FRI, SEP 5, 2014

Last time:

Defn A group is a pair

(G, m)

where m is a fxn

$m: G \times G \to G$

s.t.

(1) m is associative

(2) (G, m) has a unit i.e., $1_G g = g 1_G = g$.

(3) (G, m) has inverses ie, $g g^{-1} = g^{-1} g = 1_G$.

Exer

$G = \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

$m(s,t) := s \times t$.

Show this is a group.

Let $G = \mathbb{R}_{>0} = \{t \mid t > 0\}$

$m(s,t) = s \times t$.

Show this is a group.

Last time we saw

$(\mathbb{Z}, +)$ is a group

$(\mathbb{Z}, \times)$ is NOT a group.

So m is important. Regardless, we will often write

G

in place of (G, m) with m implicit.

Cancellation Law

Prop Let G be a grp. Suppose

$gh = gk$.

Then $h = k$.

Pf $\exists\, g^{-1}$ s.t. $g^{-1} g = 1$. (3)

$gh = gk \implies g^{-1}(gh) = g^{-1}(gk)$

$\implies (g^{-1}g)h = (g^{-1}g)k$ (1)

$\implies 1 \cdot h = 1 \cdot k$ (3)

$\implies h = k$ (2). //

used every property of being a grp!

Rmk Not true for matrix multiplication unless g, h, k are all invertible.

e.g., if $g = 0$?

Defn Let G be a group,
and $H \subset G$ a subset.
H is called a <u>subgroup</u>
of H if

(1) $\forall\, h_1, h_2 \in H$,
$h_1 h_2 \in H$. (Closed under multiplication)

(2) $id_G \in H$

(3) If $h \in H$, then $h^{-1} \in H$.

Ex $\mathbb{R}_{>0} \subset \mathbb{R}^\times$ is
a subgroup.

Exer

w/ addition

(a) Show $\mathbb{Z}_{\geq 0} \subset \mathbb{Z}$
is NOT a subgroup

(b) Show $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$
is a subgroup.

Propn

Let $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$.

Define
$$m(z_1, z_2) = z_1 \times z_2. \quad \leftarrow \text{mult. of complex \#'s.}$$

(a) $\mathbb{C}^\times$ is a group

(b) Let
$$S^1 = \{z \mid |z| = 1\}.$$

Then $S^1 \subset \mathbb{C}^\times$ is a subgroup.

Pf: (a) (1) Complex mult is assoc.

(2) $1 \times z = z \times 1 = z \ \forall z$.

(3) Set
$$z^{-1} = \frac{\overline{z}}{\|z\|^2}.$$

(b) (1) $|z_1| = |z_2| = 1$

$\Rightarrow |z_1 \times z_2| = 1$ so S^1 is closed under $\times$.

(2) $|1| = 1$ so the unit is in S^1

(3) If $|z| = 1$, then $|\overline{z}| = 1$, and $z^{-1} = \overline{z}$.

//

What kinds of functions do we want to study?

<u>Defn</u> A function

$$\phi : G \longrightarrow H$$

is called a <u>group homomorphism</u> if $\forall\, g_1, g_2 \in G$,

$$\phi(g_1 g_2) = \phi(g_1)\,\phi(g_2).$$

<u>Exer</u> Show the following are group homomorphisms:

(a) $\exp : (\mathbb{R}, +) \longrightarrow \mathbb{R}^\times$
$\quad t \longmapsto e^t$

(b) $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$
$\quad A \longmapsto \det(A)$

(c) $(\mathbb{R}, +) \longrightarrow S^1$
$\quad t \longmapsto e^{it}$

<u>Defn</u> If a group homomorphism ϕ is a bijection, ϕ is called a group <u>isomorphism</u>.

Ex

$$\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \times)$$

is a group isomorphism.

Exer Let $\phi : G \to H$ be a group homomorphism.

Show

(a) $\phi(1_G) = 1_H$

(b) $\phi(g^{-1}) = \phi(g)^{-1}$.

