Ring homomorphisms

A ring homomorphism is a map between rings that preserves both the additive and multiplicative structures.

Def: Let R and S be rings.

1.) A ring homomorphism is a function $\varphi: R \to S$ s.t. for all $a, b \in R$,

   a.) $\varphi(a+b) = \varphi(a) + \varphi(b)$, and

   b.) $\varphi(ab) = \varphi(a)\varphi(b)$

2.) The kernel of φ is $\ker \varphi := \{a \in R \mid \varphi(a) = 0\}$ (i.e. the same as the kernel of φ viewed as a group homomorphism.

3.) A bijective ring homomorphism is an isomorphism.

Ex: The map $\varphi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sending a to $\bar{a}$ is a ring homomorphism.

Ex: The map $\varphi_n: \mathbb{Z} \to \mathbb{Z}$ defined $\varphi_n(a) = na$ is not in general a ring homomorphism.

If $n \neq 1$ then $\varphi(1 \cdot 1) = n \neq n^2 = \varphi(1)\varphi(1)$.

This is, however a group homomorphism (and, we will later see, a $\mathbb{Z}$-module homomorphism).

Ex: Let R be a ring.

Define $\varphi : R[x] \to R$ by

$\varphi(f(x)) = f(0)$. That is, f maps to its constant term.

This is a homomorphism!

$\ker \varphi$ = polynomials w/ zero constant term.

Just as in the case of groups, kernels and images of homomorphisms are rings:

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

1.) $\operatorname{im} \varphi$ is a subring of S.

2.) $\ker \varphi$ is a subring of R.

Pf: We know $\operatorname{im}\varphi$ and $\ker \varphi$ are subgroups, so we just need to check they're closed under multiplication.

If $\varphi(a), \varphi(b) \in \operatorname{im}\varphi$, then $\varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{im}\varphi$.

If $a, b \in \ker\varphi$, then $\varphi(ab) = \varphi(a)\varphi(b) = 0 \Rightarrow ab \in \ker\varphi$. □

Quotient rings

If I is a subgroup of R, then since R is an

abelian group, I is normal in R, so R/I is a group.

Question: For which subrings I is R/I also a ring?

i.e. if we define $(a+I)(b+I) = ab+I$, when is this well-defined?

i.e. we want that if $i, j \in I$, then for any $a, b \in R$

$$(a+i)(b+j) \in ab+I$$

But $(a+i)(b+j) = ab + aj + ib + ij$

If $a = b = 0$, this says that $ij \in I$. That is, we need I to be closed under multiplication, which means I must be a ring.

Setting $a = 0$ and $j = 0$, we get $ib \in I$.
Similarly, we show that $aj \in I$.

That is, this shows that if $r \in R$, $a \in I$, then $ra \in I$ and $ar \in I$.

Subrings that satisfy this property are called ideals:

Def: Let R be a ring, $I \subseteq R$ a subring.

1.) If $\forall\ r \in R, a \in I$, we have $ra \in I$, then I is a left ideal.

2.) If $ar \in I\ \ \forall\ a \in I, r \in R$, then I is a right ideal.

3.) If $ar \in I$ and $ra \in I\ \ \forall\ a \in I, r \in R$, then I is a two-sided ideal, or just an ideal.

We just showed that if $I \subseteq R$ is a subgroup s.t. the multiplication on R/I is well-defined, then I is an ideal. In fact, the converse holds:

Theorem: Let $I \subseteq R$ be a subgroup of a ring R. Then the multiplication on R/I

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

is well-defined and makes R/I a ring if and only if I is an ideal (a two-sided ideal).

Pf: We just need to show the "$\Leftarrow$" implication. Assume I is an ideal.

First we show the multiplication is well-defined.

Suppose $a' \in a+I$, $b' \in b+I$. Then $a' = a+r$, $b' = b+s$, some $s, r \in R$.

$\Rightarrow a'b' = (a+r)(b+s) = ab + \underbrace{as}_{\in I} + \underbrace{rb}_{\in I} + \underbrace{rs}_{\in I} \in ab + I$

$\Rightarrow a'b' + I = ab + I$. Thus, the multiplication is well-defined.

The operation is associative and distributive, since R is a ring. Thus R/I is a ring. $\square$

Def: When I is an ideal, R/I is called the quotient ring of R by I.

Analogous to normal subgroups, I is an ideal $\Leftrightarrow$ it's the kernel of some homomorphism:

Thm: 1.) (1st isomorphism theorem for rings) If $\varphi: R \to S$ is a ring homomorphism, then $\ker\varphi$ is an ideal of R, and $R/\ker\varphi$ is isomorphic to $\operatorname{im}\varphi$.

2.) If I is any ideal of R, then the map

$$R \to R/I \quad \text{defined} \quad r \mapsto r+I$$

is a surjective ring homomorphism with kernel I.

Pf: 1.) We know $\ker\varphi$ is a subgroup, so we just need to show that if $a \in \ker\varphi$, $r \in R$, then ar and $ra \in \ker\varphi$.

$\varphi(ar) = \varphi(a)\varphi(r) = 0 = \varphi(r)\varphi(a) = \varphi(ra)$. Thus, $\ker\varphi$ is an ideal.

By the first isomorphism theorem of groups, the map

$$R/\ker\varphi \to \operatorname{im}\varphi \quad \text{defined} \quad r+I \mapsto \varphi(r)$$

is a well-defined group isomorphism. Moreover,

$$(r+I)(s+I) = rs+I \mapsto \varphi(rs) = \varphi(r)\varphi(s), \text{ so}$$

it's a ring isomorphism.

2.) The map is a surjective homomorphism by construction. The kernel is the same as the kernel when considering this as a map of groups, which is I. $\square$

In fact, the remaining isomorphism theorems also hold for rings (see D+F), though the 1st is the most important.

Remark (ideal criterion): As mentioned in the proof above, in order to check that a subset $I \subseteq R$ is an ideal, we just need to check:

- $I \neq \emptyset$
- If $a, b \in I$, then $a - b \in I$
- If $a \in I$, $r \in R$, then $ar \in I$ and $ra \in I$.

Examples:

1.) For any ring R, $\{0\}$ and R are both ideals.

2.) For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$: If $n \mid a$ then $n \mid ab$ $\forall$ $b \in \mathbb{Z}$, so $ab \in n\mathbb{Z}$. Since these are the only subgroups of $\mathbb{Z}$, these must be the only ideals of $\mathbb{Z}$.

3.) Let $R = \mathbb{Z}[x]$. Define $I \subseteq R$ to be the set of polynomials with no constant or linear term. i.e.

$$I = \{a_0 + a_1 x + \dots + a_n x^n \mid a_0 = a_1 = 0\}$$

Note that I is in fact an ideal: it's closed under subtraction, and multiplication can't decrease the powers of x that appear. i.e. if $f \in I$, $g \in R$, where

$$f = a_2 x^2 + \dots + a_m x^m, \quad g = b_0 + b_1 x + \dots + b_n x^n$$

then $fg = a_2 b_0 x^2 +$ higher degree terms $\in I$.

What is R/I in this case?

$f + I = g + I \iff f - g \in I \iff f$ and g differ by a polynomial whose terms are of degree ≥ 2.

i.e. if $f = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, then

$f + I = (a_0 + a_1 x) + I$. If we write $\bar{f}$ to mean $f + I$, then $\bar{f} = \overline{a_0 + a_1 x}$. That is, each coset has a (unique!)

representative of the form $a + bx$.

We can add and multiply w/ representatives:

$$(\overline{1+2x})(\overline{2-3x}) = \overline{2 + x - 6x^2} = \overline{2+x}.$$