09/02/2022

Last time: Defined groups, homomorphisms, 6.1

Proved: homomorphisms preserve identities and inverses.

Definition A homomorphism $f: G \to H$ between two groups is an isomorphism if there is a homomorphism $k: H \to G$ so that $k \circ f = id_G$ and $f \circ k = id_H$

Note: Any isomorphism is an invertible map (function) hence a bijection. There is also a converse:

Lemma 6.1 Suppose $f: G \to H$ is a homomorphism and a bijection. Then f is an isomorphism: $\exists$ a homomorphism $k: H \to G$ so that $f \circ k = id_H$ and $k \circ f = id_G$.

Proof Since f is a bijection, it is invertible. Let $k = f^{-1}$, the inverse of the function f. We need to check that k is a homomorphism: $k(xy) = k(x)\,k(y)$ $\forall\ x, y \in H$

Now $f(k(x)k(y)) = f(k(x))\,f(k(y)) = xy = f(k(xy))$

Since f is a bijection, it is 1-1.

$\Rightarrow$ $k(x)\,k(y) = k(xy)$ $\square$

Remark Most textbooks define isomorphisms as bijective homomorphisms. Lemma 6.1 shows that this is equivalent to our definition.

Ex $\exp: \mathbb{R} \to (0,\infty)$ is a homomorphism and a bijection.

$\Rightarrow$ $\ln: (0,\infty) \to \mathbb{R}$ is a homomorphism (by 6.1)

and $\exp: \mathbb{R} \to (0,\infty)$ is an isomorphism.

Subgroups

<u>Def</u> A <u>subgroup</u> of a group G is a subset $H \subseteq G$ so that
1) $e_G \in H$
2) $\forall h_1, h_2 \in H, \quad h_1 h_2 \in H$
3) $\forall h \in H, \quad h^{-1} \in H$

<u>Note</u> If H is a subgroup of G then H is, in fact a group with the multiplication inherited from G.

<u>Ex 0</u> For any group G, $\{e_G\}$ and G are subgroups.

<u>Ex</u> $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are subgroups.

<u>Ex</u> $SL(n,\mathbb{R}) := \{ A \in GL(n,\mathbb{R}) \mid \det A = 1 \}$ is a subgroup of $GL(n,\mathbb{R})$:
1) $I \in SL(n,\mathbb{R})$
2) $\forall A, B \in SL(n,\mathbb{R}), \quad AB \in SL(n,\mathbb{R})$ because $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$
3) $\forall A \in SL(n,\mathbb{R}), \quad \det(A^{-1}) = (\det(A))^{-1} = 1^{-1} = 1$ $\Rightarrow A^{-1} \in SL(n,\mathbb{R})$

This was a bit tedious, wasn't it?

<u>Lemma 6.2</u> A nonempty subset H of a group G is a subgroup $\Leftrightarrow \forall h_1, h_2 \in H, \quad h_1 h_2^{-1} \in H$.

<u>Proof</u> ($\Rightarrow$) If H is a subgroup, then $e_G \in H$ so $H \neq \emptyset$. $\forall h_1, h_2 \in H, \quad h_2^{-1} \in H$. And $h_1, h_2^{-1} \in H \Rightarrow h_1 h_2^{-1} \in H$.

($\Leftarrow$) Suppose $H \neq \emptyset$ and $h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$.
Since $H \neq \emptyset$, $\exists h \in H$. Then $e_G = h h^{-1} \in H$.

$\Rightarrow \forall h \in H, \quad h^{-1} = e_G \cdot h^{-1} \in H \quad (\text{since } e_G \in H)$

$\Rightarrow \forall h_1, h_2 \in H. \; h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H.$ $\square$

Definition Let $f : G \to H$ be a homomorphism. The kernel of f is the set

$$\ker f := \{ g \in G \mid f(g) = e_H \}$$

The image of f is the set

$$\operatorname{im} f := \{ f(g) \in H \mid g \in G \}$$

Lemma 6.3 For any homomorphism $f : G \to H$, $\ker f$ is a subgroup of G, $\operatorname{im} f$ is a subgroup of H.

