Quotient Rings

Recall: Given a ring homomorphism $f: R \to S$
the kernel of f is a subring of R

$$\operatorname{Ker} f \subset R$$

s.t. $\forall a \in R$, $x \in \operatorname{Ker} f$, $a \cdot r, r \cdot a \in \operatorname{Ker} f$

Defn: Given a ring homomorphism $f: R \to S$
Let $I = \operatorname{Ker} f$, and $r \in R$
The coset of $r \in R$ with respect to f (or wrt I)
is the set

$$r + I := \{ r + x \mid x \in I = \operatorname{Ker} f \}$$

The quotient ring of R by I is the set

$$R/I := \{ r + I \mid r \in R \}$$

Prop: Given a ring homomorphism $f: R \longrightarrow S$
with $I = \operatorname{Ker} f$
The quotient ring R/I is a ring with operations

$$(r + I) + (s + I) := (r + s) + I$$

$$(r + I) \cdot (s + I) := (r \cdot s) + I$$

Note: If I is understood, we will often write $\bar{r}$ for $r + I$

e.g. $(r + I) + (s + I) = (r + s) + I$

becomes $\bar{r} + \bar{s} = \overline{r + s}$

Lemma 1 If $r, s \in R$ and $(r+I) \cap (s+I) \neq \emptyset$

Then $r+I = s+I$

Pf: Suppose $x \in (r+I) \cap (s+I)$

$\Longrightarrow x \in r+I \Longrightarrow x = r+a, \ a \in I$

$x \in s+I \Longrightarrow x = s+b, \ b \in I$

$\Longrightarrow r+a = s+b.$

$\Longrightarrow r = s+(b-a), \ s = r+(a-b)$

$I \subset R$ is a subring $\Longrightarrow b-a, a-b \in I$

$\Longrightarrow r \in s+I, \ s \in r+I$

$\Longrightarrow$ If we take any element $c \in I$

Then $r+c = (s+(b-a))+c = s+\underbrace{(b-a+c)}_{\in I} \in s+I$

$\Longrightarrow r+I \subset s+I$.

Similarly, we see that $s+I \subset r+I \Longrightarrow r+I = s+I$ $\square$

Example: $f: \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $\ker f = 2\mathbb{Z}$

$n \longmapsto n \bmod 2$

Consider the coset of $1 \in \mathbb{Z}$, $1+2\mathbb{Z}$

$1+2\mathbb{Z} = 3+2\mathbb{Z} = -7+2\mathbb{Z} = 29+2\mathbb{Z}$

Lemma 2: If $r+I = r'+I$

$s+I = s'+I$

Then $(r+s)+I = (r'+s')+I$

$(r\cdot s)+I = (r'\cdot s')+I$

i.e. $+, \cdot$ are well-defined in R/I.

Pf: $r+I = r'+I \implies r = r'+x \,,\; x\in I$

$s+I = s'+I \implies s = s'+y \,,\; y\in I$ $\quad \underset{\cup}{I}$

$\implies (r+s) = (r'+x)+(s'+y) = (r'+s')+(x+y)$

$\implies r+s \in (r'+s')+I$

On the other hand $r+s = r+s+0 \in (r+s)+I$

$\implies [(r+s)+I] \cap [(r'+s')+I] \neq \emptyset$.

By Lemma 1 $\implies (r+s)+I = (r'+s')+I$.

$r\cdot s = (r'+x)\cdot(s'+y) = r's' + \underbrace{r'y + xs' + xy}_{\in I} \in r's'+I$ $\square$

Obs: R/I consists of the equivalence classes in R of the equivalence relation given by

$$x \sim y \text{ iff } x-y\in I$$

Pf: of Prop.

- $\bar{0}+\bar{a} = \overline{0+a} = \bar{a} = \overline{a+0} = \bar{a}+\bar{0}$ $\quad$ ($\bar{0}\in R/I$ is $+$ identity)
- $\bar{a}+\overline{(-a)} = \overline{a+(-a)} = \bar{0} = \overline{(-a)+a} = \overline{(-a)}+\bar{a}$
- $\bar{a}+(\bar{b}+\bar{c}) = \bar{a}+(\overline{b+c}) = \overline{a+(b+c)} = \overline{(a+b)+c} = \overline{(a+b)}+\bar{c} = (\bar{a}+\bar{b})+\bar{c}$
- $\bar{a}\cdot(\bar{b}\cdot\bar{c}) = \bar{a}\cdot(\overline{bc}) = \overline{a(b\cdot c)} = \overline{(a\cdot b)\cdot c} = \overline{ab}\cdot\bar{c} = (\bar{a}\cdot\bar{b})\cdot\bar{c}$
- $\bar{a}\cdot(\bar{b}+\bar{c}) = \bar{a}\cdot(\overline{b+c}) = \overline{a\cdot(b+c)} = \overline{a\cdot b+a\cdot c} = \overline{ab}+\overline{a\cdot c} = \bar{a}\cdot\bar{b}+\bar{a}\cdot\bar{c}$

$\square$

<u>Defn</u>: Let R be a ring, $I \subset R$

We say I is a

(1) <u>left ideal</u> if I is a subring s.t. $\forall a \in R,\ x \in I$
$$a \cdot x \in I$$

(2) <u>right ideal</u> if I is a subring s.t. $\forall a \in R,\ x \in I$
$$x \cdot a \in I$$

(3) <u>ideal</u> if I is both a left and right ideal (sometimes a <u>two-sided ideal</u>)

<u>Obs</u>: If $f: R \to S$ is a ring homomorphism then $\operatorname{Ker} f$ is an ideal in R.

