Groups and Homomorphisms

Definition Let G be a set. A binary operation / composition on G is a map
$$* : G \times G \longrightarrow G$$
$$(a,b) \longmapsto a*b$$
notation for $*(a,b)$

Examples $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $(a,b) \longmapsto a+b$, $GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$, $(A,B) \longmapsto AB$

Fundamental Definition

A group is a set G, together with a binary operation $*$, such that

- $(a*b)*c = a*(b*c) \quad \forall a,b,c \in G$ (Associativity)
- $\exists\, e \in G$, such that $e*a = a*e = a \quad \forall a \in G$ (Identity)
- Given $a \in G$, $\exists\, b \in G$ such that $a*b = b*a = e$ (Inverses)

We say $(G,*)$ is Abelian if, in addition

- $a*b = b*a \quad \forall a,b \in G$

Introduced groups in 1832

Galois

Abel

Examples

Abelian Groups : $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{Q}\setminus\{0\},\times)$, $(M_n(\mathbb{R}),+)$
$(\mathbb{Z}/m\mathbb{Z},+)$, $(V,+)$ vector space)

Non-Abelian Group : $(GL_n(\mathbb{R}),\times)$

Remark If $(G,*)$ satisfies associative and identity properties we say it is a monoid.

Example $(\mathbb{Z},\times)$, $(M_n(\mathbb{R}),\times)$.

Group = Monoid + Inverse property

Proposition If $(G,*)$ is a group the identity and inverses are unique.

Proof Assume $e, e' \in G$ such that

$e * a = a * e = g$ **and** $e' * a = a * e' = g$ $\forall a \in G$

$\Rightarrow \quad e = e * e' = e'$

Let $a \in G$ and $b, c \in G$ such that

$a * b = b * a = e$ **and** $a * c = c * a = e$. Then

$$
\begin{aligned}
a * b = e \quad &\Rightarrow \quad c * (a * b) = c * e \\
&\Rightarrow \quad (c * a) * b = c \quad \leftarrow \text{Associativity + Identity} \\
&\Rightarrow \quad e * b = c \quad \leftarrow \text{Inverses} \\
&\Rightarrow \quad b = c \quad \leftarrow \text{Identity}
\end{aligned}
$$

$\square$

Remark Any deduction about an abstract groups $(G, *)$ can only use the three defining axioms.

Notation Given $a \in G$, a^{-1} = inverse of a, and given $r \in \mathbb{Z}$

$$
a^r = \begin{cases} a * \cdots * a \ (r \text{ times}) & \text{if } r > 0 \\ e & \text{if } r = 0 \\ a^{-1} * \cdots * a^{-1} \ (-r \text{ times}) & \text{if } r < 0 \end{cases}
$$

Cancellation Law for Groups Given $a, b, c \in G$

$$a * c = b * c \quad \Rightarrow \quad a = b$$

Proof

$$
\begin{aligned}
a * c = b * c \quad &\Rightarrow \quad (a * c) * c^{-1} = (b * c) * c^{-1} \\
&\Rightarrow \quad a * (c * c^{-1}) = b * (c * c^{-1}) \\
\text{Need all axioms} \rightarrow \quad &\Rightarrow \quad a * e = b * e \\
&\Rightarrow \quad a = b
\end{aligned}
$$

$\square$

Definition Let $(G, *)$, $(H, \circ)$ be two groups. A **homomorphism** from G to H is a map

$f : G \longrightarrow H$ such that $f(a * b) = f(a) \circ f(b)$ $\forall a, b \in G$

Examples 1) V, W vector spaces, $f: V \longrightarrow W$ linear

$\Rightarrow f$ homomorphism from $(V,+)$ to $(W,+)$ ← Abelian groups

2) $\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ ← groups under $+$

$a \longmapsto [a]$

Remark : The composition of two homomorphisms is again a homomorphism. The identity map is a homomorphism

Proposition Let $(G,*)$, $(H,\circ)$ be groups with identities e_G, e_H.

If $f: G \rightarrow H$ is a homomorphism then

- $f(e_G) = e_H$
- $f(x^{-1}) = (f(x))^{-1} \quad \forall x \in G$

Proof

$f(e_G) \circ e_H = f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G)$

$\underset{\text{(C.L.)}}{\Rightarrow} f(e_G) = e_H$

Let $x \in G$.

$$\left.\begin{aligned} e_H &= f(e_G) = f(x * x^{-1}) = f(x) \circ f(x^{-1}) \\ e_H &= f(e_G) = f(x^{-1} * x) = f(x^{-1}) \circ f(x) \end{aligned}\right\} \Rightarrow (f(x))^{-1} = f(x^{-1})$$

$\square$

Definition

$f: G \longrightarrow H$ an <u>isomorphism</u> $\Leftrightarrow$ f a homomorphism <u>and</u> f a bijection

G, H isomorphic $\Leftrightarrow$ $\exists f: G \longrightarrow H$ an isomorphism

$G \cong H$

Intuition : $G \cong H \Leftrightarrow$ Same essential group with relabelled elements.

Fundamental problem : Classify all groups up to isomorphism.

Analogous to : All finite dimensional real vector spaces admit a linear isomorphism to $\mathbb{R}^n$ $(n = \dim(V))$ ← coordinate mapping after fixing basis