Section 13 - Homomorphisms

- Let G, G' groups, $\phi: G \to G'$ is homomorphism if

$$\phi(ab) = \phi(a)\phi(b) \qquad \forall a, b \in G.$$

Examples • $\phi: G \to G'$, $\phi(a) = e'$ $\forall a \in G$ (trivial homomorphism)

• $\phi: S_n \to \mathbb{Z}_2$, $\phi(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ odd} \\ 0 & \text{if } \sigma \text{ even} \end{cases}$

- Group $\mathbb{R}^n$ with vector addition, $\mathbb{R}^n = \prod_{i=1}^{n} \mathbb{R}$ direct product.

- Let A be $(m \times n)$-matrix, then

$$\phi: \mathbb{R}^m \longrightarrow \mathbb{R}^n$$
$$\phi(\vec{v}) = A\vec{v} \qquad \vec{v} \in \mathbb{R}^n$$

is a homomorphism, since

$$\phi(\vec{v}+\vec{w}) = A(\vec{v}+\vec{w}) = A\vec{v} + A\vec{w} = \phi(\vec{v}) + \phi(\vec{w}).$$

- Let $D = \{ f: \mathbb{R} \to \mathbb{R} \mid f \text{ is differentiable} \}$, a group under addition

Let $F = \{ f: \mathbb{R} \to \mathbb{R} \}$.

- Let $\phi: D \to F$ be given by $\phi(f) = f'$. $f \in D$.

$$\phi(f+g) = (f+g)' = f' + g' = \phi(f) + \phi(g),$$

so ϕ is a homomorphism.

- Let $r \in \mathbb{Z}$, $\phi_r: \mathbb{Z} \to \mathbb{Z}$ be $\phi_r(n) = rn$, $n \in \mathbb{Z}$

$$\phi_r(n_1+n_2) = r(n_1+n_2) = rn_1 + rn_2 = \phi_r(n_1) + \phi_r(n_2) \qquad \forall n_1, n_2 \in \mathbb{Z},$$

so ϕ_r is a homomorphism.

Reduction modulo n: Let $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ be given by

$\gamma(m) = r$, r remainder when dividing m by n $(m = qn + r)$.

Claim γ is homomorphism.

For $m_1, m_2 \in \mathbb{Z}$, need to show $\gamma(m_1) +_n \gamma(m_2) = \gamma(m_1 + m_2)$.

Write $m_1 = q_1 n_1 + r_1$, $m_2 = q_2 n_2 + r_2$, $q_1, q_2 \in \mathbb{Z}$

$0 \le r_1, r_2 < n$.

Then $\gamma(m_1) = r_1$, $\gamma(m_2) = r_2$.

2 cases: (1) $r_1 + r_2 \le n-1 \Rightarrow \gamma(m_1) +_n \gamma(m_2) = r_1 +_n r_2 = r_1 + r_2$

$$m_1 + m_2 = q_1 n + r_1 + q_2 n + r_2 = (q_1 + q_2) n + (r_1 + r_2),$$

$$\gamma(m_1 + m_2) = r_1 + r_2 = \gamma(m_1) +_n \gamma(m_2).$$

(2) $r_1 + r_2 \ge n \Rightarrow \gamma(m_1) +_n \gamma(m_2) = r_1 +_n r_2 = r_1 + r_2 - n$

$$m_1 + m_2 = q_1 n + r_1 + q_2 n + r_2 = (q_1 + q_2 + 1) n + (r_1 + r_2 - n)$$

$$\Rightarrow \gamma(m_1 + m_2) = r_1 + r_2 - n = \gamma(m_1) +_n \gamma(m_2).$$

Properties of homomorphisms

Def Let X, Y be sets, $\phi : X \to Y$, $A \subseteq X$, $B \subseteq Y$.