<u>Note</u>: We may define R/I for <u>any</u> ideal $I \subset R$ whether or not $I = \operatorname{Ker} f$ for some ring homom. $f: R \to S$

<u>Thm:</u> (The First Isomorphism Theorem)

If $f: R \to S$ is a ring homomorphism

and $I = \operatorname{Ker} f$

Then $R/I \cong \operatorname{Im} f$ as rings.

<u>Pf:</u> If $r \in R$, then $r + I = f^{-1}(f(r))$

pre-image, not inverse.

$= \{x \in R \mid f(x) = f(r)\}$

[If $a \in I$, then $f(r+a) = f(r) + f(a) = f(r)$

$\implies r + a \in f^{-1}(f(r)) \implies r + I \subset f^{-1}(f(r))$.

If $x \in f^{-1}(f(r))$, then $f(r) = f(x)$

$\implies f(r) - f(x) = 0$

$f(r - x) = 0$

$\implies x - r \in \operatorname{Ker} f \implies x = r + (x - r) \in r + I$

$\implies f^{-1}(f(r)) \subset r + I \implies r + I = f^{-1}(f(r))$]

There is a bijective map.

$$\bar{f} : R/I \longrightarrow \operatorname{Im} f$$

$$\bar{r} \longmapsto f(r)$$

The point being that $\bar{f}$ is independent of the representative $r \in R$

□

<u>Thm:</u> If $I \subset R$ is an ideal

Then the <u>quotient map</u>

$$f : R \longrightarrow R/I$$
$$r \longmapsto \bar{r}$$

is a surjective ring homomorphism.

with $\operatorname{Ker} f = I$.

<u>Pf:</u> • f is clearly surjective.

• $f(a+b) = \overline{a+b} = \bar{a} + \bar{b} = f(a) + f(b)$

• $f(a \cdot b) = \overline{a \cdot b} = \bar{a} \cdot \bar{b} = f(a) \cdot f(b)$.

• If $f(a) = \bar{0}$, then by definition $\bar{a} = \bar{0}$

i.e. $a \in I$ $\square$

<u>Example:</u> For any integer $n \in \mathbb{Z}$

$$n\mathbb{Z} = \{ nx \mid x \in \mathbb{Z} \}$$ is an ideal in $\mathbb{Z}$

and the quotient ring of $\mathbb{Z}$ by $n\mathbb{Z}$ is exactly the ring

$$\mathbb{Z}/n\mathbb{Z}$$

Example: $R = \mathbb{Z}[X]$

$I := \{ p(x) \in R$ with all non-zero terms having degree at least $2 \}$

e.g. $7x^2 + 3x^3 + 10x^9 \in I$

Note: $0 \in I$ b/c it has no terms with non-zero coeff.

Exercise: I is an ideal.

If $p(x), q(x) \in R$ and $\overline{p(x)} = \overline{q(x)}$

then $p - q \in I$

So $p-q$ consists of terms of at least degree 2.

i.e. The degree 0 and degree 1 parts of p, q agree.

e.g. $\overline{5 + x + 7x^3} = \overline{5 + x - 21x^5 + 7x^{19}}$

$\Longrightarrow$ The polynomials of degree at most 1 represent distinct cosets in R/I

e.g. $5+x, \; -7+2x, \; 11-4x$

$\Longrightarrow$ There is a bijection between

$$R/I \longleftrightarrow \{ a + bx \mid a, b \in \mathbb{Z} \}$$

Obs: R/I has zero divisors: $\overline{x} \cdot \overline{x} = \overline{x^2} = \overline{0}$

Example: Let R be a ring, X a non-empty set.

Consider the ring

$$\mathcal{F}(X,R) := \{f : X \longrightarrow R\}$$

For a fixed element $a \in X$, the evaluation map at a is

$$Ev_a : \mathcal{F}(X,R) \longrightarrow R$$
$$f \longmapsto f(a).$$

Exercise: Ev_a is a ring homomorphism.

Moreover, Ev_a is a surjective ring homom.

and $Ker(Ev_a) := \{f \in \mathcal{F}(X,R) \mid f(a) = 0\}$

In particular, by the First Isomorphism Thm

$$\Longrightarrow \mathcal{F}(X,R)/Ker(Ev_a) \cong R$$