26: Homomorphism and Quotient Rings

Given a ring R and $S \leq R$ a subring, we wish to make $R/S = \{r + S : r \in R\}$ (additive cosets) into a ring.

If we only consider the additive groups of R, S. We already know that R/S is an abelian group because R is an abelian group, so S must be a normal subgroup.

Now let's consider the multiplication:

$$(r_1 + S) \times (r_2 + S) = r_1 r_2 + S.$$

Let's try

$$\begin{aligned}(r_1 + s_1 + S) \times (r_2 + s_2 + S) &= (r_1 + s_1)(r_2 + s_2) + S \\ &= r_1 r_2 + s_1 r_2 + r_1 s_2 + s_1 s_2 + S\end{aligned}$$

We need $(r_1 r_2 + s_1 r_2 + r_1 s_2 + s_1 + s_2) - r_1 r_2 = s_1 r_2 + r_1 s_2 + s_1 + s_2 \in S$.

This must work when $r_1 = r_2 = 0$, $s_1 s_2 \in S \ \forall \ s_1, s_2 \in S$.

This must work when $s_1 = 0$, $r_1 s_2 \in S \ \forall \ r_1 \in R, s_2 \in S$.

This must work when $s_2 = 0$, $s_1 r_2 \in S \ \forall \ s_1 \in S, r_2 \in R$.

By the above observation/requirements, we need to require S to be nonempty, closed under $+, -$, and if $r \in R$ and $s \in S$, then $rs, sr \in S$.

Definition: ideal

Let R be a ring and let $I \leq R$. We say I is a (two-sided) **ideal** of R if

(i) $0 \in I$ or $I \neq \emptyset$.

(ii) If $i_1, i_2 \in I$ then $i_1 + i_2 \in I$ and $i_1 - i_2 \in I$ (or negation).

(iii) If $i \in I$ and $r \in R$ then $ri \in I$ (left ideal) and $ir \in I$ (right ideal).

If I is an ideal of R, we write $I \trianglelefteq R$.

Note. The first two conditions are already given by subring. The third condition implies closure under multiplication.

Example. $\mathbb{Z} \leq \mathbb{Q}$ but $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$. Take $r = 3 \in \mathbb{Z}$ and $\frac{1}{7} \in \mathbb{Q}$, but $3 \times \frac{1}{7} \notin \mathbb{Z}$.

Example. $2\mathbb{Z} \trianglelefteq \mathbb{Z}$. We know this is a subring. If $i \in 2\mathbb{Z}$ and $r \in \mathbb{Z}$, then $ri = ir \in 2\mathbb{Z}$. "Multiplying an even integer by any integer gives an even integer."

Example. $R = M_2(\mathbb{R})$ (matrix ring). Let $s = \{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{R}\}$. It's a subring.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & 0 \\ f & 0 \end{pmatrix} = \begin{pmatrix} ae + bf & 0 \\ ce + df & 0 \end{pmatrix}.$$

But it wouldn't work on the right.

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin S.$$

So this is a left ideal but not a ring ideal. If we swap the columns or transpose, we can get a right ideal.

Let R be a ring and $I \trianglelefteq R$. Define $R/I = \{r + I : r \in R\}$. Define

$$\begin{aligned} (r + I) + (s + I) &= r + s + I \\ (r + I) \times (s + I) &= rs + I \text{ well-defined} \end{aligned}$$

To show that this is a ring, we need to show associativity of $\times$ and distributive laws.

Distributivity:

$$\begin{aligned} ((r + I) + (s + I))(t + I) &= ((r + s) + I) \times (t + I) \\ &= (r + s)t + I \\ &= rt + st + I \\ &= (rt + I) + (st + I) \\ &= ((r + I)(t + I)) + ((s + I)(t + I)) \end{aligned}$$

The rest are similar. Thus R/S is a ring!

Example. Let $n \in \mathbb{N}$. Then $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z}$ is a ring. This is $\mathbb{Z}_n$ by definition.

Example. $\mathbb{Z}_7 \coloneqq \mathbb{Z}/7\mathbb{Z}$.

$$\begin{aligned} (5 + 7\mathbb{Z}) \times (4 + 7\mathbb{Z}) &= 20 + 7\mathbb{Z} \\ &= 6 + 7\mathbb{Z} \text{ because } 20 - 6 \in 7\mathbb{Z} \end{aligned}$$

So $\overline{5} \times \overline{4} = \overline{6}$.

Theorem

If R is commutative, then so is R/I. (The converse is false.)

If R has identity 1_R, then so does R/I which is $1_R + I$.

Let $\phi : R \to S$ be a ring homomorphism. It preserves addition and multiplication. The kernel

$$\ker \phi = \{r \in R : \phi(r) = 0_S\}.$$

Theorem

$\ker \phi \trianglelefteq R$.

Proof

We know $\ker \phi \leq R$ subgroup by applying group theory and ignoring multiplication. We also need to know if $k \in \ker \phi, r \in R$, then $rk \in \ker \phi$ and $kr \in \ker \phi$.

$$\phi(rk) = \phi(r)\phi(k) = \phi(r) \cdot 0 = 0$$
$$\phi(kr) = 0$$

Thus, $rk \in \ker \phi, kr \in \ker \phi$. □

Example. Let $I \trianglelefteq R$. Consider the map $\pi : R \to R/I, r \mapsto r + I$. Then π is a ring homomorphism.

$$\pi(r + s) = (r + s) + I$$
$$\pi(r) + \pi(s) = (r + I) + (s + I)$$
$$\pi(r \times s) = rs + I$$
$$\pi(r) \times \pi(s) = (r + I)(s + I)$$

$\operatorname{im} \pi = R/I$. The zero element of R/I is $0_R + I$.

$$r \in \ker \phi \Leftrightarrow \pi(r) = 0 + I$$
$$\Leftrightarrow r + I = 0 + I$$
$$\Leftrightarrow r - 0 \in I \Leftrightarrow r \in I$$

Summary: kernels of ring homomorphisms are ideals. Ideals are kernels of ring homomorphisms.

Theorem

Let $\phi : R \to S$ be a homomorphism of rings. ϕ is injective if and only if $\ker \phi = \{0_R\}$.