The Isomorphism Theorems

Images of Hom $\Longleftrightarrow$ Factor Groups

$\phi : G \to H$ a hom.

Recall

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

- Canonical homomorphisms (H is a normal subgroup)

$$\phi : G \longrightarrow G/H$$
$$g \longmapsto gH$$

Note $\ker(\phi) = H$

$$\phi(g_1 g_2) = g_1 g_2 H = g_1 H g_2 H = \phi(g_1)\phi(g_2)$$

Thm: (First isomorphism Thm.)

Let G, H be groups, $\psi : G \to H$ a homomorphism,

$K = \ker \psi$. Let $\phi : G \to G/\ker\psi$ be the

Canonical Hom. (for K). $\exists$ a unique isomorphism η

$\eta : G/\ker\psi \longrightarrow \psi(G)$ s.t. $\psi = \eta \circ \phi$

$\Updownarrow$

$\psi(G) = \eta \circ \phi(G)$

$$\begin{tikzcd} G \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & H \\ & G/\ker\psi \arrow[ur, "\cong\ \eta"'] & \end{tikzcd}$$

– theorem says η exists

$$\boxed{\psi(G) \cong G/\ker\psi}$$

$\eta : G/\ker\psi \longrightarrow \psi(G)$

Proof: $K = \ker(\psi)$ is normal in G

Define $\eta : G/K \longrightarrow \psi(G)$

$gK \longmapsto \psi(g)$

Show η is well defined, i.e. doesn't depend on coset representative

If $g_1 K = g_2 K$

If $g_1 K = g_2 K$ $K = \ker\psi$ $\exists\, k_1 k_2 \in K$ s.t

$g_1 k_1 = g_2 k_2$

$g_1 \underbrace{k_1 k_2^{-1}}_{= \bar{k}} = g_2$ $\therefore$

$$\eta(g_1 K) = \psi(g_1)\cdot \underbrace{\psi(\bar{k})}_{= e_H \text{ since } \bar{k}\in\ker\psi}$$
$$= \psi(g_1 \bar{k})$$
$$= \psi(g_2) = \eta(g_2 K)$$

$\therefore$ well defined !!

Show η is a homomorphism:

$$\eta(g_1 K g_2 K) = \eta(g_1 g_2 K) = \psi(g_1 g_2)$$
$$= \psi(g_1)\,\psi(g_2) = \eta(g_1 K)\,\eta(g_2 K)$$

η is onto since $\eta : G/\ker\psi \longrightarrow \psi(G)$

$gK \longmapsto \psi(g)$.

Show η is 1-1: Say $\eta(g_1 K) = \eta(g_2 K)$

$$\Rightarrow \quad \psi(g_1) = \psi(g_2)$$

$$e_H = (\psi(g_1))^{-1}\,\psi(g_2)$$
$$= \psi(g_1^{-1})\,\psi(g_2) = \psi(g_1^{-1} g_2)$$

$\therefore$ $g_1^{-1} g_2 \in \ker(\psi)$

$$g_1^{-1} g_2 K = K$$

$$g_2 K = g_1 K$$

$\therefore$ η is 1-1

$\blacksquare$

<u>Ex</u> $G = \langle g \rangle$

$$\phi : \mathbb{Z} \longrightarrow G$$
$$n \longmapsto g^n$$

This is a surjective hom.

$$\phi(\mathbb{Z}) = \langle g \rangle = G$$

If $|g| = m \Rightarrow g^m = e$

$\therefore$ $\ker(\phi) = m\mathbb{Z}$

$\therefore$ By 1^{st} iso. thm. $\mathbb{Z}/\ker(\phi) = \underbrace{\mathbb{Z}/m\mathbb{Z}}_{}^{=\mathbb{Z}_m} \cong G$

$\therefore$ a cyclic group of order m is $\cong$ to $\mathbb{Z}_m$

If $|g| = \infty \Rightarrow \ker\phi = \{0\}$

$$\therefore \quad \mathbb{Z}/\ker(\phi) \cong \phi(G) = G$$
$$\mathbb{Z}/\{0\} \cong \mathbb{Z} \qquad \therefore G \cong \mathbb{Z}$$

$\therefore$ an infinite cyclic group $\cong \mathbb{Z}$.

