Quotient Rings

Wednesday, 23 March 2022 14:12

Recall: A homomorphism of (abelian) groups is a map $\varphi : G \to G'$ s.t.
$\varphi(a+b) = \varphi(a) +' \varphi(b)$.

$H = \ker(\varphi)$ for some $\varphi : G \to G'$
$\Leftrightarrow$ H is a normal subgp of G,
i.e. G/H is a well-defined quotient gp

$G/\ker(\varphi) \cong \varphi(G)$ $\quad \varphi : G \longrightarrow G/H$

A ring homomorphism $\varphi : R \to R'$ is a map s.t.

(1) $\varphi(a+b) = \varphi(a) +' \varphi(b)$

(2) $\varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b)$

$\ker(\varphi) = \{ r \in R : \varphi(r) = 0_{R'} \}$
$= \varphi^{-1}(0_{R'})$.

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

(i) $\varphi(0_R) = 0_{R'}$

(ii) $\varphi(-a) = -\varphi(a)$

(iii) If $S \subseteq R$ is a subring, then $\varphi(S)$ is a subring of R'

(iv) If $S' \subseteq R'$ is a subring, then $\varphi^{-1}(S')$ is a subring of R

(v) If R has a unity 1, then $\varphi(1)$ is a unity of $\underline{\varphi(R)}$.

(vi) If R has a unity 1, then $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Proof: (i), (ii) are statements about group homomorphisms.

(iii) Only need to check $\varphi(S)$ is closed under $\cdot$.

Let $\varphi(a), \varphi(b) \in \varphi(S)$, $a, b \in S$

$$\varphi(a) \cdot' \varphi(b) = \varphi(a \cdot b) \quad \begin{pmatrix}\text{Axiom of} \\ \text{ring morphism}\end{pmatrix}$$

$$\in \varphi(S) \quad \begin{pmatrix}S \text{ is closed} \\ \text{under } \cdot\end{pmatrix}$$

(iv) Only need to check $\varphi^{-1}(S')$ is closed under $\cdot$.

Let $a, b \in \varphi^{-1}(S')$, i.e., $\varphi(a), \varphi(b) \in S'$.

$$\varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b) \in S'$$

$$\Rightarrow a \cdot b \in \varphi^{-1}(S').$$

(v) Need to check $\forall r' \in \varphi(R)$,

$$\varphi(1_R) \cdot' r' = r' \cdot \varphi(1_R) = r'.$$

Let $r' = \varphi(r)$.

$$\varphi(1_R) \cdot' r' = \varphi(1_R) \cdot' \varphi(r)$$

$$= \varphi(1_R \cdot r)$$

$$= \varphi(r) = r'$$

(vi) Need to check
$$\varphi(a^{-1})\cdot'\varphi(a) = 1_{\varphi(R)} \left(= \varphi(1_R)\right)$$
$$\varphi(a^{-1})\cdot'\varphi(a) = \varphi(a^{-1}\cdot a)$$
$$= \varphi(1_R) = 1_{\varphi(R)} \quad \square$$

Example:
- $\varphi: \mathbb{Z} \to \mathbb{Z}_n$
- $ev_\alpha(f) = f(\alpha)$ $\quad ev_\alpha : \{f: \mathbb{R} \to \mathbb{R}\} \to \mathbb{R}$, $\alpha \in \mathbb{R}$
- Let $R_1, \dots, R_n$ be rings. $1 \le i \le n$

Then $\pi_i : R_1 \times \dots \times R_n \to R_i$

by $\pi_i((r_1, \dots, r_n)) = r_i$

- $\iota : R_i \to R_1 \times \dots \times R_n$ by

$i(r_i) = (0_1, \dots, r_i, \dots, 0_n)$

$\iota : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$

$\iota(1) = (1,0)$ is a unity of $\iota(\mathbb{Z}) \cong \mathbb{Z}\times\{0\}$ but not the unity of $\mathbb{Z}\times\mathbb{Z}$, which is $(1,1)$. (A non-example for (v) that $\varphi(1_R)$ need not to be the unity of R')

Def: Let $\varphi: R \to R'$. We define $R/\ker\varphi$ ($= I$) as $\{a+I : a \in R\}$.

