Gallian Ch 15 Ring homomorphisms

Part I: Ring homomorphisms

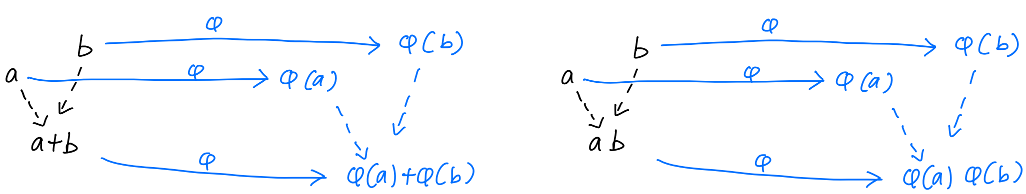
(Just as a group homomorphism preserves the group operation, a ring homomorphism preserves the two ring operations)

<u>Def</u> A <u>ring homomorphism</u> from a ring R to a ring S

is a map $\varphi : \underset{\text{domain}}{R} \longrightarrow \underset{\text{codomain}}{S}$ satisfying

$$\underbrace{\varphi(a +_R b) = \varphi(a) +_S \varphi(b)}_{\varphi \text{ preserves addition}} \quad \text{AND} \quad \underbrace{\varphi(a \cdot_R b) = \varphi(a) \cdot_S \varphi(b)}_{\varphi \text{ preserves multiplication}} \quad \text{for all } a, b \in R$$

Illustration:



<u>Def</u> The <u>kernel</u> of $\varphi : R \to S$ is the set

$$\ker \varphi = \{ x \in R : \varphi(x) = 0_S \}$$

<u>Def</u> If a ring homomorphism is injective and surjective, it is called an <u>isomorphism</u>.

Ex Given $n \in \mathbb{Z}_{>0}$, the map $\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}_n$

(Extra) defined by $a \longmapsto a \pmod{n}$

is a surjective ring homomorphism.

Check that • $\varphi(a+b) = \varphi(a) + \varphi(b)$

• $\varphi(ab) = \varphi(a)\,\varphi(b)$

$\ker \varphi = \{ nk : k \in \mathbb{Z} \} = n\mathbb{Z}$

It is a surjective map.

Ex The map $\varphi: \mathbb{C} \longrightarrow \mathbb{C}$

$\varphi(a+bi) = a - bi$

is a ring isomorphism.

(Prove that $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in \mathbb{C}$)

Prove that $\varphi(xy) = \varphi(x)\,\varphi(y)$ for all $x, y \in \mathbb{C}$:

$$\begin{aligned}
\varphi((a+bi)(c+di)) &= \varphi((ac - bd) + (ad+bc)i) \\
&= ac - bd - (ad+bc)i \\
&= (a-bi)\,(c-di) \\
&= \varphi(a+bi)\,\varphi(c+di)
\end{aligned}$$

Prove that φ is injective:

Let $\varphi(a+bi) = \varphi(c+di)$

$a - bi = c - di$

Then $a = c$ and $b = d$, so $a+bi = c+di$.

(Prove that φ is surjective)

<u>Ex</u> Let $\mathbb{R}[x]$ denote the ring of all polynomials with real coefficients.

* Consider the map $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{R}$

$$p(x) \mapsto p(5)$$

that is, if $p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

then $\varphi(p(x)) = a_0 + a_1 5 + a_2 5^2 + \dots + a_n 5^n$

Then φ preserves addition and multiplication.

This map is called the <u>evaluation homomorphism</u> at 5.

<u>Note</u> $\ker \varphi = \{ p(x) \in \mathbb{R}[x] : \underbrace{\varphi(p(x))}_{p(5)} = 0 \}$

$= \{ p(x) \in \mathbb{R}[x] :$ 5 is a zero/root of $p(x) \}$

$p(x) \in \ker \varphi$ iff 5 is a root of $p(x)$

* In general, given $\alpha \in \mathbb{R}$,

the map $\varphi_\alpha : \mathbb{R}[x] \longrightarrow \mathbb{R}$

$$p(x) \mapsto p(\alpha)$$

is called <u>the evaluation homomorphism at α</u>.

