Today: other isom thms

HW 9
- Syl
- ep extensions
- free gps
- gp presentations

Isomorphism Thms at Lightning Speed

0. Let \( \varphi : G \to G' \) be a gphom. Then \( G/\text{ker} \varphi \cong G' \).

2. Let \( H \leq G \) and \( N \leq G \). Then
   \[
   HN = \{hn \mid hH, nN \leq G \}
   \]
   and \( HN/N \cong H/\text{NN}H \).

3. Let \( N \leq G \). Then
   
   \[
   \frac{G}{N} \cong \frac{G/N}{\text{NN}N} \cong \frac{G/N}{\text{NN}N}.
   \]

Examples using them

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

Let \( G = \mathbb{Z} \), \( H = 2\mathbb{Z} \), \( N = 3\mathbb{Z} \). Then
   \[
   a = 2x, b = 3y, a = \frac{a}{x}, b = \frac{b}{y}, \frac{a}{x}, \frac{b}{y} \in \mathbb{Z}
   \]
   so \( \gcd(a, b) = x \) and \( \text{lcm}(a, b) = y \).

Short Exact Sequences of Groups

A short exact sequence (SES) of groups is notation

\[
\begin{array}{c}
\varepsilon \\
\rightarrow \\
N \\
\rightarrow \\
\rightarrow \\
G \rightarrow \\
P \\
\rightarrow \\
Q \\
\rightarrow \\
\rightarrow \\
e
\end{array}
\]

which neatly packages a lot of info:

- \( N, G, Q \) are groups and \( i, p \) are gphoms
- \( i \) is injective \( 1 \rightarrow N \rightarrow G \)
- \( p \) is surjective \( G \rightarrow Q \rightarrow 1 \)
- \( \text{ker}(p) = \text{im}(i) \)

What is this telling us?

1. We know \( \text{ker}(p) \leq G \), and by 1st iso
   \( G/\text{ker}(p) \cong \text{im}(p) \)
2. But \( p \) is surjective, so \( G/\text{ker}(p) \cong \text{im}(p) = Q \).
3. By exactness, \( \ker(p) = \text{im}(i) \) so \( G/\text{im}(i) \cong Q \).

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

\[
G/N \cong Q
\]

The group \( G \) is called the extension of \( Q \) by \( N \).

Sometimes, \( G \cong N \times G/N \cong N \times Q \). \( \Box \) not always!

Examples (from HW9 Exc1)

1. \[
\begin{array}{cccc}
\mathbb{Z} & \mathbb{Z}/2 & \mathbb{Z}/2 & 0 \\
a \mapsto & a & b & 0 \\
& \mapsto & b \mod 2 & 0
\end{array}
\]

(i) Everything involved is a gp \( \to \) gp hom.
(ii) \( i \) is injective since if \( a, b \in \mathbb{Z} \) are equal in \( \mathbb{Z} \), then equal in \( \mathbb{Z}/2 \).
(iii) \( q \) is surjective since \( 0, 1 \in \mathbb{Z}/2 \) map to \( [0], [1] \).

4. \( \ker(q) = \text{im}(i) \) ...

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

Note: \( \mathbb{Z} \not\cong \mathbb{Z} \times \mathbb{Z}/2 \) e.g. the RHS has non-id elem \((0, 1)\) of finite order but we can understand elmts of \( \mathbb{Z} \times \mathbb{Z}/2 \) as "\( \mathbb{Z}/2 \) part" plus "1 or 0".

2. \[
\begin{array}{cccc}
\mathbb{Z}/2 & \mathbb{Z}/2 & \mathbb{Z}/2 & 0 \\
a \mapsto & (a, 0) & (a, b) & 0 \\
& \mapsto & b & 0
\end{array}
\]

(i) \( i \) is injective since if \( (a, 0) = (a', 0) \) then \( a = a' \).
(ii) \( \pi_2 \) is surjective since for any \( b \in \mathbb{Z}/2 \), \( \pi_2(0, b) = b \).
(iv) \( \text{im}(i) = \ker(\pi_2) \):

\[
\ker(\pi_2) = \{ (a, b) | b = q(a, b) = 0 \}
\]

\[
= \{ (a, 0) | a \in \mathbb{Z}/2 \}
\]

and \( \text{im}(i) = \{ (a, 0) | a \in \mathbb{Z}/2 \} \), 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: \( e \to (n, e) \to N \times Q \to Q \to e \) is a SES

(iv) \( \text{im}(i) = \ker(p) \)

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

(\( \geq \)) Suppose \( (n, g) \in \ker(p) \), so \( p(n, g) = e \). This means \( g = e \) so \( (n, g) = (n, e) = i(n) \in \text{im}(i) \). \( \Box \)
**Def:** A SES \( e \to N \xrightarrow{\pi} G \to Q \to e \) is *split* if \( \exists \sigma : G \to N \) s.t. \( \sigma \circ i = \text{id}_N \)

