Prop Let $(G,*)$ be a group. Then $(a*b)^{-1} = b^{-1}*a^{-1}$ $\forall a,b \in G$.

We use g^{-1} to denote the inverse of g in G.

PF Since we know inverses are unique, it suffices to show that $(a*b)^{-1}$ and $b^{-1}*a^{-1}$ are inverses of the same element.

Well $(a*b)^{-1}*(a*b) = (a*b)*(a*b)^{-1} = e$ by definition.

We also have $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*(a*b))$

$= b^{-1}*((a^{-1}*a)*b)$ (associativity)

$= b^{-1}*(e*b)$

$= b^{-1}*b$

$= e$

Similarly, check that $(a*b)*(b^{-1}*a^{-1}) = e$.

Ex

$(GL_n(\mathbb{R}), \times)$	$(\mathbb{Z}, +)$
• $AB = AC \Rightarrow B = C$	• $a+b = a+c \Rightarrow b = c$
• $I = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$ is unique	• 0 is the unique identity
• A^{-1} is uniquely defined by the adjugate matrix. But we don't need to know that to get uniqueness! Since $GL_n(\mathbb{R})$ is a group as long as we find one we are done	• $-a$ is the inverse of a
• $(AB)^{-1} = B^{-1}A^{-1}$	• $-(a+b) = -b-a = -a-b$ (The integers are more special, see below)

Defn A group $(G,*)$ is said to be abelian if the commutativity axiom holds

(4) commutativity: $a*b = b*a$ $\forall a,b \in G$.

Ex • $(\mathbb{Z},+)$ is abelian

• $(GL_n(\mathbb{R}), \times)$ is not abelian

Homomorphisms

We have a name for a function between groups that preserves the group structure:

Defn Let $(G, *)$ and $(H, \bullet)$ be groups. Then a homomorphism from G to H is a function $f: G \to H$ satisfying,

$$f(a*b) = f(a) \bullet f(b) \quad \forall\, a, b \in G.$$

Ex • $F: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$, $n \longmapsto 3n$ is a homomorphism

pf $f(n+m) = 3(n+m) = 3n + 3m = f(n) + f(m)$.

- $F: (G, *) \longrightarrow (H, \bullet)$, $g \longmapsto e_H \ \forall\, g \in H$.

  This is called the "trivial homomorphism" ← check this.
- Linear maps between vector spaces

Prop If $f: (G, *) \to (H, \bullet)$ is a homomorphism, then

$$f(e_G) = e_H.$$

pf $f(e_G) = f(e_G * e_G) \overset{\text{homomorphism}}{=} f(e_G) \bullet f(e_G)$

Also $f(e_G) = e_H \bullet f(e_G)$.

Thus $e_H \bullet f(e_G) = f(e_G) \bullet f(e_G) \Rightarrow e_H = f(e_G)$ ■

(cancellation)

More properties

- A composition of homomorphisms is a homomorphism
- Given $(G, *)$, we have a homomorphism $id_G: G \to G$

Exercise: Check the above two statements.

Similar to how bijective functions of sets essentially tells us that the two sets are the "same" we have an analogous notion for groups.

Defn An isomorphism $f: (G, *) \longrightarrow (H, \cdot)$ is a homomorphism that is also bijective (as a map of sets). Denoted by $G \cong H$, $G \simeq H$ or $f: G \xrightarrow{\sim} H$.

Huh $f: G \to H$ is an isomorphism $\iff$ $\exists\ g: H \to G$ a homomorphism satisfying $g \circ f = id_G$ AND $f \circ g = id_H$.

↑ be careful

- An isomorphism from a group G to itself i.e. $f: G \to G$ is called an automorphism.

Ex • $(\mathbb{Z}, +) \longrightarrow (2\mathbb{Z}, +)$, $n \longmapsto 2n$ is an isomorphism

• $(\mathbb{R}^{n^2}, +) \longrightarrow (M_{n\times n}(\mathbb{R}), +)$, $(x_{11}, \dots, x_{1n}, x_{21}, \dots, x_{2n}, \dots, x_{n1}, \dots, x_{nn}) \mapsto \begin{bmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{bmatrix}$

is an isomorphism

Non example • Two finite groups of different sizes cannot be isomorphic

Prop $(\mathbb{Z},+)$ and $(\mathbb{Q},+)$ are not isomorphic.

Warning: There are bijections of sets $\mathbb{Q} \longrightarrow \mathbb{Z}$, but none of them are homomorphisms.

Pf Assume $\exists$ an isomorphism $f: \mathbb{Q} \longrightarrow \mathbb{Z}$. Then $\exists\, q \in \mathbb{Q}$ such that $f(q)=1$. By definition of a homomorphism and since $\frac{q}{2} \in \mathbb{Q}$ we have $1 = f(q) = f\left(\frac{q}{2}+\frac{q}{2}\right) = f\left(\frac{q}{2}\right)+f\left(\frac{q}{2}\right)$

$$\Rightarrow 1 = 2f\left(\frac{q}{2}\right).$$

But $f\left(\frac{q}{2}\right)$ must be an integer (by assumption), which is a contradiction ∎

Subgroups

Notation: · If $a \in G$ we will write a^n to mean $\underbrace{a * a * \cdots * a}_{n\text{-times}}$ for $n \geq 1$.

· $a^0 := e_G$

· a^{-1} is the inverse of a and thus a^{-n} means $a^{-1} * \cdots * a^{-1}$ for $n \geq 1$.

Thus $a^{m+n} = a^m \cdot a^n \quad \forall m, n \in \mathbb{Z}$.

Defn Let $(G,*)$ be a group. A subgroup of G is a subset $H \subseteq G$ that's closed under $*$ i.e., it satisfies:

1) $e_G \in H$
2) $a \in H \Rightarrow a^{-1} \in H$
3) $a, b \in H \Rightarrow a * b \in H$

EX · $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$

· $\{e_G\}$ is always a subgroup of $(G,*)$ (trivial subgroup)

· Upper triangular matrices are a subgroup of $(GL_n(\mathbb{R}),\times)$

Exercise Invertible matrices with determinant $=1$ is a subgroup of $GL_n(\mathbb{R})$; this is denoted by $SL_n(\mathbb{R})$.