<u>Note:</u> $p(x) \in \ker \varphi_\alpha$ iff α is a root of $p(x)$

<u>Recall</u> Since $\mathbb{R}$ is a field, an elt $\alpha \in \mathbb{R}$ is a root of $p(x) \in \mathbb{R}[x]$ iff $(x-\alpha)$ is a factor of $p(x)$ in $\mathbb{R}[x]$.

Prop Let $\varphi: R \to S$ be a ring homomorphism.

1. $\varphi(0_R) = 0_S$

   Compare with: "If $f: G \to H$ is a group homomorphism, then $f(e_G) = e_H$"

2. We cannot say the same about the multiplicative identity (unity) since not all rings have them.

   If R and S have unities 1_R and 1_S (respectively) and if φ is surjective, then $\varphi(1_R) = 1_S$.

Proof of 1

$$\varphi(0_R) \overset{\text{def of } 0_R}{=} \varphi(0_R + 0_R) \overset{\text{def. of homomorphism}}{=} \varphi(0_R) + \varphi(0_R) \quad \text{and}$$

$$\varphi(0_R) = 0_S + \varphi(0_R)$$

So $0_S + \varphi(0_R) = \varphi(0_R) + \varphi(0_R)$.

By cancellation (since $(S,+)$ is a group), we have $\varphi(0_R) = 0_S$

Prop The kernel of a ring homomorphism $\varphi: R \to S$ is an ideal of R.

Proof We know from group theory that $\ker\varphi$ is an additive subgroup of R.

Let $r \in R$, $a \in \ker\varphi$.

Show that $ar \in \ker\varphi$:

$$\varphi(ar) = \varphi(a)\varphi(r) = 0\,\varphi(r) = 0$$

Show that $ra \in \ker\varphi$:

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)\,0 = 0. \quad \square$$

$\boxed{\text{If } \ker\varphi = \{0\}, \text{ then } \varphi \text{ is injective}}$

Part II: First Isomorphism Theorem

Note

Recall the natural or canonical homomorphism of groups

$$\pi : R \longrightarrow R/I$$
$$r \longmapsto r+I$$

The kernel of π is I and π is surjective.

Thm Let I be an ideal of R.

The map $\pi : R \longrightarrow R/I$

$r \longmapsto r+I$

is a ring homomorphism from R onto R/I with kernel I.

Pf The note above tells us π is surjective, is a group homomorphism, and has kernel I.

It remains to show that π preserves multiplication.

Let $s, t \in R$. Then

$$\pi(s)\,\pi(t) = (s+I)(t+I) = st+I = \pi(st) \qquad \square$$

First Isomorphism Thm

Let $f: R \to S$ be a ring homomorphism

Let K denote $\ker f$.

Let $i: R/K \to S$ be defined by

$$r+K \longmapsto f(r) \quad \text{for all } r+K \in R/K$$

Then i is an injection $R/K \hookrightarrow S$.

In particular, we have an isomorphism given by i

$$\boxed{R/K \xrightarrow{\cong} \operatorname{Im} f}$$ — the upshot

Furthermore, $f = i \circ \pi$

the natural onto homomorphism
$R \longrightarrow R/\ker f$

The diagram

$$\begin{tikzcd}
R \arrow[r, "\pi"] \arrow[dr, "f"'] & R/\ker f \arrow[d, dashed, "i"'] \\
 & f(R)
\end{tikzcd}$$

, called a "commutative diagram"

illustrates the 1st isomorphism Thm.

We say "the diagram commutes" to mean $f = i \circ \pi$.

<u>Note</u> This tells us that every ring homomorphism can be written as a composition

$$(\text{1-1 homomorphism}) \circ (\text{onto homomorphism}).$$

<u>Ex</u> $\varphi: \mathbb{Z}[x] \to \mathbb{Z}$ defined by $\varphi(p(x)) = p(0)$

the constant term of $p(x)$

$\ker \varphi = \langle x \rangle = \{ f(x)\, x : f(x) \in \mathbb{Z}[x] \}$

By 1st Isomorphism Thm, $\mathbb{Z}[x] / \langle x \rangle \cong \mathbb{Z}$

— the end —