A group is a set G with a function

$$\begin{aligned} G\times G &\to G \\ (g_1,g_2) &\mapsto g_1g_2 \end{aligned} \quad \text{such that}$$

(a) If $g_1, g_2, g_3 \in G$ then $g_1(g_2g_3) = (g_1g_2)g_3$,

(b) There exists $1 \in G$ such that

if $g \in G$ then $1\cdot g = g$ and $g \cdot 1 = g$.

(c) If $g \in G$ then there exists $g^{-1} \in G$ such that

$g \cdot g^{-1} = 1$ and $g^{-1}\cdot g = 1$.

An abelian group is a set A with a function

$$\begin{aligned} A\times A &\to A \\ (a_1,a_2) &\mapsto a_1+a_2 \end{aligned} \quad \text{such that}$$

(a) If $a_1, a_2, a_3 \in A$ then $a_1+(a_2+a_3) = (a_1+a_2)+a_3$,

(b) ~~There~~ There exists $0 \in A$ such that

if $a \in A$ then $0+a = a$ and $a+0 = a$.

(c) If $a \in A$ then there exists $-a \in A$ such that

$a+(-a) = 0$ and $(-a)+a = 0$

(d) If $a_1, a_2 \in A$ then $a_1+a_2 = a_2+a_1$

Every abelian group is a group.

$$GL_2(\mathbb{R}) = \{2\times 2 \text{ invertible matrices with entries in } \mathbb{R}\}$$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \text{ and } ad-bc \neq 0 \right\}$$

$GL_2(\mathbb{R})$ is a group with product matrix multiplication.

$GL_2\mathbb{R}$ is <u>not</u> an abelian group.

Let G be a group.

The <u>order</u> of G is $\mathrm{Card}(G)$, the number of elements in G.

The <u>order</u> of an element $g\in G$ is the smallest $k\in\mathbb{Z}_{>0}$ such that $g^k=1$

If there does not exist $k\in\mathbb{Z}_{>0}$ such that $g^k=1$ then the order of $g\in G$ is ∞.

A <u>subgroup</u> of G is a subset $H\subseteq G$ such that

(a) If $h_1,h_2\in H$ then $h_1h_2\in H$,

(b) $1\in H$

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

Group homomorphisms are for comparing groups.

Group homomorphisms are for comparing groups.

Let G and K be groups.

A <u>group homomorphism</u> <u>from K to G</u> is a function $f: K \to G$ such that

if $k_1, k_2 \in K$ then $f(k_1 k_2) = f(k_1) f(k_2)$.

An <u>isomorphism from K to G</u> is a group homomorphism $f: K \to G$ such that

there exists a group homomorphism $f^{-1}: G \to K$ such that $f \circ f^{-1} = id_G$ and $f^{-1} \circ f = id_K$.

Let $f: K \to G$ be a group homomorphism.

The <u>kernel</u> <u>of f</u> is the set

$$\ker f = \{g \in G \mid f(g) = 1\}$$

The <u>image</u> <u>of f</u> is the set

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

<u>Theorem</u> Let $f: K \to G$ be a group homomorphism.

Then $f: K \to G$ is an isomorphism if and only if $f: K \to G$ is bijective.

Proof

$\Rightarrow$ Assume $f: K \to G$ is an isomorphism from K to G

To show: $f: K \to G$ is bijective.

Since f is an isomorphism, there exists an inverse function to f,

$g: G \to K$ such that $g \circ f = id_G$ and $f \circ g = id_K$.

Thus, by theorem

Theorem Let $f: K \to G$ be a function.
An inverse function to f exists if and only if f is bijective

which is proved fully in Lecture notes,

f is bijective.

$\Leftarrow$ Assume $f: K \to G$ is a group homomorphism and $f: K \to G$ is bijective.

To show: $f: K \to G$ is an isomorphism.

To show: (a) There exists a function $g: G \to K$ such that $g \circ f = id_G$ and $f \circ g = id_K$

(b) $g: G \to K$ is a group homomorphism.

(a) follows from Theorem.

(b) To show: If $x_1, x_2 \in G$ then $g(x_1 x_2) = g(x_1) g(x_2)$.

Assume $x_1, x_2 \in G$

To show: $g(x_1 x_2) = g(x_1)\, g(x_2)$.

Since f is bijective, f is injective, which means

if $k_1, k_2 \in K$ and $f(k_1) = f(k_2)$ then $k_1 = k_2$.

To show: $f(g(x_1 x_2)) = f(g(x_1)\, g(x_2))$

$f(g(x_1 x_2)) = x_1 x_2$, ~~and~~ since $f \circ g = id_G$, and

$f(g(x_1)\, g(x_2)) = f(g(x_1))\, f(g(x_2))$, since f is a homomorphism

$= x_1 \cdot x_2$, since $f \circ g = id_G$.

So $f(g(x_1)\, g(x_2)) = f(g(x_1 x_2))$.

So $g(x_1)\, g(x_2) = g(x_1 x_2)$.

So g is a homomorphism. //.