Kernel

Definition

Let $\phi : G \to G'$ be a homomorphism of groups. The *kernel* of ϕ, denoted $\ker(\phi)$, is given by:

$$\ker(\phi) = \{g \in G \mid \phi(g) = e'\}$$

The kernel contains all elements that map to the identity.

Theorem

Let $\phi : G \to G'$ be a homomorphism of groups:

$$\ker(\phi) \leq G$$

Proof

Assume $a, b \in \ker(\phi)$
$a, b \in G$
By closure, $ab \in G$
$\phi(ab) = \phi(a)\phi(b) = e'e' = e'$
So $ab \in \ker(\phi)$
$\therefore \ker(\phi)$ is closed under the operation.

$\phi(e) = e'$
So $e \in \ker(\phi)$
$\therefore \ker(\phi)$ has an identity.

Assume $a \in \ker(\phi)$
$a \in G$
$a^{-1} \in G$
$\phi(a^{-1}) = \phi(a)^{-1} = (e')^{-1} = e'$
So $a^{-1} \in \ker(\phi)$
$\therefore \ker(\phi)$ is closed under inverses.

$\therefore \ker(\phi) \leq G$

Theorem

Let $\phi : G \to G'$ be a homomorphism of groups:

$$\phi \text{ is one-to-one} \iff \ker(\phi) = e$$

Proof

Assume ϕ is one-to-one
$\phi(e) = e'$
Assume $\exists\, a \in G, \phi(a) = e'$
$\phi(e) = \phi(a)$
$e = a$
$\therefore \ker(\phi) = \{e\}$

Assume $\ker(\phi) = \{e\}$
Assume $a, b \in G, \phi(a) = \phi(b)$
$\phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) = e'$
$ab^{-1} = e$
$a = b$
$\therefore \phi$ is one-to-one

Theorem

Let $\phi : G \to G'$ be a homomorphism of groups and $K = \ker(\phi)$:

$$\forall\, a \in G, aK = \{x \in G \mid \phi(x) = \phi(a)\}$$

A homomorphism collapses all of the elements in the coset to the same element in G'.

$$\underbrace{\begin{matrix} a \\ x_1 \\ x_2 \\ \vdots \\ x_n \end{matrix}}_{aK} \xrightarrow{\phi} \phi(a)$$

Proof

Assume $a \in G$

Assume $y \in aK$
$\exists\, k \in K, y = ak$
$\phi(y) = \phi(ak) = \phi(a)\phi(k) = \phi(a)e' = \phi(a)$
$\therefore y \in \{x \in G \mid \phi(x) = \phi(a)\}$

Assume $y \in \{x \in G \mid \phi(x) = \phi(a)\}$
$\phi(y) = \phi(a)$
$\phi(a)^{-1}\phi(y) = \phi(a^{-1})\phi(y) = \phi(a^{-1}y) = e'$
So $a^{-1}y \in K$ and thus $\exists\, k \in K, a^{-1}y = k$
$y = ak$
$\therefore y \in aK$

$\therefore aK = \{x \in G \mid \phi(x) = \phi(a)\}$

Theorem

Let $\phi : G \to G'$ be a homomorphism of groups and $K = \ker(\phi)$:

$$\forall\, a \in G, Ka = \{x \in G \mid \phi(x) = \phi(a)\}$$

Proof

Assume $a \in G$

Assume $y \in Ka$
$\exists\, k \in K, y = ka$
$\phi(y) = \phi(ka) = \phi(k)\phi(a) = e'\phi(a) = \phi(a)$
$\therefore y \in \{x \in G \mid \phi(x) = \phi(a)\}$

Assume $y \in \{x \in G \mid \phi(x) = \phi(a)\}$
$\phi(y) = \phi(a)$
$\phi(y)\phi(a)^{-1} = \phi(y)\phi(a^{-1}) = \phi(ya^{-1}) = e'$
So $ya^{-1} \in K$ and thus $\exists\, k \in K, ya^{-1} = k$
$y = ka$
$\therefore y \in Ka$

$\therefore Ka = \{x \in G \mid \phi(x) = \phi(a)\}$

Corollary

Let $\phi : G \to G'$ be a homomorphism of groups and $\ker(\phi) = K$:

$$\forall\, a \in G, aK = Ka$$

Theorem

Let $\phi : G \to G'$ be a homomorphism of groups and $\ker(\phi) = K$:

$$\forall\, g_1, g_2 \in G, \phi[g_1 K g_2] = \{\phi(g_1 g_2)\}$$

Proof

Assume $g_1, g_2 \in G$
Assume $k \in K$
$\phi(g_1 k g_2) = \phi(g_1)\phi(k)\phi(g_2) = \phi(g_1)e'\phi(g_2) = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$