last time: defined a group

Recall

A group \( G \) is a triple \((G, *, e)\) where

1) \( *: G \times G \rightarrow G \) is a binary operation

which is associative

2) \( e \in G \) is a distinct element (the identity) so that
\[ a * e = e = e * a \quad \forall a \in G \]

3) \( \forall a \in G \) there is a (unique) \( a^{-1} \in G \)
\[ a * a^{-1} = e = a^{-1} * a. \]

Examples \((\mathbb{Z}, +, 0)\), \((\mathbb{C}^*, \cdot, 1)\), \(GL(n, \mathbb{R})\)...

Another example \( X \) is a set

\[ \text{Aut}(X) = \{ f: X \rightarrow X \mid f \text{ is invertible} \}, \]

binary operation is composition \( \circ \)

\[ (f \circ g)(x) = f(g(x)) \quad \forall x \in X \]

identity element is \( \text{Id}_X: X \rightarrow X \), \( \text{Id}_X(x) = x \quad \forall x \in X \).

Proposition 1 (10)

Let \((G, *, e)\) be a group.

1) if \( \forall a \in G \) with \( a * e' = a \neq e \) then \( e' = e \).
2) inverses are unique
3) \( (a^{-1})^{-1} = a \)
4) \( \forall n, m, a \in G \)
\[ a_1 * (a_2 * f \quad (a_{n+1} * a_n) \ldots) = (a_1 * a_2) * (a_3 \ldots a_n) \]
e tc.
order of parentheses doesn't matter.

We proved (2). Last time. (4) is easy. Take \( a = e \).
Then \( e \cdot e = e \) by assumption.

(3): \( a \cdot a^{-1} = e = a^{-1} \cdot a = 1 \) is the inverse of \( a^{-1} \), ie \( a \cdot (a^{-1})^{-1} \) is the inverse of \( a \).

(4) read as text.

**Def.** A group \( G \) is _abelian (commutative)_ if \( a \cdot b = b \cdot a \) for all \( a, b \in G \).

**Ex.** \((\mathbb{Z}, +, 0)\) is abelian, \(GL(2, \mathbb{R})\) is not.

**Def.** Let \((G, \cdot), (H, *)\) be two groups. A map \( \varphi : G \to H \) is a _homo-morphism_ if \( \varphi(a \cdot b) = \varphi(a) * \varphi(b) \) for all \( a, b \in G \).

**Ex.** \((\mathbb{R}, *, 0) = (\mathbb{R}, +, 0)\) \((\mathbb{R}^*, *, 0) = (\mathbb{R} \setminus \{0\}, *, 1)\) \(\exp : \mathbb{R} \to \mathbb{R}^* \), \( \exp(x) = e^x \) is a homomorphism since \( \exp(x+y) = e^{x+y} = e^x \cdot e^y = \exp(x) \cdot \exp(y) \).

**Ex.** \( \det : GL(n, \mathbb{R}) \to \mathbb{R}^* \) is a homomorphism since \( \det(AB) = \det(A) \cdot \det(B) \).

**Ex.** \( \log : (0, \infty) \to (\mathbb{R}, +, 0) \) is a homomorphism since \( \log(ab) = \log a + \log b \).
\[ \pi : (\mathbb{Z}, +, 0) \rightarrow (\mathbb{Z}_n, +, 101) \]
\[ \pi(a) = [a] \]

A homomorphism:
\[ \pi(a + b) = [a + b] = [a] + [b] = \pi(a) + \pi(b) \]

*For any group \( G \), \( \text{Id}_G : G \rightarrow G \), \( \text{Id}_G (a) = a \)

is a homomorphism.

**Def.** A homomorphism \( \varphi : G \rightarrow H \) is an isomorphism if it is invertible: \( \exists \) a homomorphism \( \psi : H \rightarrow G \)

such that \( \psi \circ \varphi = \text{Id}_G \), \( \varphi \circ \psi = \text{Id}_H \).

*Remark:* This is different from the definition of the text.

Text requires \( \varphi \) to be a bijection.

So one needs to prove: if \( \varphi : G \rightarrow H \) is a homomorphism and a bijection then \( \varphi^{-1} : H \rightarrow G \) preserves multiplication.

