong \{[0],[1],\dots,[n-1]\} = \langle 1 \mid n\cdot 1 = 0\rangle$

$D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$ s.t. $r^4 = e$, $s^2 = e$, $rs = sr^{-1}$
$= \langle r, s \mid r^4 = e,\ rs = sr^{-1}\rangle$

$\mathbb{Z} = \langle 1 \rangle = \langle 1 \mid \phi\rangle$.

in general, $G = \langle$ letters $\mid$ relations $\rangle$ and the elmts of G are **words**.

e.g. $1+2+4-3$ is a word in $\mathbb{Z}/3$
$= 7-3 = 4 \equiv 1$ using relns ←

$rsr^3ss^{-1}r^2$ is a word in D_4 "reduced words"
$= rsr^3er^2 = rsr^5 = rsr$ using relns ←

If {relations} $= \phi$, G is called a **free group**

Defn For any set S, the **free group** on S is (lying a bit: there's a UP) the group $F(S) = \langle s \in S \mid \phi\rangle$.

Intuition S is like a "basis" for $F(S)$.

This intuition is bad b/c (1) not every gp "has a basis" (i.e. is free) (e.g. finite gps)
(2) this "basis" is non-commutative

Better intuition(?) S is an "alphabet" for $F(S)$.

Rmks.
- $F(\emptyset) = e$
- The rank of $F(S)$ is $|S|$, and $F(S) \cong F(S') \iff |S| = |S'|$.
- UP: $\mathrm{Hom}_{Gp}(F(S), G) \cong \mathrm{Hom}_{Set}(S, G)$ ← as a set
- $F(\{s\}) \cong \mathbb{Z}$
- ★ $F(S)$ is non-Abelian iff $|S| \geq 2$.
- If $H \leq F(S)$ then H is free (i.e. $H \cong F(S')$ for some S')

e.g. $F(\{x,y\}) \not\cong F(\{x\}) \times F(\{y\}) \cong \mathbb{Z} \times \mathbb{Z}$

$\mathbb{Z} * \mathbb{Z} \cong F(\{x,y\}) \ni x^{-3}y^{2}xxy^{100}ey^{-1}x \qquad (x^k, y^j) \in F(\{x\}) \times F(\{y\})$

Q. How do I get from $F(\{x,y\})$ to $F(\{x\}) \times F(\{y\})$?

A. "Abelianize": impose reln $xy = yx \iff xy(yx)^{-1} = e$, where $xy(yx)^{-1} = xyx^{-1}y^{-1} = [x,y]$

⇝ quotient by "commutator subgp"

$$F(\{x,y\}) / [F(\{x,y\}), F(\{x,y\})] \cong F\{x\} \times F\{y\}.$$

$$F(\{x,y\}) / [F(\{x,y\}), F(\{x,y\})] = \langle x, y \mid xyx^{-1}y^{-1} \rangle$$

Rmk. Can "Abelianize" any G by declaring $gh = hg$ in this way

$$G^{ab} := G / [G,G].$$

Abstract Observation if $G = \langle S \mid R \rangle$ then "$G \cong F(S)/R$"

i.e. ∃SES $1 \to N(R) \to F(S) \to G \to 1$

$N(R)$: smallest normal subgp containing $R \subseteq F(S)$.

Ex. We saw $\langle x, y \mid xyx^{-1}y^{-1} \rangle \cong \mathbb{Z}^2$

but $\langle x, y \mid x^4, y^2, xyx^{-1}y \rangle \cong D_4$

Ex (Exc 3) $G = \langle x, y \mid xy^2 \overset{①}{=} y^2x,\ x^4 \overset{②}{=} y^3 \rangle$. Show: all elmts of G can be written $y^{2k}x^r$.

From ①, even powers of y commute w/ x + can be moved to the front. From ②, $y = y^{-2}x^4$

So every word in G can be expressed using only even powers of y. Hence of the form $y^{2k}x^r$

Then: Show G Ab

Show $G \cong \mathbb{Z}$

Ex. $G = \langle x, y \mid xyx^{-1}y^{-2}, x^{-2}y^{-1}xy \rangle$

Note $xyx^{-1}y^{-2} = e \iff xy = (x^{-1}y^{-2})^{-1} = y^2x$

and $x^{-2}y^{-1}xy = e \iff xy = (x^2y^{-1})^{-1} = yx^2$

So $y^2x = yx^2$ in G. Multiplying by y^{-1}, we get $yx = x^2$ so multiplying by x^{-1} we get $y = x$. Then $xy = y^2x$ implies $x^2 = x^3$ so $x = e$ and $y = e$.

Thus $G = e$!

Hard Word Problems (early 1900s)

(1) Word Problem: can we decide when 2 words are equal?

(2) Isomorphism problem: can we decide when $\langle S \mid R \rangle \cong \langle S' \mid R' \rangle$?

↳ e.g. $\langle S \mid R \rangle = e$?

A. It's undecidable.

~ break ~

HW time: Exercise 4 only!

Exercise 4. We show in this exercise that every group is determined by its finitely generated subgroups. Conceptually, this is not surprising. The multiplication gh in G for $g, h \in G$ is entirely determined in the finitely generated subgroup $\langle g, h \rangle$.

(1) A *partially ordered set* $I = (I, \leq)$ is a non-empty set I together with a relation $\leq$ which is reflexive, antisymmetric (i.e. if $a \leq b$ and $b \leq a$, then $a = b$), and transitive. A *filtered set* $I = (I, \leq)$ is a partially ordered set together with upper bounds: for all $a, b \in I$, there exists $c \in I$ such that $a \leq c$ and $b \leq c$. Show that $(\mathbb{N}, \leq)$ and $(\mathbb{R}, \leq)$ are filtered sets.

(2) A *filtered system of groups* $I = (I, \leq)$ is a filtered set in groups: each element in I is a group and we fix injections $\iota_{HK} : H \to K$ for some pairs of groups $H, K \in I$. The relation $\leq$ is defined as $H \leq G$ if and only if we have chosen an injective homomorphism $\iota_{H,G} : H \to G$, for H, G in I. Fix now a group G and let I_G be the set of all finitely generated subgroups of G. Show that I_G is a filtered system of groups.

(3) Let I be a filtered set of groups. We define the *filtered colimit* $(G, \{f_H\}_{H \in I})$ *of* I as follows. It is a group G together with homomorphisms $f_H : H \to G$ for each $H \in I$ such that for all injective homomorphisms $\iota_{HK} : H \hookrightarrow K$ in the filtered system I, we have $f_K \circ \iota_{HK} = f_H$ for all $H, K \in I$. It respects a universal property that reads: for any other group G' with homomorphisms $\{f'_H\}_{H \in I}$ such that $f'_K \circ \iota_{HK} = f'_H$ for all $H, K \in I$, then there exists a unique homomorphism $F : G \to G'$ such that $F \circ f_H = f'_H$ for all $H \in I$. Show that given a filtered set of groups I, the filtered colimit of I is unique up to isomorphism if it exists.

(4) Let G be a group and let I_G be the filtered set as in (2). Show that G is the filtered colimit of I_G.

minute sheet

- which isothm is the best isothm?
- what was most helpful today?