Quotient Rings

Recall that given a ring homomorphism $f : R \to S$, the kernel of f, $\operatorname{Ker} f$, is a subring of R.

Definition 4.1: Coset and Quotient Ring

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 w.r.t I) is the set

$$r + I \coloneqq \{r + x | x \in I = \operatorname{Ker} f\}$$

The **quotient ring** of R by I is the set

$$R/I \coloneqq \{r + I | r \in R\}$$

Proposition 4.1: Coset space is a ring

Given a ring homomorphism $f : R \to S$ with $I = \operatorname{Ker} f$, the quotient ring R/I is a ring with operations

$$(r + I) + (s + I) \coloneqq (r + s) + I$$
$$(r + I) \bullet (s + I) \coloneqq (r \bullet s) + I$$

Note: If I is understood, we will often write $\overline{r}$ for $r + I$, e.g

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

becomes

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

Lemma 4.1

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

Proof. Suppose $x \in (r + I) \cap (s + I)$, then

$$x \in r + I \implies x = r + a, a \in I$$
$$x \in s + I \implies x = s + b, a \in I$$

These together lead to three equivalent equations

$$r + a = s + b \iff r = s + (b - a) \iff s = r + (a - b)$$

Since $I \subset R$ is a subring then we know $b - a, a - b \in I$. Then the previous equations imply

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

Now take any element $c \in I$, then

$$r + c = (s + (b - a)) + c = s + (b - a + c) \in s + I \implies r + I \subset s + I$$

where the last implication comes from the fact that $b - a + c$ are elements in I and as such their combination is as well.
With similar logic we see that

$$s + c = (r + (a - b)) + c = r + (a - b + c) \in r + I \implies s + I \subset r + I$$

Hence, $r + I = s + I$. ■

Example 4.1. Let f be the homomorphism from the integers to the integers mod 2, i.e

$$\begin{aligned} f :& \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \\ & n \mapsto n \bmod 2 \end{aligned}$$

Immediately we know that the kernel is the set of even integers, $\operatorname{Ker} f = 2\mathbb{Z}$.
Consider the coset of $1 \in Z$ which is $1 + 2\mathbb{Z}$, then

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

where the equivalence follows from Lemma 4.1.

Lemma 4.2

If

$$\begin{aligned} r + I &= r' + I \\ s + I &= s' + I \end{aligned}$$

then

$$\begin{aligned} (r + s) + I &= (r' + s') + I \\ (r \bullet s) + I &= (r' \bullet s') + I \end{aligned}$$

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

Proof. Let $r, r', s, s' \in R$, then

$$\begin{aligned} r + I = r' + I &\implies r = r' + x,\ x \in I \\ s + I = s' + I &\implies s = s' + y,\ y \in I \end{aligned}$$

Then their sum

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

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

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

By Lemma 4.1, it is immediate that

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

Similarly,

$$r \bullet s = (r' + x) \bullet (s' + y) = r's' + r'y + xs' + xy \in r' \bullet s' + I$$

■

Observe that R/I consists of the equivalence classes in R of the equivalence relation given by

$$x \sim y \iff x - y \in I$$

Proof of Prop 4.1.
We check that the quotient is a ring

$$\overline{0} + \overline{a} = \overline{0 + a} = \overline{a} = \overline{a + 0} = \overline{a} + \overline{0} \qquad (\overline{0} \in R/I \text{ is the additive identity})$$

$$\overline{a} + \overline{(-a)} = \overline{a + (-a)} = \overline{0} = \overline{(-a) + a} = \overline{(-a)} + \overline{a}$$

$$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + (\overline{b + c}) = \overline{a + (b + c)} = \overline{(a + b) + c} = \overline{(a + b)} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}$$

$$\overline{a} \bullet (\overline{b} \bullet \overline{c}) = \overline{a} \bullet (\overline{bc}) = \overline{a \bullet (b \bullet c)} = \overline{(a \bullet b) \bullet c} = \overline{ab} \bullet \overline{c} = (\overline{a} \bullet \overline{b}) \bullet \overline{c}$$

$$\overline{a} \bullet (\overline{b} + \overline{c}) = \overline{a} \bullet (\overline{b + c}) = \overline{a \bullet (b + c)} = \overline{a \bullet b + a \bullet c} = \overline{ab} + \overline{ac} = \overline{a} \bullet \overline{b} + \overline{a} \bullet \overline{c}$$

■

Definition 4.2: Ideal

Let R be a ring and $I \subset R$.
We say I is a

(i) **Left ideal** if I is a subring such that for all $a \in R, x \in I$
$$a \bullet x \in I$$
(ii) **Right ideal** if I is a subring such that for all $a \in R, x \in I$
$$x \bullet a \in I$$
(iii) **Ideal** if I is both a left and right ideal (sometimes called a **two-sided ideal**).