"Image of A under ϕ" $= \phi[A] = \{\phi(a) \mid a \in A\}$

"Range of ϕ" $= \phi[X]$

"Inverse image of B" $= \phi^{-1}[B] = \{x \in X \mid \phi(x) \in B\}$

Thm "A homomorphism preserves identity elements, inverses & subgroups (both ways)"

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

(1) If $e \in G$ identity, $\phi(e) = e'$, identity in G'

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

(3) If $H \leq G$, $\phi[H]$ is a subgroup of G'

(4) If $K' \leq G'$, $\phi^{-1}[K']$ is a subgroup of G.

Proof (1) $\phi(e) = \phi(e)\phi(e) \Rightarrow \phi(ee) = \phi(e)\phi(e)$

$e' = \phi(e)\phi(e)^{-1} = \phi(e)\phi(e)\phi(e)^{-1} = \phi(e)$.

(2) $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e' \implies \phi(a^{-1}) = \phi(a)^{-1}$

(4) $\phi^{-1}[K']$ closed: $a, b \in \phi^{-1}[K'] \Rightarrow \phi(a), \phi(b) \in K' \Rightarrow \phi(ab) = \phi(a)\phi(b) \in K'$

$\Rightarrow ab \in \phi^{-1}[K']$

$e \in \phi^{-1}[K']$ since $e' \in K'$ & $\phi(e) = e'$

$a \in \phi^{-1}[K'] \Rightarrow \phi(a) \in K' \Rightarrow \phi(a^{-1}) = \phi(a)^{-1} \in K' \Rightarrow a^{-1} \in \phi^{-1}[K']$. □

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

The kernel ("kjernen") of ϕ is

$$\mathrm{Ker}(\phi) = \phi^{-1}[\{e'\}] = \{a \in G \mid \phi(a) = e'\}.$$

Example • $\phi: \mathbb{R}^m \to \mathbb{R}^m$ by $\phi(\vec{v}) = A\vec{v}$, $\mathrm{Ker}\,\phi$ = null space of A.

• $\phi: S_n \to \mathbb{Z}_2$, $\phi(\sigma) = \begin{cases} 1 & \sigma \text{ odd} \\ 0 & \sigma \text{ even} \end{cases} \Rightarrow \mathrm{Ker}\,\phi = \{\sigma \in S_n \mid \sigma \text{ even}\} = A_n$.

• $\phi: D \to F$, $\phi(f) = f'$. $\mathrm{Ker}\,\phi = \phi^{-1}[\{0\}] = \{f \in D \mid f' = 0\}$

$D = \{\text{differentiable functions}\}$, $F = \{\text{functions}\}$

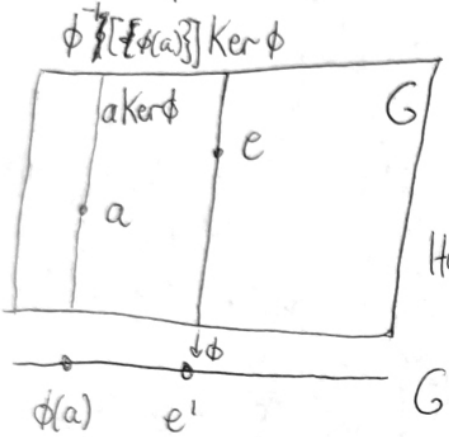
$= \{f: \mathbb{R} \to \mathbb{R} \mid f \text{ is constant}\}$.

- $\phi: \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $\phi(m) = r$ = remainder of m divided by n

$\ker \phi = \phi^{-1}[\{0\}] = \{ m \in \mathbb{Z} \mid \text{remainder is } 0 \}$

$= \{ m \in \mathbb{Z} \mid n \text{ divides } m \} = n\mathbb{Z}.$

"ϕ collapses cosets of $\ker \phi$ to one element"



Thm Let $\phi: G \longrightarrow G'$ be a homomorphism of groups, let $a \in G$, let $H = \ker \phi$. Then

$Ha = aH = \phi^{-1}[\{\phi(a)\}] = \{ x \in G \mid \phi(x) = \phi(a) \}$.

