Quotient Rings

- If $R$ is a ring and $I$ is a two-sided ideal, the set of cosets of $R$ mod $I$ is denoted $R/I$. $R/I$ is the quotient ring of $R$ mod $I$; it becomes a ring under the operations
  
  \[(r + I) + (s + I) = (r + s) + I \quad \text{and} \quad (r + I)(s + I) = rs + I.\]

- (The First Isomorphism Theorem) If $f : R \rightarrow S$ is a ring map, then $\frac{R}{\ker f} \cong \text{im } f$.

Let $R$ be a ring, and let $I$ be a (two-sided) ideal. Considering just the operation of addition, $R$ is a group and $I$ is a subgroup. In fact, since $R$ is an abelian group under addition, $I$ is a normal subgroup, and the quotient group $\frac{R}{I}$ is defined. Addition of cosets is defined by adding coset representatives:

\[(a + I) + (b + I) = (a + b) + I.\]

The zero coset is $0 + I = I$, and the additive inverse of a coset is given by $-(a + I) = (-a) + I$.

However, $R$ also comes with a multiplication, and it’s natural to ask whether you can turn $\frac{R}{I}$ into a ring by multiplying coset representatives:

\[(a + I) \cdot (b + I) = ab + I.\]

I need to check that that this operation is well-defined, and that the ring axioms are satisfied. In fact, everything works, and you’ll see in the proof that it depends on the fact that $I$ is an ideal. Specifically, it depends on the fact that $I$ is closed under multiplication by elements of $R$.

By the way, I’ll sometimes write “$\frac{R}{I}$” and sometimes “$R/I$”; they mean the same thing.

Theorem. If $I$ is a two-sided ideal in a ring $R$, then $R/I$ has the structure of a ring under coset addition and multiplication.

Proof. Suppose that $I$ is a two-sided ideal in $R$. Let $r, s \in I$.

Coset addition is well-defined, because $R$ is an abelian group and $I$ is a normal subgroup under addition. I proved that coset addition was well-defined when I constructed quotient groups.

I need to show that coset multiplication is well-defined:

\[(r + I)(s + I) = rs + I.\]

As before, suppose that

\[r + I = r' + I, \quad \text{so} \quad r = r' + a, \quad a \in I\]
\[s + I = s' + I, \quad \text{so} \quad s = s' + b, \quad b \in I\]

Then

\[(r + I)(s + I) = rs + I = (r' + a)(s' + b) + I = r's' + r'b + as' + ab + I = r's' + I = (r' + I)(s' + I).\]

\[(r'b + as' + ab \in I, \text{ because } I \text{ is an ideal; hence } r'b + as' + ab + I = I.) \text{ Therefore, coset multiplication is well-defined.}\]

Verification of the ring axioms is easy but tedious: It reduces to the axioms for $R$.

For instance, suppose I want to verify associativity of multiplication. Take $r, s, t \in R$. Then

\[((r + I)(s + I))(t + I) = (rs + I)(t + I) = (rs)t + I = r(st) + I = (r + I)(st + I) = (r + I)((s + I)(t + I)).\]
(Notice how I used associativity of multiplication in \( R \) in the middle of the proof.) The proofs of the other axioms are similar. \( \square \)

**Definition.** If \( R \) is a ring and \( I \) is a two-sided ideal, the **quotient ring** of \( R \) mod \( I \) is the group of cosets \( \frac{R}{I} \) with the operations of coset addition and coset multiplication.

**Proposition.** Let \( R \) be a ring, and let \( I \) be an ideal

(a) If \( R \) is a commutative ring, so is \( R/I \).

(b) If \( R \) has a multiplicative identity 1, then \( 1 + I \) is a multiplicative identity for \( R/I \). In this case, if \( r \in R \) is a unit, then \( (r + I)^{-1} = r^{-1} + I \).

**Proof.** (a) Let \( r + I, s + I \in R/I \). Since \( R \) is commutative,

\[
(r + I)(s + I) = rs + I = sr + I = (s + I)(r + I).
\]

Therefore, \( R/I \) is commutative.