$(a+I)+(b+I) = (a+b)+I$

$(a+I)\cdot(b+I) = ab+I$.

Prop: R/I is a ring

Proof: All statements involving only + follow from quotient group.

- Multiplication is well-defined.

Suppose $a' \in a+I$, $b' \in b+I$.

Then need to show $a'b'+I = ab+I$.

$a' = a+h_1$, $b' = b+h_2$, $h_1, h_2 \in I$.

$$a'b' = (a+h_1)(b+h_2)$$
$$= ab + \underbrace{ah_2 + h_1 b + h_1 h_2}_{\text{Want to check it is in } I. \; = \ker(\varphi)}$$

$$\varphi(ah_2 + h_1 b + h_1 h_2)$$

$$= \varphi(a)\overset{0}{\varphi(h_2)} + \overset{0}{\varphi(h_1)}\varphi(b) + \overset{0}{\varphi(h_1)}\overset{0}{\varphi(h_2)}$$
$$= 0$$

$\Rightarrow ah_2 + h_1 b + h_1 h_2 \in \ker(\varphi) = I$

$\Rightarrow a'b' + I = ab + I$ $\square$

Theorem: Let $\varphi: R \to R'$. Then

$R/\ker(\varphi) \cong \varphi(R)$, by

$\mu: a+I \longmapsto \varphi(a)$.

(where $\ker(\varphi) = I$)

Proof: μ is a group isomorphism.

Only need to show μ preserves $\cdot$

$$\begin{aligned}
&\mu((a+I)(b+I)) \\
&= \mu(ab+I) \\
&= \varphi(ab) \\
&= \varphi(a)\cdot\varphi(b) \\
&= \mu(a+I)\mu(b+I)
\end{aligned}$$

$\square$

Def: A subring $I \subseteq R$ is an ideal if $\forall a \in R$

$aI = \{ah : h \in I\} \subseteq I$

$Ia = \{ha : h \in I\} \subseteq I$

Example: $6\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal b/c $\forall m \in \mathbb{Z}, \forall 6n \in 6\mathbb{Z}$,

$m(6n) = 6(mn) \in 6\mathbb{Z}$

$\Rightarrow m(6\mathbb{Z}) \subseteq 6\mathbb{Z}$

$\{0\} \subseteq \mathbb{Z}$ is an ideal b/c

$\forall m \in \mathbb{Z}, \; m \cdot 0 = 0 \in \{0\}$

In general, $\{0\}$ is an ideal of any ring. Any ring is an ideal of itself.

Prop: R/I is well-defined if and only if I is an ideal.

Proof: "$\Rightarrow$" Suppose

$(a+I)(b+I) = ab+I$ is well-defined.

Need to check $aI \subseteq I$ ($\forall a \in R$)

Need to check $\forall a \in R, \forall h \in I, ah \in I$.

Since $(a+I)I$ is well-defined.

$(a+I)I = (a+I)(0+I) = (a \cdot 0) + I = 0 + I$

$(a+I)I = (a+I)(h+I) = ah + I$

are the same, i.e., $ah \in I$

"$\Leftarrow$": Need to show

$(a+I)(b+I) = ab + I$ is well-defined.

$a' \in a + I$, $b' \in b + I$

$\Rightarrow a' = a + h_1$, $b' = b + h_2$ for $h_1, h_2 \in I$

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

$= ab + \underbrace{h_1 b}_{\in I} + \underbrace{ah_2}_{\in I} + \underbrace{h_1 h_2}_{\in I} \Big\} \in I$

$\Rightarrow a'b' + I = ab + I$

So multiplication is well-defined in R/I. $\square$

- - - -

Prop: Let I be an ideal of R.

Then $R/I = \{a + I : a \in R\}$

with $(a+I) + (b+I) = (a+b) + I$

and $(a+I)(b+I) = ab + I$

is a well-defined ring.

Also, $\gamma : R \to R/I$ by

$\gamma(a) = a + I$ is a ring homomorphism

whose kernel is precisely I.

"kernels of ring homomorphisms $\Leftrightarrow$ ideals"

Both are for forming quotient rings.