(HINT: Cancellation Law)

Soln:

(a) For any $g \in G$,

$\phi(g) = \phi(1_G \cdot g)$ (2)

$= \phi(1_G) \cdot \phi(g)$. Defn of homomorphism

Let h be inverce of $\phi(g)$.

Then

$\phi(g) h = \phi(1_G) \cdot \phi(g) \cdot h$

$\Longrightarrow 1_H = \phi(1_G) \cdot 1_H$ (3). (1) on RHS

$\rightarrow 1_H = \phi(1_G)$ (2)

(b) $\phi(g \cdot g^{-1}) = \phi(g)\phi(g^{-1})$

$\parallel$

$\phi(1_G) = 1_H$. //

Exer If $\phi : G \to H$ is a group isomorphism, ϕ^{-1} is a group isomorphism.

Soln $\phi^{-1}(h_1 \cdot h_2) = \phi^{-1}(\phi(g_1) \cdot \phi(g_2))$

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

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

$= g_1 g_2$

$= \phi^{-1}(h_1)\phi^{-1}(h_2)$ //

Rmk · Could there be two elements, 1 and $1'$, st $1g = g = g1$, $1'g = g = g1'$?

· Or two inverses to g?

Your hmwk: No.

Defn Given a group homomorphism
$$\phi: G \longrightarrow H$$
the kernel of ϕ is the set
$$\mathrm{Ker}(\phi) = \{g \in G \text{ s.t. } \phi(g) = 1_H\}.$$
The image of ϕ is the set
$$\mathrm{im}(\phi) = \{h \in H \text{ s.t. } h = \phi(g) \text{ for some } g \in G\}.$$

Exer $\mathrm{Ker}(\phi) \subset G$, $\mathrm{im}(\phi) \subset H$ are subgroups.

Pf: • (1) $\phi(g_1), \phi(g_2) = 1_H$
$$\Rightarrow \phi(g_1 g_2) = \phi(g_1)\cdot\phi(g_2)$$
$$= 1_H \cdot 1_H$$
$$= 1_H.$$
(2) $\phi(1_G) = 1_H$, so $1_G \in \mathrm{Ker}(\phi)$

(3) $\phi(g) = 1_H \Rightarrow \phi(g^{-1}) = 1_H^{-1} = 1_H.$
$$\Rightarrow g^{-1} \in \mathrm{Ker}(\phi).$$
• (2) $\phi(1_G) = 1_H$ so $1_H \in \mathrm{im}(\phi)$

(1) $h_i = \phi(g_i) \Rightarrow h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$

(3) $h = \phi(g) \Rightarrow h^{-1} = \phi(g^{-1}).$

Ex If V, W are vector spaces, they are groups under $+$.

Any linear map
$$\phi : V \to W$$
is a group homomorphism.

Any linear subspace is a subgroup.

Prop • Let X be a set. Let
$$\mathrm{Aut}_{\mathrm{Set}}(X) = \{\text{bijections } X \to X\}.$$
This is a group under composition

• Let G be a group. Let
$$\mathrm{Aut}(G) = \{\text{group isomorphisms } G \to G\}.$$
This is also a group.

Pf • $id_X = 1$, any bijection has an inverse which is also a bijection

• Likewise, noting that if ϕ is an isomorphism, so is ϕ^{-1}. //

Defn Let $\langle n \rangle = \{1, \cdots, n\}$.

$$S_n := \mathrm{Aut}_{\mathrm{Set}}(\langle n \rangle).$$

Ex

- $\underline{n=1}$. $S_1 = \{\text{bijections } \{1\} \to \{1\}\}$

$$= \{\mathrm{id}_{\langle 1 \rangle}\}.$$

Group w/ one element.

- $\underline{n=2}$. $S_2 = \left\{ \left(\mathrm{id}: \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 2 \end{array}\right), \left(\sigma: \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \end{array}\right) \right\}$

group w/ two elements.

$\sigma \circ \sigma = \sigma^2 = \mathrm{id}$.

- In general, S_n is group with $n!$ elements.