(b) Suppose \( R \) has a multiplicative identity 1. Let \( r \in R \). Then

\[
(r + I)(1 + I) = r \cdot 1 + I = r + I \quad \text{and} \quad (1 + I)(r + I) = 1 \cdot r + I = r + I.
\]

Therefore, \( 1 + I \) is the identity of \( R/I \).

If \( r \in R \) is a unit, then

\[
(r^{-1} + I)(r + I) = r^{-1}r + I = 1 + I \quad \text{and} \quad (r + I)(r^{-1} + I) = rr^{-1} + I = 1 + I.
\]

Therefore, \( (r + I)^{-1} = r^{-1} + I \). \( \square \)

**Example.** (A quotient ring of the integers) \( 2\mathbb{Z} \), the set of even integers, is an ideal in \( \mathbb{Z} \). Form the quotient ring \( \mathbb{Z}/2\mathbb{Z} \). Here are some cosets:

\[
2 + 2\mathbb{Z}, \quad -15 + 2\mathbb{Z}, \quad 841 + 2\mathbb{Z}.
\]

But two cosets \( a + 2\mathbb{Z} \) and \( b + 2\mathbb{Z} \) are the same exactly when \( a \) and \( b \) differ by an even integer. Every even integer differs from 0 by an even integer. Every odd integer differs from 1 by an even integer. So there are really only two cosets (up to renaming): \( 0 + 2\mathbb{Z} = 2\mathbb{Z} \) and \( 1 + 2\mathbb{Z} \).

Here are the addition and multiplication tables:

\[
\begin{array}{ccc}
+ & 0 + 2\mathbb{Z} & 1 + 2\mathbb{Z} \\
0 + 2\mathbb{Z} & 0 + 2\mathbb{Z} & 1 + 2\mathbb{Z} \\
1 + 2\mathbb{Z} & 1 + 2\mathbb{Z} & 0 + 2\mathbb{Z}
\end{array}
\quad
\begin{array}{ccc}
\times & 0 + 2\mathbb{Z} & 1 + 2\mathbb{Z} \\
0 + 2\mathbb{Z} & 0 + 2\mathbb{Z} & 0 + 2\mathbb{Z} \\
1 + 2\mathbb{Z} & 0 + 2\mathbb{Z} & 1 + 2\mathbb{Z}
\end{array}
\]

You can see that \( \mathbb{Z}/2\mathbb{Z} \) is isomorphic to \( \mathbb{Z}_2 \! \).

In general, \( \mathbb{Z}/n\mathbb{Z} \) is isomorphic to \( \mathbb{Z}_n \). What’s the difference? The difference is that in \( \mathbb{Z}/2\mathbb{Z} \) I write \( 0 + 2\mathbb{Z} \) and \( 1 + 2\mathbb{Z} \); in \( \mathbb{Z}_2 \) I abuse notation and write 0 and 1. The elements of the quotient ring are cosets — remember that each coset is a subset of the original ring! — while the elements of \( \mathbb{Z}_2 \) are “single elements” (though in a sense they also stand for congruence classes). \( \square \)