Proof

- $\forall a, b \in \ker f, \quad f(ab^{-1}) = f(a)(f(b))^{-1} = e_H e_H^{-1} = e_H.$

  $\Rightarrow ab^{-1} \in \ker f$ and $\ker f$ is a subgroup by 6.2
- Suppose $x, y \in \operatorname{im} f$. Then $x = f(a)$, $y = f(b)$ for some $a, b \in G$.

  $\Rightarrow xy^{-1} = f(a)(f(b))^{-1} = f(ab^{-1}) \in \operatorname{im} f.$

  $\therefore \operatorname{im} f$ is a subgroup of H by 6.2. $\square$

Ex $SL(n, \mathbb{R}) = \ker(\det : GL(n, \mathbb{R}) \to \mathbb{R}^\times)$, hence a subgroup of $GL(n, \mathbb{R})$.

Ex $\exp : \mathbb{R} \to \mathbb{R}^\times$, $\exp(x) = e^x$ is a homomorphism.

$\Rightarrow \operatorname{im}(\exp) = (0, \infty)$ is a subgroup of $\mathbb{R}^\times$.

Powers of an element a of a group G: for $n \in \mathbb{Z}$ we define

$$a^n := \begin{cases} \overbrace{a \cdots a}^{n}, & n > 0 \\ e & n = 0 \\ \underbrace{a^{-1} \cdots a^{-1}}_{|n|} & n < 0 \end{cases}$$

Exercise Let G be a group, $a \in G$. Then $f : \mathbb{Z} \to G$, $f(n) = a^n$ is a homomorphism: $a^{n+m} = a^n \cdot a^m$

<u>Consequence:</u> $\forall a \in G$, $\mathrm{im} f = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G. It's called the subgroup <u>generated</u> by a. One usually writes $\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$.

<u>Example</u> $G = \mathbb{C}^\times = \{z \in \mathbb{C} \mid z \neq 0\}$. $(\mathbb{C}^\times, \cdot, 1)$ is a group.
Let $a = \sqrt{-1}$. Then
$$\langle \sqrt{-1} \rangle = \{\sqrt{-1}, (\sqrt{-1})^2, (\sqrt{-1})^3, (\sqrt{-1})^4\} = \{\sqrt{-1}, -1, -\sqrt{-1}, 1\}.$$

<u>Example</u> $G = (\mathbb{Z}, +, 0)$. $a = 5$.
Then "a^{-1}" $= -5$, "a^2" $= 5+5$ "a^{-2}" $= -5-5$ ...
and $\langle a \rangle = \{5n \mid n \in \mathbb{Z}\} =: 5\mathbb{Z}$

<u>Recall</u> A linear map $T: V \to W$ is 1-1 $\Leftrightarrow$ $\mathrm{null}\, T = \{\vec{0}\}$.

<u>Lemma 6.4</u> A homomorphism $f: G \to H$ is 1-1 $\Leftrightarrow$ $\ker f = \{e_G\}$.
<u>Proof</u> ($\Rightarrow$) Suppose f is 1-1 and $x \in \ker f$. Then $f(x) = e_H = f(e_G)$.
Since f is 1-1, $x = e_G$. $\therefore$ $\ker f = \{e_G\}$.
($\Leftarrow$) Suppose $\ker f = \{e_G\}$ and $f(x) = f(y)$. Then
$e_H = f(x) f(y)^{-1} = f(xy^{-1})$. $\Rightarrow$ $xy^{-1} \in \ker f = \{e_G\}$.
$\Rightarrow$ $xy^{-1} = e_G$. $\Rightarrow$ $x = e_G y = y$. $\Rightarrow$ f is 1-1. $\square$

<u>Corollary 6.5</u> Suppose G is a group, $a \in G$ s.t $a^m = e_G \Rightarrow m = 0$.
Then $\langle a \rangle$ is isomorphic to $\mathbb{Z}$.
<u>Proof</u> Consider $f: \mathbb{Z} \to G$, $f(n) = a^n$. $\ker f = \{m \mid a^m = e\}$.
By assumption, $\ker f = \{0\}$. By 6.4, f is 1-1.
By definition of $\langle a \rangle$, $\langle a \rangle = \mathrm{im} f$. Hence $f: \mathbb{Z} \to \langle a \rangle$ is a bijection. By 6.1, $f: \mathbb{Z} \to \langle a \rangle$ is an isomorphism.
$\square$