Thm (2nd iso Theorem)

Let H be a subgroup of G. Let N be a normal subgroup of G. Then $HN = \{hn \mid h \in H, n \in N\}$ is a subgroup of G, $H \cap N$ is a normal subgroup of G and

$$H/(H \cap N) \cong HN/N.$$

Proof:

Show HN is a subgroup.

- $e \in HN$ since $e \in H$, $e \in N$

Closure: Let $h_1 n_1, h_2 n_2 \in HN$

$$(h_1 n_1)(h_2 n_2) = \underbrace{\overbrace{h_1 h_2}^{\hat{h}}}_{\in H} \underbrace{\overbrace{h_2^{-1} n_1 h_2}^{\hat{n}}}_{\in N \text{ since } N \text{ is normal}} n_2$$

Since N is normal
$h^{-1} N h = N$
$\Rightarrow h^{-1} n h \in N \quad \forall n \in N$

$$= \hat{h} \hat{n} n_2 = \hat{h} \bar{n} \in HN$$

$$(hn)^{-1} = n^{-1} h^{-1} = h^{-1} \underbrace{\overbrace{h n^{-1} h^{-1}}^{\hat{n}}}_{\in N \text{ since } N \text{ is normal}}$$

$$= h^{-1} \hat{n} \in HN$$

$\therefore$ HN is a subgroup

Now prove $H \cap N$ is normal in H, $h \in H$, $n \in H \cap N$

Show $h^{-1} n h \in H \cap N$ $\forall n \in H \cap N$, $h \in H$

$\Rightarrow$

$h^{-1} n h \in H$, $h^{-1} n h \in N$ since N is normal in G, $h \in G$

$\therefore$ $h^{-1} n h \in H \cap N$

$\therefore \quad h^{-1}(H\cap N)h \subseteq H\cap N \quad \therefore\ H\cap N$ is normal in H

Show $\quad H/(H\cap N) \simeq HN/N$.

Define $\quad \phi : H \longrightarrow HN/N$

$$h \longmapsto hN \qquad (h\in H,\ n\in N)$$

- ϕ is onto since $\quad hnN = hN = \phi(h) \quad \therefore\ \phi(H) = HN/N$
- $\phi(h_1 h_2) = h_1 h_2 N = h_1 N h_2 N = \phi(h_1)\phi(h_2)$

$\therefore\ \phi$ is a hom and $\phi(H) = HN/N$

By the first isomorphism theorem

$$\phi(H) \simeq H/\ker(\phi)$$

$$\Updownarrow \qquad HN/N \simeq H/\ker(\phi)$$

$$\ker(\phi) = \{ h\in H \mid \underbrace{\phi(h) = N}_{hN = N} \}$$

$$\therefore\ \ker(\phi) = \{ h\in H \mid h\in N \} = H\cap N$$

$$\therefore \quad HN/N \simeq H/(H\cap N) \quad . \qquad \blacksquare$$

Thm: (Third Iso Thm)

Let G be a group, N, H be normal subgroups, $N \subseteq H$.

Then

$$G/H \simeq (G/N)/(H/N)$$

Thm (Correspondence Thm) Let N be a normal subgroup of G. There is a 1-1 corespondence (bijective map) between

$$\{ \text{Subgroups } H \mid N \subseteq H \} \xleftrightarrow{1-1} \{ \text{Subgroups of } G/N \}$$

map is given by $\gamma: H \longmapsto H/N$

Further

$$\{ \text{normal subgroups } H \mid N \subseteq H \} \xleftrightarrow{1-1} \{ \text{normal subgroups of } G/N \}$$

Proof: Let H be a subgroup of G, $N \subseteq H$

N is normal in G $\therefore$ N is normal in H, i.e. H/N makes sense

Show H/N is a subgroup of G/N

- $N \in H/N$ $\therefore$ contains identity
- let $aN, bN \in H/N$

$$aN(bN)^{-1} = ab^{-1}N \in H/N \quad \text{since } a, b \in H$$

$\therefore$ H/N is a subgroup G/N

Show that $\gamma : \tilde{H} \longmapsto \tilde{H}/N$ is onto:

Let S be a subgroup of G/N

set $H = \{ g \in G \mid gN \in S \}$ ✓ check this is a subgroup of G containing N

$N \subseteq H$ since if $n \in N$ $nN = N \in S$

If $h_1, h_2 \in H$, since S is a group,

$$h_1 N \, h_2 N = h_1 h_2 N \in S \quad \text{and} \quad h_1^{-1} N \in S$$

$$\therefore \; h_1 h_2 \in H \quad \text{and} \quad h_1^{-1} \in H$$

$\therefore$ H is a subgroup and $\gamma : \tilde{H} \longmapsto \tilde{H}/N$ is onto

Show γ is 1-1:

Let H_1, H_2 be subgroups of G, $N \subseteq H_1$, $N \subseteq H_2$

$$\gamma(H_1) = \gamma(H_2)$$
$$H_1/N = H_2/N$$

[show $H_1 \subseteq H_2$ $H_2 \subseteq H_1$ $\therefore H_1 = H_2$]

If $h_1 \in H_1 \;=\; h_1 N \in H_1/N$, $h_1 N = h_2 N$ for some $h_2 \in H_2$

$$\therefore \; h_1 \in h_1 N = h_2 N \subseteq H_2$$

$$h_1 \in H_2 \Rightarrow H_1 \subseteq H_2$$

Similarly $H_2 \subseteq H_1$ $\therefore$ $H_1 = H_2$ $\therefore$ γ is 1-1.

Suppose - H is normal in G

- N is a subgroup of H

$$\phi : G/N \longrightarrow G/H$$
$$gN \mapsto gH \qquad \text{This is a hom (check)}$$

$\ker(\phi) = H/N$ Since $hH = H$ $h \in H$

$\therefore$ H/N is normal in G/N

and by the 1^{st} isomorphism thm

$$\phi(G/N) \cong G/N \big/ \ker(\phi) = G/N \big/ (H/N)$$

ϕ is onto since we take all rep. of each coset gN to all rep. of gH i.e. if $\tilde{g}H \in G/H$

$\tilde{g}H = \phi(\tilde{g}N)$ $\therefore$ onto

$$G/H \cong G/N \big/ \ker(\phi) = G/N \big/ (H/N)$$

This proves the 3^{rd} isomorphism Thm.

Now suppose H/N is normal in G/N

$$G \xrightarrow{\psi} G/N \xrightarrow{\phi} G/N \big/ H/N$$

$\ker(\psi) = N \subseteq H$ $\qquad$ $\ker(\phi) = H/N$

all together $G \xrightarrow{\rho} G/N / H/N$

$\ker(\rho) = H$

$\therefore H$ is is normal in G $\blacksquare$

The isomorphism theorems are neede to prove:

Thm (Fund. Thm. Fin. Gen. Abel. Groups)
Let G be a finitely generated abelian group,
$G = \langle g_1, \ldots, g_n \rangle = \{ g_1^{a_1} \cdots g_n^{a_n} \mid a_1, \ldots, a_n \in \mathbb{Z} \}$. Then

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_m^{\alpha_m}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}.$$

Rings

Def: A non-empty set R is a ring if it is closed under 2 binary operations, which we refer to as addition and multiplication, with the following properties $a, b, c \in R$

- $a + b = b + a$
- $(a+b)+c = a+(b+c)$
- $0 \in R$ s.t. $a + 0 = a$
- For all $a \in R$ $\exists$ $-a \in R$ s.t $a + (-a) = 0$

$(R,+)$ is a abelian group

- $(ab)\cdot c = a\cdot(bc)$
- $a\cdot(b+c) = a\cdot b + a\cdot c$

  $(a+b)\cdot c = a\cdot c + b\cdot c$

End def.