**Example.** (A quotient ring of a polynomial ring) \( \mathbb{Z}_2[x] \) denotes the ring of polynomials with coefficients in \( \mathbb{Z}_2 \).
The constant polynomials are 0 and 1.
The polynomials of degree 1 are \( x \) and \( x + 1 \).
The polynomials of degree 2 are \( x^2, x^2 + 1, x^2 + x, \) and \( x^2 + x + 1 \).
In general, if \( n \geq 1 \), there are \( 2^n \) polynomials of degree \( n \) in \( \mathbb{Z}_2[x] \).
The set \( \langle x^2 + 1 \rangle \) consists of all multiples of \( x^2 + 1 \) by elements of \( \mathbb{Z}_2[x] \). Here are some elements of \( \langle x^2 + 1 \rangle \):
\[
x \cdot (x^2 + 1) = x^3 + x, \quad (x + 1)(x^2 + 1) = x^3 + x^2 + x + 1, \quad (x^2 + 1)(x^2 + 1) = x^4 + 1.
\]
(In the last case, the middle term is 0 because multiples of 2 are 0 in \( \mathbb{Z}_2 \).
\( \langle x^2 + 1 \rangle \) is an ideal in \( \mathbb{Z}_2[x] \).
\( 0 = 0 \cdot (x^2 + 1) \) is in \( \langle x^2 + 1 \rangle \).
If \( p(x) \cdot (x^2 + 1) \in \langle x^2 + 1 \rangle \), then its additive inverse \(-p(x) \cdot (x^2 + 1)\) is in \( \langle x^2 + 1 \rangle \) as well.
If \( p(x) \cdot (x^2 + 1), q(x) \cdot (x^2 + 1) \in \langle x^2 + 1 \rangle \), then
\[
p(x) \cdot (x^2 + 1) + q(x) \cdot (x^2 + 1) = (p(x) + q(x)) \cdot (x^2 + 1) \in \langle x^2 + 1 \rangle.
\]
Finally, if \( f(x) \in \mathbb{Z}_2[x] \) and \( p(x) \cdot (x^2 + 1) \in \langle x^2 + 1 \rangle \), then
\[
f(x) \cdot p(x) \cdot (x^2 + 1) = (f(x)p(x)) \cdot (x^2 + 1) \in \langle x^2 + 1 \rangle.
\]
Form the quotient ring \( \frac{\mathbb{Z}_2[x]}{\langle x^2 + 1 \rangle} \). Cosets look like \( f(x) + \langle x^2 + 1 \rangle \). Here are some cosets:
\[
0 + \langle x^2 + 1 \rangle = \langle x^2 + 1 \rangle, \quad (0^3 + x^3 + 1) + \langle x^2 + 1 \rangle, \quad (x + 1) + \langle x^2 + 1 \rangle.
\]
You add and multiply cosets by adding and multiplying representatives:
\[
\left[ (x^2 + x + 1) + \langle x^2 + 1 \rangle \right] + \left[ (x^2 + 1) + \langle x^2 + 1 \rangle \right] = x + \langle x^2 + 1 \rangle,
\]
\[
\left[ (x + 1) + \langle x^2 + 1 \rangle \right] \cdot \left[ (x^2 + 1) + \langle x^2 + 1 \rangle \right] = (x^3 + x^2 + x + 1) + \langle x^2 + 1 \rangle.
\]
Remember that multiples of \( x^2 + 1 \) equal 0 in the quotient ring. Thus,
\[
\left[ (x + 1) + \langle x^2 + 1 \rangle \right] \cdot \left[ (x + 1) + \langle x^2 + 1 \rangle \right] = (x^2 + 1) + \langle x^2 + 1 \rangle = \langle x^2 + 1 \rangle.
\]
This shows that \( (x + 1) + \langle x^2 + 1 \rangle \) is a zero divisor in the quotient ring \( \frac{\mathbb{Z}_2[x]}{\langle x^2 + 1 \rangle} \).
Again, since multiples of \( x^2 + 1 \) equal 0 in the quotient ring,
\[
x^2 + (x^2 + 1) = [x^2 + (x^2 + 1)] + \langle x^2 + 1 \rangle = 1 + \langle x^2 + 1 \rangle.
\]
At the moment, this may seem like a lot of meaningless symbol manipulation. However, the same idea is used to construct the complex numbers from the real numbers. \( \square \)

The next result is true for group maps, and I could cite the group map version as a quick proof; however, I’ll write the proof out to remind you of how it goes.

**Lemma.** Let \( \phi : R \to R \) be a ring map. \( \phi \) is injective if and only if \( \ker \phi = \{0\} \).

**Proof.** Suppose \( \phi \) is injective, and let \( r \in \ker \phi \). This means \( \phi(r) = 0 \). But \( \phi(0) = 0 \), so \( r = 0 \) by injectivity. Therefore, \( \ker \phi = \{0\} \).