**Here is a proof:** we need to show \( \forall x, y \in H \)

\[ \varphi^{-1}(xy) = \varphi^{-1}(x) \varphi^{-1}(y) \]

Now \( \psi(\varphi^{-1}(x) \varphi^{-1}(y)) = \psi(\varphi^{-1}(x)) \cdot \psi(\varphi^{-1}(y)) \) since \( \varphi \) preserves mult.

\[ = xy = \psi(\varphi^{-1}(xy)) \]

Since \( \varphi \) is a bijection,

\[ \varphi^{-1}(x) \cdot \varphi^{-1}(y) = \varphi^{-1}(xy) \]

**Ex.** \( G = \{ \pm 1 \} \), group operation is multiplication.

Define \( \varphi : \mathbb{Z}/2 \rightarrow G \) by

\[ \varphi([k]) = (-1)^k \]
Note: if \( k \equiv l \pmod{2} \), \( k - l \) is even, \( \Rightarrow (-1)^{k-l} = 1 \)
\( \Rightarrow (-1)^k = (-1)^l \)
\( \Rightarrow \Phi \) is well-defined.

Also, \( \Phi \) is onto, since \( \Phi([0]) = 1 \), \( \Phi([1]) = -1 \).

Finally if \( \Phi([k]) = \Phi([l]) \),

\( (-1)^k = (-1)^l \)
\( \Rightarrow (-1)^{k-l} = 1 \)
\( \Rightarrow k - l \) is even
\( \Rightarrow k \equiv l \pmod{2} \)
\( \Rightarrow [k] = [l] \) in \( \mathbb{Z}/2 \).

Conclusion \( \Phi: \mathbb{Z}/2 \rightarrow \{ \pm 1 \} \) is an isomorphism.

Example

\( \log: (0, \infty) \rightarrow (\mathbb{R}, +) \) is an isomorphism.

Reason \( \exp(\log(x)) = x + x \in (0, \infty) \)
\( \log(\exp(y)) = y \quad \forall y \in \mathbb{R} \).

**Lemma 6.2** Suppose \( \Phi: G \rightarrow H \) is a homomorphism.

Then \( \Phi(e_G) = e_H \).

**Proof**
\( e_G \cdot e_G = e_G \)
\( \Rightarrow \Phi(e_G) = \Phi(e_G \cdot e_G) = \Phi(e_G) \cdot \Phi(e_G) \)
\( \Rightarrow e_H = (\Phi(e_G))^{-1} \Phi(e_G) = \Phi(e_G)^{-1} \Phi(e_G) = e_H \cdot \Phi(e_G) = \Phi(e_G) \).

Example

\( \Phi: \mathbb{Z} \rightarrow \{ \pm 1 \}, \quad \Phi(n) = (-1)^n \) is a homomorphism.

\( \Phi(n + m) = (-1)^{n+m} = (-1)^n \cdot (-1)^m = \Phi(n) \cdot \Phi(m) \)
\( \Phi \) is onto but not 1-1.
An action of a group $G$ on a set $A$ is a map $\alpha: G \times A \to A$, $\alpha(g, a) = g \cdot a$ so that

1) $e \cdot a = a \quad \forall a \in G$

2) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a \quad \forall g_1, g_2 \in G, a \in A$

Example $G = GL(2, \mathbb{R})$ = invertible $2 \times 2$ matrices acts on $\mathbb{R}^2$

$$
\begin{pmatrix}
a_{11} & a_{12} \\
a_{21} & a_{22}
\end{pmatrix}
\begin{pmatrix}
x \\
y
\end{pmatrix} =
\begin{pmatrix}
a_{11}x + a_{12}y \\
a_{21}x + a_{22}y
\end{pmatrix}
$$

It's an action since

(i) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$

(ii) $\forall A, B \in GL(2, \mathbb{R}), \forall \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$

$$
A \left( B \begin{pmatrix} x \\ y \end{pmatrix} \right) = (AB)\begin{pmatrix} x \\ y \end{pmatrix}
$$

Example $(\mathbb{C}, 0, 1)$ acts on $\mathbb{C}$ by

$$
\lambda \cdot z = \lambda z \quad \text{multi of complex numbers}
$$

It's an action since

$$
1 \cdot z = z \quad \forall z
$$

$$
\lambda \cdot (\mu \cdot z) = (\lambda \mu) z \quad \forall \lambda, \mu \in \mathbb{C}
$$