Special types of Rings

- Say R has <u>unity</u> or <u>identity</u> if $\exists\ 1 \in R$ s.t. $1 \neq 0$ and

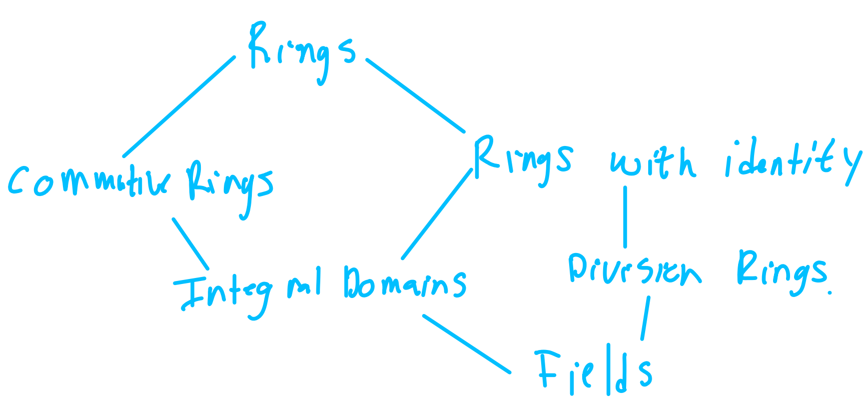
$$1\cdot a = a\cdot 1 = a \quad \forall a \in R.$$

- <u>Commutative ring</u> $\quad ab = ba \quad \forall\, a,b \in R$

- A commutative ring with identity where $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$ is called an <u>Integral Domain</u>.

- A ring R is a <u>Division Ring</u> if $\forall a \in R$ $a \neq 0$ $\exists$ $a^{-1} \in R$ s.t. $a^{-1}a = aa^{-1} = 1$. we call a a <u>unit</u> in R.

- A commutative Division ring is a <u>field</u>.



Ex) $\mathbb{Z}$ - integral domain, Not a field

1, -1 are only units

Fields : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Ex) $\mathbb{Z}_n$ is a commutative ring, but not an integral domain

Provided n is not prime

Ex) $\mathbb{Z}_{12}$ $\quad 3 \cdot 4 = 12 \bmod 12 = 0$

$\therefore$ $3 \neq 0$ and $4 \neq 0$ are zero divisors

$\therefore$ Not an integral domain

Def) $a \in R$ is a zero divisor $(a \neq 0)$ if $\exists$ $b \in R$ $(b \neq 0)$

s.t $a \cdot b = 0$.

Integral domain = commutative ring with 1 and with <u>no</u> zero divisors.

Ex) $C[a,b]$ = continuous real valued functions on $[a,b]$

commutative ring

$f, g \in C[a,b]$

$(f+g)(x) = f(x) + g(x) \quad \forall x \in [a,b]$

$(f \cdot g)(x) = f(x)\, g(x) \quad \forall x \in [a,b]$.

Ex] 2×2 real matrices

$$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad 1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$AB \neq BA$ a ring, but <u>not</u> commutive

has units = A s.t. $\det(A) \neq 0$, but <u>Not</u> a division ring

Ex] The Quternions are a non-commutive division ring

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$\mathbb{H} = \{ a\cdot 1 + bI + cJ + dK \mid a,b,c,d \in \mathbb{R} \}$ is a ring

Not commutive, $IJ = K$, $JI = -K$

- Has identity $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\therefore \quad (a + bI + cJ + dK)^{-1} = \left(\frac{a - bI - cJ - dK}{a^2 + b^2 + c^2 + d^2} \right)$$

$\therefore$ Division Ring

<u>Proposition</u> | Let R be a ring with $a,b \in R$. Then

1) $a \cdot 0 = 0 \cdot a = 0$

2) $a(-b) = (-a)(b) = -ab$

3) $(-a)(-b) = ab$

Proof: (1) $a \cdot 0 = a(0+0) = a0 + a0$

$$\cancel{a \cdot 0 - a0} = a0 + \cancel{a0 - a0}$$

$$0 = a0$$

By the same argument $0 \cdot a = 0$.

2) show $a(-b) = (-a)b = -ab$.

$$\underbrace{ab + a(-b)}_{\text{these are additive inverses}} = a(b-b) = a \cdot 0 = 0$$

$\therefore \quad a(-b) = -ab$

Same argument for $(-a)b = -ab$

3) show $(-a)(-b) = ab$

$$(-a)(-b) \overset{\text{By (2)}}{=} -(a(-b)) \overset{\text{By (2)}}{=} -(-ab) = ab$$

■