Homomorphisms

Definition

Let G and G' be groups. To say that a map $\phi : G \to G'$ is a *homomorphism* means that it satisfies the homomorphism property:

$$\forall\, x, y \in G, \phi(xy) = \phi(x)\phi(y)$$

Theorem

For any two groups G and G', there exists at least the trivial homomorphism:

$$\forall\, x \in G, \phi(x) = e'$$

Proof

Assume G and G' are groups
Let $\phi : G \to G'$ be defined by $\phi(x) = e'$
Assume $x, y \in G$
$\phi(xy) = e' = e'e' = \phi(x)\phi(y)$

Example

1). Evaluation

Let $F = \{f : \mathbb{R} \to \mathbb{R}\}$ and define $\phi_c : F \to \mathbb{R}$ by:

$$\phi_c(f) = f(c)$$

$\phi_c(f + g) = (f + g)(c) = f(c) + g(c) = \phi_c(f) + \phi_c(g)$

2). Linear Transformation

Let $A \in M_{m\times n}(\mathbb{R})$ and define $\phi_A : \mathbb{R}^n \to \mathbb{R}^m$ by:

$$\phi_A(x) = Ax$$

$\phi_A(x + y) = A(x + y) = Ax + Ay = \phi_A(x) + \phi_A(y)$

3). Determinant

Define $\phi : GL(n, R) \to \mathbb{R}$ by:

$$\phi(A) = \det(A)$$

$\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B)$

4). Projection

Let $G = \prod_{k=1}^{n} G_k$ and define $\pi_k : G \to G_k$ by:

$$\pi_k(g) = g_k$$

$\pi_k(g_1 + g_2) = g_{1_k} + g_{2_k} = \pi_k(g_1) + \pi_k(g_2)$

5). Modulo

Define $\phi : \mathbb{Z} \to \mathbb{Z}_n$ by:

$$\phi(m) = m \bmod n$$

$$\phi(r+s) = (r+s) \bmod n = r +_n s = \phi(r) +_n \phi(s)$$

Theorem

Let $\phi : G \to G'$ be an onto homomorphism:

G abelian $\implies$ G' abelian

Proof

Assume G is abelian
Assume $a', b' \in G'$
Since ϕ is onto, $\exists\, a, b \in G, \phi(a) = a'$ and $\phi(b) = b'$
$a'b' = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = b'a'$
$\therefore G'$ is abelian

Theorem

Let $\phi : G \to G'$ and $\gamma : G' \to G''$ be group homomorphisms:

$\gamma\emptyset : G \to G''$ is a homomorphism

A composition of homomorphisms is a homomorphism.

Proof

Assume $x, y \in G$
$(\gamma\emptyset)(xy) = \gamma(\phi(xy)) = \gamma(\phi(x)\phi(y)) = \gamma(\phi(x))\gamma(\phi(y)) = (\gamma\phi)(x)(\gamma\phi)(y)$
$\therefore \gamma\phi$ is a homomorphism

Definition

Let X and Y be non-empty sets, $A \subseteq X$ and $B \subseteq Y$, $A, B \neq \emptyset$, and $\phi : X \to Y$:

1). $\phi[A] = \{\phi(a) \mid a \in A\}$ is called the image of A in Y under ϕ

2). $\phi[X]$ is called the range of ϕ

3). $\phi^{-1}[B] = \{x \in X \mid \phi(x) \in B\}$ is called the inverse image of B in X under ϕ

Theorem

Let $\phi : G \to G'$ be a group homomorphism:

1). $\phi(e) = e'$

2). $\forall\, a \in G, \phi(a^{-1}) = \phi(a)^{-1}$

3). $H \leq G \implies \phi[H] \leq G'$

4). $K' \leq \phi[G] \implies \phi^{-1}[K'] \leq G$

Proof

1). Assume $a \in G$

$\phi(a)\phi(e) = \phi(ae) = \phi(a) = \phi(a)e'$
$\therefore \phi(e) = e'$

2). Assume $a \in G$

$\phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = e'$
But inverses are unique
$\therefore \phi(a^{-1}) = \phi(a)^{-1}$

3). Assume $H \leq G$

Assume $a', b' \in \phi[H]$
$\exists\, a, b \in H, \phi(a) = a'$ and $\phi(b) = b'$
By closure, $ab \in H$
$\phi(ab) = \phi(a)\phi(b) = a'b' \in \phi[H]$
$\therefore \phi[H]$ is closed under the operation.

$\phi(e) = e'$
$\therefore \phi[H]$ has an identity.

Assume $a' \in \phi[H]$
$\exists\, a \in H, \phi(a) = a'$
$a^{-1} \in H$
$\phi(a^{-1}) = \phi(a)^{-1} = (a')^{-1} \in \phi[H]$
$\therefore \phi[H]$ is closed under inverses.

$\therefore \phi[H] \leq G$

4). Assume $K' \leq G'$

Assume $a, b \in \phi^{-1}[K']$
$\exists\, a', b' \in K', \phi(a) = a'$ and $\phi(b) = b'$
By closure, $a'b' \in K'$
$\phi(ab) = \phi(a)\phi(b) = a'b' \in K'$
So $ab \in \phi^{-1}[K']$
$\therefore \phi^{-1}[K']$ is closed under the operation.

$\phi(e) = e'$
So $e \in \phi^{-1}[K']$
$\therefore \phi^{-1}[K']$ has an identity.

Assume $a \in \phi^{-1}[K']$
$\exists\, a' \in K', \phi(a) = a'$
$(a')^{-1} = \phi(a)^{-1} = \phi(a^{-1}) \in K'$
So $a^{-1} \in \phi^{-1}[K']$
$\therefore \phi^{-1}[K']$ is closed under inverses.

$\therefore \phi^{-1}[K'] \leq H$