Math 322, Lecture 7, 28/9/2017

- PS 1, PS2 in filing cabinet next to MATH 225

Last time: - Group axioms, examples
- Homomorphisms: $f(gh) = f(g)f(h)$

Today: - subgroups
- orders of elements
- cyclic groups

Lemma: Let $(G, \cdot)$ be a group, and let $H \subset G$ be non-empty, and closed under $\cdot$, $^{-1}$ (if $h, g \in H$ then $hg \in H$, $h^{-1} \in H$). Then $(H, \cdot\restriction_{H \times H})$ is a group

Pf: Let $x \in H$ be any element. Then $e_G = x x^{-1} \in H$, similarly if $x \in H$ have $x^{-1} \in H$ then $x^{-1} x = e_G$.

That $(xy)z = x(yz)$, $ex = x$ hold for all $x, y, z \in H$ is true because they are true in G.

Remark: (1) to check if H is non-empty, check if $e \in H$.
(2) combine operations: equivalently have H closed under map $(x, y) \mapsto xy^{-1}$.

Examples: (1) $n\mathbb{Z}$ $(n \geq 0)$ are the subgroups of $\mathbb{Z}$
(2) $\mathbb{Z}_{\geq 0} \subset \mathbb{Z}$ closed under $+$, has 0, no inverses

Pf: (this list exhausts the subgps of $\mathbb{Z}$, hence the possibilities for $\mathrm{Ker}(f)$)

(1) In this case f is injective, f is also always surjective on $\langle g \rangle$. So f is an isom.

(2) Suppose $\mathrm{Ker}(f) = n\mathbb{Z}$, $n \geq 1$, define $\bar{f} : \mathbb{Z}/n\mathbb{Z} \to G$ by

$$\bar{f}([a]_n) = f(a) = g^a.$$

• $\bar{f}$ is well-def: if $a \equiv a' \ (n)$ then $g^{a'} = g^a \cdot g^{a'-a}$

$$= \underset{\substack{\uparrow \\ n \mid a'-a}}{g^a \cdot g^{n \cdot \frac{a'-a}{n}}} = g^a \cdot (g^n)^{\frac{a'-a}{n}} = g^a \cdot e^{\frac{a'-a}{n}} = g^a$$

(or $g^{a'} = g^a \cdot g^{a'-a}$ and $a'-a \in n\mathbb{Z} = \mathrm{Ker}(f)$)

• $\bar{f}$ is a hom: $\bar{f}([a]_n + [b]_n) = \bar{f}([a+b]_n) = g^{a+b} =$

$$= \underset{\substack{\uparrow \\ f \text{ is a hom}}}{g^a g^b} = \bar{f}([a]_n) \cdot \bar{f}([b]_n)$$

• $\bar{f}$ injective:

suppose $\bar{f}([a]_n) = \bar{f}([b]_n)$, that is $g^a = g^b$.

Then $g^{a-b} = g^a (g^b)^{-1} = e$, i.e. $a-b \in \mathrm{Ker}(f) = n\mathbb{Z}$

so $a \equiv b \ (n)$

• $\bar{f}$ is surjective because f is: any $x \in \langle g \rangle$ has the form g^a, i.e. $\bar{f}([a]_n)$.

Def: the order of $g \in G$ is the order (no. of elements) of $\langle g \rangle$.

Cor: order(g) = smallest $k \geq 1$ s.t. $g^k = e$ (if finite)

Def: (PS3) For $g \in G$ set $g^0 = e$, $g^{n+1} = g^n \cdot g$. for $n \geq 0$,
set $g^{-n} = (g^{-1})^n$ for $n \geq 0$.

Lemma: (PS3) $g^n g^m = g^{n+m}$, $(g^n)^m = g^{nm}$.

i.e. map $n \mapsto g^n$ is a gp hom $\mathbb{Z} \to G$.

Lemma: The image $\{g^n\}_{n \in \mathbb{Z}}$ of this homomorphism is the smallest subgroup containing g. Denote it $\langle g \rangle$, call it "the subgp generated by g".

Pf: The image of any hom is a subgp. If $g \in H$ then $g^n \in H$ for any n (H is closed under $\cdot, ^{-1}$) so $\langle g \rangle \subseteq H$.

Eg: $G = \mathbb{Z}$, $g = m$ $\quad \langle g \rangle = \{0, m, m+m, m+m+m, \ldots$
$-m, -m-m, -m-m-m, \ldots\}$
$= m\mathbb{Z}$

Def: A group G is <u>cyclic</u> if $G = \langle g \rangle$ for some $g \in G$.

Eg: $\mathbb{Z} = \langle 1 \rangle$, $(\mathbb{Z}/n\mathbb{Z}, +) = \langle [1]_n \rangle$ are non-isom cyclic groups

Prop: Let G be cyclic, generated by g, let $f(n) = g^n$ be the std hom $f: \mathbb{Z} \to G$. Then either:

(1) $\ker f = \{0\}$, f is an isom

(2) $\ker f = n\mathbb{Z}$ and f induces an isom $\mathbb{Z}/n\mathbb{Z} \to G$.