Conversely, suppose \( \ker \phi = \{0\} \). Suppose \( \phi(a) = \phi(b) \). Then \( 0 = \phi(a) - \phi(b) = \phi(a-b) \), so \( a-b \in \ker \phi \).
But \( \ker \phi = \{0\} \), so \( a-b = 0 \), and hence \( a = b \). This shows \( \phi \) is injective. \( \square \)
Lemma. Let $R$ be a ring, $I$ a two-sided ideal. Define $\pi : R \to R/I$ by $\pi(r) = r + I$. Then $\pi$ is a surjective ring map, and $\ker \pi = I$.

Proof. $\pi$ preserves addition:

$$\pi(r + s) = (r + s) + I = (s + I) + (s + I) = \pi(r) + \pi(s).$$

$\pi$ is also preserves multiplication:

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

Therefore, $\pi$ is a ring map.

If $r + I \in R/I$, then $\pi(r) = r + I$. Hence, $\pi$ is surjective.

Finally, suppose $r \in \ker \pi$. Then $\pi(r) = I \in R/I$ (remember that $I$ is the zero element of $R/I$), i.e. $r + I = I$. By an earlier remarks, $r \in I$. This proves ker $\pi \subset I$.

Conversely, suppose $r \in I$. Then $r + I = I$, so $\pi(r) = I$. This means $r \in \ker \pi$, so $I \subset \ker \pi$. Hence, ker $\pi = I$. $\square$

The map $\pi : R \to \frac{R}{I}$ is called the canonical quotient map, or the canonical projection map.

I showed earlier that the kernel of a ring map is a two-sided ideal. The last lemma shows that every two-sided ideal is the kernel of at least one ring map. It follows that ideals are exactly the subsets of rings which are kernels of ring maps. This is one reason why ideals are so important in ring theory.

The next result is the analog of the Universal Property of the Quotient for groups. I’ll prove it from scratch, even though I could save some writing by citing the result for groups.

Theorem. (Universal Property of the Quotient) Let $\phi : R \to S$ be a ring map, and let $I \subset \ker \phi$. There is a unique ring map $\hat{\phi} : R/I \to S$ such that the following diagram commutes:

$$
\begin{array}{ccc}
R & \xrightarrow{\pi} & \frac{R}{I} \\
\downarrow{\phi} & & \downarrow{\hat{\phi}} \\
S & & \\
\end{array}
$$

To say that the diagram commutes means that if you follow that arrows around the diagram in the two possible ways, you get the same thing.

Proof. Define $\hat{\phi} : R/I \to S$ by

$$\hat{\phi}(r + I) = \phi(r).$$

I first need to show that $\hat{\phi}$ is well-defined (independent of the choice of the coset representative $r$). Suppose $r + I = r' + I$. This means by an earlier remark that $r = r' + a$ for some $a \in I$. Then

$$\hat{\phi}(r + I) = \phi(r) = \phi(r' + a) = \phi(r') + \phi(a) = \phi(r') + 0 = \phi(r') = \hat{\phi}(r' + I).$$

($\phi(a) = 0$ because $a \in I \subset \ker \phi$.) This proves that $\hat{\phi}$ is well-defined.

Note that

$$\hat{\phi} \circ \pi(r) = \hat{\phi}(r + I) = \phi(r).$$

Therefore, $\hat{\phi}$ makes the diagram commute.

Finally, I need to verify that $\hat{\phi}$ is a ring map.

$$\hat{\phi}((r + I) + (r' + I)) = \hat{\phi}(r + r' + I) = \phi(r + r') = \phi(r) + \phi(r') = \hat{\phi}(r + I) + \hat{\phi}(r' + I)$$

$$\hat{\phi}((r + I)(r' + I)) = \hat{\phi}(rr' + I) = \phi(rr') = \phi(r)\phi(r') = \hat{\phi}(r + I)\hat{\phi}(r' + I).
$$
The Universal Property of the Quotient tells you how to construct a ring map that starts in a quotient ring \( R/I \) and ends in some other ring \( S \). It says: First construct a ring map \( \phi : R \to S \) which sends \( I \) to 0 — i.e. such that \( I \subseteq \ker \phi \). The Universal Property then produces a map \( R/I \to S \) automatically.