Observe that 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 **any** ideal $I \subset R$, whether or not $I = \operatorname{Ker} f$ for some ring homomorphism $f : R \to S$.

Theorem 4.1: 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.

Proof. We first prove a smaller claim.
Claim: If $r \in R$, then
$$r + I = f^{-1}(f(r)) = \{x \in R | f(x) = f(r)\}$$
(Here f^{-1} is the preimage, not the inverse).

Proof. If $a \in I$, then
$$f(r + a) = f(r) + f(a) = f(r) \implies r + a \in f^{-1}(f(r)) \implies r + I \subset f^{-1}(f(r))$$
Similarly, if $x \in f^{-1}(f(r))$, then
$$f(r) = f(x) \implies f(r) - f(x) = 0 \implies f(r - x) = 0$$
This last equality means $r - x$ (and $x - r$) $\in \operatorname{Ker} f$, hence
$$x - r \in \operatorname{Ker} f \implies x = r + (x - r) \in r + I \implies f^{-1}(f(r)) \subset r + I$$
Therefore, both inclusions are proved and $r + I = f^{-1}(f(r))$. ■

There is a bijective map
$$\begin{aligned} \overline{f} : & R/I \to \operatorname{Im} f \\ & \overline{r} \mapsto f(r) \end{aligned}$$
The point being that $\overline{r}$ is independent of the representative $r \in R$. ■

Theorem 4.2: Canonical quotient map is surjective

If $I \subset R$ is an ideal, then the **quotient map**
$$\begin{aligned} f : & R \to R/I \\ & r \mapsto \overline{r} \end{aligned}$$
is a surjective ring homomorphism with $\operatorname{Ker} f = I$

Proof. Firstly, f is clearly surjective because every element of $r \in R$ will be an element of its own equivalence class. It remains to show that this is a homomorphism.
$$f(a + b) = \overline{a + b} = \overline{a} + \overline{b} = f(a) + f(b)$$
$$f(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = f(a) \cdot f(b)$$
For the kernel, by definition of the map $f(a) = \overline{a}$, but if we also have that $f(a) = \overline{0}$ then by definition of equivalence classes $\overline{a} = \overline{0}$ because if $a \sim 0$ then $\overline{a} = \overline{0}$.
Therefore $a \in I = \operatorname{Ker} f$. ■

Example 4.2. For any integer $n \in \mathbb{Z}$, we have that

$$n\mathbb{Z} = \{nx | x \in \mathbb{Z}\}$$

is an ideal in $\mathbb{Z}$.
Furthermore, the quotient ring of $\mathbb{Z}$ by $n\mathbb{Z}$ is exactly the ring $\mathbb{Z}/n\mathbb{Z}$.

Example 4.3. Let $R = \mathbb{Z}[X]$ and define

$$I \coloneqq \{p(X) \in R | \text{ all nonzero terms have degree at least 2}\}$$

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

<u>**Note:**</u> $0 \in I$ because it has **no** terms with non-zero coefficient. **Exercise:** Prove that I is an ideal. Now consider two polynomials $p(X), q(X) \in R$ and $\overline{p(X)} = \overline{q(X)}$, then by definition of equivalence, $p - q \in I$.
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

$$5 + X + 7X^3 = 5 + X - 21X^5 + 7X^{19}$$

This implies that the polynomials of degree at most 1 represent *distinct* cosets in R/I, e.g

$$5 + X, \; -7 + 2X, \; 11 - 4X$$

Therefore, there is a bijection between

$$R/I \iff \{a + bX | a, b, \in \mathbb{Z}\}$$

Observe that R/I has zero divisors: $\overline{x} \cdot \overline{X} = \overline{X^2} = \overline{0}$.

Example 4.4. Let R be a ring and X a non-empty set.
Consider the ring

$$\mathcal{F}(X, R) \coloneqq \{f : X \to R\}$$

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

$$\begin{aligned} \mathrm{Ev}_a : \mathcal{F}(X, R) &\to R \\ f &\mapsto f(a) \end{aligned}$$

Exercise: Ev_a is a ring homomorphism.
Moreover, Ev_a is a *surjective* ring homomorphism and

$$\mathrm{Ker}(\mathrm{Ev}_a) \coloneqq \{f \in \mathcal{F}(X, R) | f(a) = 0\}$$

In particular, by the First Isomorphism Theorem we have

$$\mathcal{F}(X, R)/\mathrm{Ker}(\mathrm{Ev}_a) \cong R$$