# Section 26 - Homomorphisms & factor rings

Recall a map of rings $\phi: R \to R'$ is a homomorphism if for all $a, b \in R$,

$$\phi(a) + \phi(b) = \phi(a+b)$$
$$\phi(a)\phi(b) = \phi(ab).$$

Examples: • For $n \in \mathbb{Z}^+$, $\phi: \mathbb{Z} \to \mathbb{Z}_n$ $\phi(k)$ = remainder of $k$ divided by $n$.

• For $F$ a field, $a \in F$, evaluation homomorphism

$$\phi_a : F[x] \longrightarrow F$$
$$\phi_a(f(x)) = f(a)$$

• For $R = \{f : \mathbb{R} \to \mathbb{R}\}$ ring of real 1-variable functions

$$\phi : R \longrightarrow \mathbb{R}$$
$$\phi(f) = f(0).$$

Properties of homomorphisms Thm: Let $R$, $R'$ be rings, $S'$ a subring of $R'$, $\phi: R \to R'$ a homomorphism. Then

- $\phi[R] \subseteq R'$ is a subring of $R'$
- $\phi^{-1}[S'] \subseteq R$ ——— " ——— $R$
- $\phi(0_R) = 0_{R'}$
- For $a \in R$, $\phi(-a) = -\phi(a)$.
- If $R$ has unity $1 \in R$, then $\phi(1)$ is unity for $\phi[R]$.

**Def** If $\phi: R \to R'$ is a homomorphism of rings, its kernel is

$$\operatorname{Ker}\phi = \phi^{-1}[\{0\}] = \{r \in R \mid \phi(r) = 0\},$$

a subring of $R$.

**Example** $\phi: \mathbb{Z} \to \mathbb{Z}_n$, $\operatorname{Ker}\phi = n\mathbb{Z} \leq \mathbb{Z}$.

**Thm:** $a, b \in R$, $\phi: R \to R'$ a ring homomorphism, then

$$\phi^{-1}[\phi(a)] = \{b \in R \mid \phi(b) = \phi(a)\} = a + \operatorname{Ker}\phi.$$

**Corollary:** $\phi: R \to R'$ a ring homomorphism. Then

$$\phi \text{ is injective} \iff \operatorname{Ker}\phi = \{0\}.$$

---

**Factor rings** Let $\phi: R \to R'$ be a ring homomorphism, $H = \operatorname{Ker}\phi$. Then $R/H = \{\text{left cosets of } H\}$ has a ring structure by, for $a, b \in R$

$$(a+H) + (b+H) = (a+b) + H$$
$$(a+H)(b+H) = ab + H$$

**Proof** (1) $R/H$ is an abelian group, ok since $H$ is a normal subgroup of $(R, +)$.

(2) Multiplication well-defined: If $a+H = a'+H$, $b+H = b'+H$, then $a' = a + h_1$, $b' = b + h_2$ $\quad h_1, h_2 \in H$. Get

$$a'b' = (a+h_1)(b+h_2) = ab + h_1 b + a h_2 + h_1 h_2.$$

Claim: $h_1 b + a h_2 + h_1 h_2 \in H$.

Check: $\phi(h_1 b + a h_2 + h_1 h_2) = \phi(h_1)\phi(b) + \phi(a)\phi(h_2) + \phi(h_1)\phi(h_2)$

$$= 0\phi(b) + \phi(a)0 + 00 = 0,$$

so $h_1 b + a h_2 + h_1 h_2 \in \operatorname{Ker}\phi = H$.

Hence $a'b' \in ab+H$, so $a'b'+H = ab+H$, multiplication well-defined

(3) Multiplication associative & distributive laws, hold, easy to check.

~~$((a+H)(b+H))(c+H) = (ab+H)(c+H)$~~

**Thm** In above setting $\mu : R/H \longrightarrow \phi[R]$ is a ring iso given by

$$\mu(a+H) = \phi(a)$$

is a ring isomorphism.

**Proof** Know from factor group theory that $\mu$ is a group isomorphism $(R/H, +) \cong (\phi[R], +)$. The map $\mu$ is a ring homomorphism by

$$\mu((a+H)(b+H)) = \mu(ab+H) = \phi(ab) = \phi(a)\phi(b)$$
$$= \mu(a+H)\mu(b+H).$$

□

**Ideals:** Let $R$ be a ring $N$ a subgroup of $(R,+)$. Then $N$ is an *ideal* if for all $a \in R$ we have

$$aN \subseteq N \quad \& \quad Na \subseteq N.$$

~~Thm Let R be~~

**Example** · $n \in \mathbb{Z}^+$, $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal since for any $m \in \mathbb{Z}$,

$$m(n\mathbb{Z}) = mn\mathbb{Z} \subseteq n\mathbb{Z} \qquad n\mathbb{Z}m = (nm)\mathbb{Z} \subseteq n\mathbb{Z}.$$

· If $\phi : R \to R'$ is a ring homomorphism, $\ker\phi$ is an ideal of $R$, since for $a \in R$, $n \in \ker\phi$ we have

$$\phi(an) = \phi(a)\phi(n) = \phi(a)0 = 0 \implies an \in \ker\phi$$
$$\phi(na) = \phi(n)\phi(a) = 0\,\phi(a) = 0 \qquad na \in \ker\phi.$$

**Thm** Let $H \subseteq R$ be a subgroup of $(R,+)$. Then $R/H$ has a well-defined ring structure with

$$(a+H)+(b+H) = (a+b)+H$$
$$(a+H)(b+H) = ab+H$$

if and only if $H$ is an ideal.

---

$R/H$ is the factor ring / quotient ring of $R$ by $N$.

**Example** In $F[x]$, the set $H = \{ f(x) = \sum_{n=0}^{\infty} a_n x^n \mid a_0 = 0 \}$ is an ideal.

Direct proof: $f(x) \in H$, $f(x) = a_n x^n + \cdots + a_1 x$

$g(x) \in F[x]$, $g(x) = b_m x^m + \cdots + b_0$

$$f(x)g(x) = g(x)f(x) = a_n b_m x^{m+n} + \cdots + a_1 b_0 x \in H.$$

Alternatively: $H = \ker \phi_0$, $\phi_0 : F[x] \to F$

$$\phi_0(f(x)) = f(0).$$

**Fundamental homomorphism theorem for rings** Let $\phi : R \to R'$ be a ring homomorphism, $H = \ker \phi$. Then have $\gamma : R \to R/N$, $\mu : R/N \to R'$,

$$\gamma(a) = a+H$$
$$\mu(a+H) = \phi(a),$$

these are ring homomorphisms, & $\phi = \mu \circ \gamma$.

$\mu$ gives an isomorphism $R/H \simeq \phi[R]$