Question: Is every subgp is the kernel of a hom?
the image?

Ex: Every subspace of a vector space is the kernel of a linear map

Lemma: $f \in \mathrm{Hom}(G, H)$ is injective iff $\mathrm{Ker}(f) = \{e_G\}$

Orders of elements

In $(\mathbb{Z}/8\mathbb{Z})^\times$ have $1 \equiv 1 \ (8)$
$3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \ (8)$
(but $3, 5, 7 \not\equiv 1 \ (8)$)

In $(\mathbb{Z}/5\mathbb{Z})^\times$ have $1 \equiv 1 \ (5)$
$4^2 \equiv 1 \ (5)$
$2^4 \equiv 3^4 \equiv 1 \ (5)$ but $2^2 \equiv 3^2 \equiv -1 \not\equiv 1 \ (5)$

Say: $[3], [5], [7]$ have order 2 in $(\mathbb{Z}/8\mathbb{Z})^\times$
$[2], [3]$ have order 4 in $(\mathbb{Z}/5\mathbb{Z})^\times$.

Cor $(\mathbb{Z}/8\mathbb{Z})^\times \not\cong (\mathbb{Z}/5\mathbb{Z})^\times$

Pf: Let $f \in \mathrm{Hom}((\mathbb{Z}/8\mathbb{Z})^\times, (\mathbb{Z}/5\mathbb{Z})^\times)$.
Then for any $x \in (\mathbb{Z}/8\mathbb{Z})^\times$ $x^2 = [1]_8$
so $[1]_5 = f([1]_8) = f(x^2) = (f(x))^2$
in particular, f is not surjective

(3) $\Gamma = (V, \in)$ graph. $Aut(\Gamma) = \{\sigma \in S_V \mid \sigma$ preserves ~~adjacenc~~ adjacency $\}$

is a subgp of S_V.

(need to ~~do~~ check: suppose $\forall (x \sim y$ iff $\sigma(x) \sim \sigma(y))$

then $(x \sim y$ iff $\sigma^{-1}(x) \sim \sigma^{-1}(y))$

and suppose $((x \sim y$ iff $\sigma(x) \sim \sigma(y))$ and $(x \sim y$ iff $\tau(x) \sim \tau(y))$

$\overset{(!)}{\Downarrow}$

$(x \sim y$ iff $(\sigma\tau)(x) \sim (\sigma\tau)(y))$.

(use subgp idea so don't have to check $Aut(\Gamma)$ is a gp)

Import kinds of subgps:

<u>Def:</u> let $f \in Hom(G, H)$. The <u>Kernel</u> of f is $f^{-1}(e_H) = Ker(f)$

The <u>image</u> of f is $Im(f) = f(G)$

<u>Lemma:</u> $f \in Hom(G,H) \leftrightarrow f(xy) = f(x)f(y)$

<u>Lemma;</u> $Ker(f) < G$, $Im(f) < H$.

subgroup

Pf; Ex. Do for Image. (1) $Im(f)$ non empty, eg. $f(e_G) \in Im(f)$

(2) let $h_1, h_2 \in Im(f)$. Then we have $g_1, g_2 \in G$

s.t. $f(g_1) = h_1$, $f(g_2) = h_2$

Then $h_1 h_2 = f(g_1)f(g_2) = f(g_1 g_2) \in Im(f)$

Also, $h_1^{-1} = f(g_1)^{-1} = f(g_1^{-1}) \in Im(f)$

__Observation:__ If G is finite, every element has finite order

__Example:__ In $\mathbb{Z}$, 0 has order 1, all non-zero elements have infinite order

__Example:__ $GL_2(\mathbb{R})$: $\begin{pmatrix}1&x\\&1\end{pmatrix}\begin{pmatrix}1&y\\&1\end{pmatrix}=\begin{pmatrix}1&x+y\\&1\end{pmatrix}$

so $\begin{pmatrix}1&1\\&1\end{pmatrix}$ has infinite order

On the other hand $\begin{pmatrix}&1\\1&\end{pmatrix}$ has order 2.

__Example__ (PS 2): In the group $(P(X), \Delta)$ every non-identity element has order 2.

__Example:__ linear groups

Write $GL_n(\mathbb{R}) = \{g \in M_n(\mathbb{R}) \mid g^{-1} \text{ exists}\} = \{g \in M_n(\mathbb{R}) \mid \det(g) \neq 0\}$

__Gp:__ matrix mult is associative, I_n is invertible, have inverses

(more generally a "linear group" is a group isomorphic to a subgroup of $GL_n(F)$, F a field)

Rephrase thm "$\det(gh) = \det(g)\cdot\det(h)$"

as "$\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ is a gp hom"

$\mathrm{Tr}(aA+B) = a\,\mathrm{Tr}(A) + \mathrm{Tr}(B)$: $\mathrm{Tr} : M_n(F) \to F$ is a linear map

But: $\det(\exp(A)) = \exp(\mathrm{Tr}\,A)$, $\exp(A) = \sum_{n=0}^{\infty} \frac{A^n}{n!}$