**Q:** Why is this the same as "\( G \cong N \times Q \)"? (or "\( G \) is split extension")

**A.** Ex 2.2

**Prop:** A SES splits iff \( \exists \sigma : G \cong N \times Q \) s.t. TFDC:

\[
\begin{align*}
\sigma(i(n)) &= i(n) = (n,e) \\
p(q) &= \pi_2(d(g)) \Rightarrow \sigma(g) = (?, p(g))
\end{align*}
\]

**Proof:** \((\Leftarrow)\) Suppose \( \exists \sigma : G \cong N \times Q \) which commutes appropriately. Define \( r : G \to N \) by

\[
r : G \xrightarrow{\sigma} N \times Q \xrightarrow{\pi_1} N
\]

i.e. \( r = \pi_1 \circ \sigma \)

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

\((\Rightarrow)\) Suppose \( \exists r : G \to N \) s.t. \( \text{roi} = \text{id}_N \). Define \( \sigma : G \to N \times Q \) by

\[
\sigma(g) = (r(g), p(g)).
\]

Note that \( \sigma \) is a gp hom since \( r \) and \( q \) are, and TFDC:

\[
\begin{align*}
r &\rightarrow N \\
N \rightarrow Q \xleftarrow{(r(g), p(g))} N \times Q \\
G \xrightarrow{\sigma} N \times Q \xrightarrow{\pi_1} N
\end{align*}
\]

\[
\begin{align*}
r(i(n)) &= (r(i(n)), p(i(n))) = (n,e)
\end{align*}
\]

\[
\begin{align*}
r(i(n)) &= (r(i(n)), p(i(n))) = (n,e)
\end{align*}
\]

\[
\begin{align*}
r(i(n)) &= (r(i(n)), p(i(n))) = (n,e)
\end{align*}
\]

\[
\begin{align*}
r(i(n)) &= (r(i(n)), p(i(n))) = (n,e)
\end{align*}
\]

Remains to show \( \sigma \) is bijective.

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

\((\text{surjective})\) Let \( (n,e) \in N \times Q \). \text{WTS} \exists g s.t. \( (n,e) = \sigma(g) = (r(g), p(g)) \)

\[
\begin{align*}
\text{Know ASIDE}
\end{align*}
\]

- Since \( p \) is surjective, \( \exists h \in G \) s.t. \( p(h) = q \), but probably not \( r(h) = n \).
- \( \sigma(i(n)) = (r(i(n)), p(i(n))) = (n, e) \)

\[
\begin{align*}
\text{Idea: combine them}
\end{align*}
\]

- \( \sigma(i(n)h) = \sigma(i(n)) \sigma(h) = (n, e) \cdot (r(g), q) = (nr(g), q) \) almost...
- \( \sigma(i(n)h' r(g)^{-1}) = \sigma(i(n)) \sigma(h) \sigma(i(r(g)^{-1})) = (n, e) \cdot (r(g), q) \cdot (r(g)^{-1}, e) = (n, e) \cdot (r(g), q) \cdot (e, e) = (n, e) \cdot (r(g), q) = (n, q) \).
Set \( g = i(n) \circ i(r(g)^{-1}) \). Then \( L(i(n) \circ i(r(g)^{-1})) = (n,q) \) by above. \( \square \)

**UPSHOT:** Split extensions are when \( G \cong \mathbb{Z} \times Q \) in a nice way. These always exist and are nice, but sometimes more interesting things happen.

**Ex.** two extensions of \( \mathbb{Z}/2 \) by \( \mathbb{Z}/3 \\
\\split \quad 0 \to \mathbb{Z}/3 \to \mathbb{Z}/6 \to \mathbb{Z}/2 \to 0 \\
\\\downarrow \quad \downarrow \quad \downarrow \\
\\2/3 \times \mathbb{Z}/2 \\
\\non-split \quad 0 \to \mathbb{Z}/3 \to S_3 \to \mathbb{Z}/2 \to 0 \\
\\\text{by } S_3 \not\cong \mathbb{Z}/6 \\
\\0 \mapsto e \\
\\1 \mapsto (123) \\
\\2 \mapsto (123)^2 = (132) \\
\\\text{What is } p? S_3/\langle (123) \rangle = \langle \{ (123), (12) \mid (123)^2 \} \rangle \\
\\\text{So } p : S_3 \to \mathbb{Z}/2 \text{ from univ. prop.} \\
\\pmb{Note} \quad \mathbb{Z}/3 \cong A_3 \text{ so similar argument shows } 0 \to A_3 \to S_3 \to \mathbb{Z}/2 \to 0 \text{ is non-split w/o aor.}

**Special examples:** Group Presentations \( \leftrightarrow \) special kind of f.g. group

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

\( \text{e.g. } \mathbb{Z}/n \cong \{ [0], [1], \ldots, [n-1] \} = \langle 1 | n \cdot 1 = 0 \rangle \)

\( D_4 = \{ e, r, r^2, r^3, sr, sr^2, sr^3 \} \text{ s.t. } r^4 = e, rs = sr^{-1} \)

\( \mathbb{Z} = \langle 1 \rangle = \langle 1 | \phi \rangle. \)

In general, \( G = \langle \text{letters } | \text{relations} \rangle \) and the elements of \( G \) are words.