Important because:
- Describes solutions to equation $\phi(x) = \phi(a)$ as a coset
- Shows $H = \ker \phi$ has special property $aH = Ha \quad \forall a \in G$, this property does not hold for all subgroups of G!

Proof

Show only $aH = \{ x \in G \mid \phi(x) = \phi(a) \}$, omit Ha case.

(1) $aH \subseteq \{ x \in G \mid \phi(x) = \phi(a) \}$. Let $x \in aH$, then $x = ah$ for some $h \in H$.

$\Longrightarrow \phi(x) = \phi(ah) = \phi(a)\phi(h) = \phi(a)\, e' = \phi(a) \Rightarrow x \in \{ x \in G \mid \phi(x) = \phi(a) \}$.

(2) $\{ x \in G \mid \phi(x) = \phi(a) \} \subseteq aH$. Let $x \in G$ be s.t. $\phi(x) = \phi(a)$.

Then $\phi(a^{-1}x) = \phi(a^{-1})\,\phi(x) = \phi(a)^{-1}\phi(x) = \phi(a)^{-1}\phi(a) = e'$

$\Longrightarrow a^{-1}x \in H \Longrightarrow x = a(a^{-1}x) \in aH$.

□

Examples • $\phi : \mathbb{R}^n \to \mathbb{R}^m$, $\phi(\vec{v}) = A\vec{v}$. Fix $\vec{w} \in \mathbb{R}^n$

$$\{\vec{x} \in \mathbb{R}^n \mid A\vec{x} = A\vec{w}\} = \vec{w} + \operatorname{Ker}\phi = \{\vec{w} + \vec{y} \mid \vec{y} \in \mathbb{R}^n, A\vec{y} = 0\}.$$

• $\gamma : \mathbb{Z} \to \mathbb{Z}_n$, reduction modulo n. Let $m \in \mathbb{Z}$.

$$\{k \in \mathbb{Z} \mid \gamma(k) = \gamma(m)\} = m + \operatorname{Ker}\phi = m + n\mathbb{Z} = \{m + ni \mid i \in \mathbb{Z}\}.$$

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

ϕ is one-to-one $\iff \operatorname{Ker}\phi = \{e\}$

Proof If ϕ is one-to-one, then $\phi(x) = e' \Rightarrow x = e$, so $\operatorname{Ker}\phi = \{e\}$.

If $\operatorname{Ker}\phi = \{e\}$, then for any $y \in G$, $\{x \in G \mid \phi(x) = \phi(y)\} = y\operatorname{Ker}\phi = y\{e\} = \{y\}$.

Hence ϕ is one-to-one.

Corollary To check $\phi : G \to G'$ is isomorphism, need

(1) ϕ is homomorphism
(2) $\operatorname{Ker}\phi = \{e\}$
(3) ϕ is onto.

Example Let p be a prime, $\phi : \mathbb{Z}_p \to G'$ a group homomorphism. Then ϕ is either one-to-one or trivial (i.e. $\phi(n) = e' \ \forall n \in \mathbb{Z}_p$).

Proof $\operatorname{Ker}\phi \leq \mathbb{Z}_p$, the only subgroups of $\mathbb{Z}_p$ are $\{0\}$ & $\mathbb{Z}_p$. (Lagrange's thm!)

So either $\operatorname{Ker}\phi = \{0\} \iff \phi$ one-to-one,

or $\operatorname{Ker}\phi = \mathbb{Z}_p \iff \phi$ is trivial.

Def Let G be a group, $H \leq G$. Say H is **normal** if

$$gH = Hg \qquad \forall g \in G.$$

Examples • $\ker \phi$ is normal for any $\phi : G \to G'$ homomorphism

• If G is abelian, all $H \leq G$ are normal

• ~~$\langle (12) \rangle \leq S_3$ is not normal~~

• $\langle (12) \rangle = \{e, (12)\} \leq S_3$ is not normal:

$$(13)\langle (12) \rangle = \{(13), (123)\}$$

$$\langle (12) \rangle (13) = \{(13), (132)\}.$$