The point is that it’s usually easy to check that a map \( \phi \) you’re defining sends an ideal \( I \) to 0. It’s messier to verify that a map \( R/I \to S \) is well-defined, in the sense above. The proof of the Universal Property has done the verification of well-definedness once and for all, so you should never have to do it again. The Universal Property is the right way to define a map out of a quotient ring.

As you’d expect, the First Isomorphism Theorem for groups has an analog for rings. I’ll prove this from scratch as well; you might try to write a shorter proof, citing the First Isomorphism Theorem for groups.

**Theorem. (The First Isomorphism Theorem)** Let \( \phi : R \to S \) be a ring map. There is an isomorphism \( \tilde{\phi} : R/(\ker \phi) \to \im \phi \) such that the following diagram commutes:

\[
\begin{array}{ccc}
R & \xrightarrow{\pi} & R/(\ker \phi) \\
\downarrow{\phi} & & \downarrow{\tilde{\phi}} \\
\im \phi & \rightarrow & S
\end{array}
\]

**Proof.** \( \tilde{\phi} \) is produced via the Universal Property of the Quotient, so it is a ring map which makes the diagram commute. I only need to show it’s bijective.

If \( \phi(r) \in \im \phi \), then \( \tilde{\phi}(r + \ker \phi) = \phi(r) \). Hence, \( \tilde{\phi} \) is surjective.

I will show \( \tilde{\phi} \) is injective by showing \( \ker \phi = \{0\} \). Since the zero element of \( R/(\ker \phi) \) is \( \ker \phi \), this amounts to saying that \( \ker \tilde{\phi} = \ker \phi \).

Take \( a + \ker \phi \in \ker \tilde{\phi} \). This means that \( \tilde{\phi}(a + \ker \phi) = 0 \), or \( \phi(a) = 0 \) by definition of \( \tilde{\phi} \). But then \( a \in \ker \phi \), so \( a + \ker \phi = \ker \phi \). Hence, \( \ker \tilde{\phi} = \ker \phi \), \( \tilde{\phi} \) is injective, and therefore \( \tilde{\phi} \) is an isomorphism. \( \square \)

**Example. (Applying the First Isomorphism Theorem)** Consider the ring \( \mathbb{R}[x] \) and the ideal \( \langle x - 1 \rangle \).

There is a ring map \( \phi : \mathbb{R}[x] \to \mathbb{R} \) given by

\[ \phi(f) = f(1). \]

That is, \( \phi \) evaluates the polynomial \( f \) at 1. It is routine to verify that \( \phi \) is a ring map. Moreover, \( \phi(a) = a \) for all \( a \in \mathbb{R} \), so \( \phi \) is surjective.

Obviously \( \langle x - 1 \rangle \subseteq \ker \phi \). Conversely, suppose \( \phi(f) = f(1) = 0 \). Write \( f(x) = \sum_{k=0}^{n} a_k x^k \). Then

\[ 0 = f(i) = \sum_{k=0}^{n} a_k 1^k = \sum_{k=0}^{n} a_k. \]

Therefore, \( a_0 = -\sum_{k=1}^{n} a_k \), and

\[ f(x) = \sum_{k=1}^{n} a_k x^k - \sum_{k=1}^{n} a_k = \sum_{k=1}^{n} a_k (x^k - 1). \]

But \( (x - 1) \mid (x^k - 1) \) for all \( k \geq 1 \), so \( (x - 1) \mid f(x) \). Therefore, \( f \in \langle x - 1 \rangle \), and \( \ker \phi \subseteq \langle x - 1 \rangle \).

Since \( \langle x - 1 \rangle = \ker \phi \), the First Isomorphism Theorem gives

\[ \frac{\mathbb{R}[x]}{\langle x - 1 \rangle} = \frac{\mathbb{R}[x]}{\ker \phi} \approx \im \phi = \mathbb{R}. \]