\( \text{e.g. } 1 + 2 + 4 - 3 \text{ is a word in } \mathbb{Z}/3 \)

\( = 9 - 3 = 4 \equiv 1 \) using relns \( \leftarrow \text{"reduced words"} \)

\( rsr^3s^{-1}r^2 \text{ is a word in } D_4 \)

\( = rsr^3r^2 = r^5 \text{ using relns} \)

If \{relations\} = \phi, \( G \) is called a free group \( \text{lying a bit: there's a UP} \)

**Defn** For any set \( S \), the free group on \( S \) is the group \( F(S) = \langle s \in S | \phi \rangle. \)

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

This intuition is bad \( \text{b/c} \)

1. not every gp "has a basis" (i.e. is free)
2. this "basis" is non-commutative
Better intuition? S is an "alphabet* for F(S).

Remarks.
- \( F(\emptyset) = \mathbb{E} \)
- The rank of \( F(S) \) is \( |S| \), and \( F(S) \cong F(S') \iff |S| = |S'| \).
- UP: \( \text{Hom}_{gp}(F(S), G) \cong \text{Hom}_{sets}(S, G) \) as a set.
- \( F(S,3) \cong \mathbb{Z} \)
- \( F(S) \) is non-Abelian if \( |S| \geq 2 \).
- If \( H \subseteq F(S) \) then \( H \) is free (i.e. \( H \cong F(S') \) for some \( S' \)).

E.g. \( F(x,y) \) is not \( F(x) \times F(y) \), \( F(S) \cong \mathbb{Z} \times \mathbb{Z} \)

\[ x^2 y^2 \] \[ (x^k, y^j) \]

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

A. "Abelianize"; impose relations \( xy = yx \iff xy(yx^{-1}) = e \)

\[ x \mapsto \text{quotient by } "\text{commutator subgp}" \]

\[ [F(x,y)] \cong F(x,y) \times F(x,y) \]

\[ <x,y | xyx^{-1}y^{-1}> \]

Remark. Can "Abelianize" any \( G \) by declaring \( gh = hg \) in this way.

\[ G_{ab} = G/[G,G] \]

Abstract Observation. If \( G = <S | R> \) then "\( G \cong F(S)/R \)"

\[ 1 \rightarrow N(R) \rightarrow F(S) \rightarrow G \rightarrow 1 \]

Smallest normal subgroup containing \( R \) contained in \( F(S) \).

Ex. We saw \( <x,y | xyx^{-1}y^{-1}> \cong \mathbb{Z}^2 \)

but \( <x,y | x^4, y^2, xyx^y> \cong D_4 \)

Ex (Ex 3) \( G = <x,y | xy^2 = yx^2 = y^4 = 1> \). Show: all elements of \( G \) can be written \( y^kx^r \).

From 0, even powers of \( y \) commute with \( x \), so can be moved to the front. From \( \odot \), \( y^2 = y^2x^4 \)

So every word in \( G \) can be expressed using only even powers of \( y \). Hence of the form \( y^kx^r \).

Then: Show \( G \) Ab

Show \( G \cong \mathbb{Z} \).
Ex. \( G = \langle x, y \mid xyx^{-1}y^{-2}, x^2y^3xy \rangle \)

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

and \( x^2y^3xy = e \iff x \cdot y \cdot (x^2y^3)^{-1} = yx^2 \)

So \( y^2x \cdot y \cdot x^2 \) in \( G \). Multiplying by \( y^{-1} \), we get \( yx = x^2 \) so multiplying by \( x^{-1} \)
we get \( y = x \). Then \( x \cdot y \cdot y^2 \cdot x \) 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 \( \langle S | R \rangle \cong \langle S' | R' \rangle \)?

\( \rightarrow \) e.g. \( \langle S | R \rangle = e ? \)

\( \rightarrow \) It's undecidable.

---

**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 \( \iota_{HG} : H \to G \), 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 \( \{ G, \{ f_I \}_{I \in I} \} \) 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 \( \iota_{HK} : H \to K \) 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 \( \{ f'_{I} \}_{I \in I} \) 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 \( I_G \).