MA542 Lecture

Timothy Kohl

Boston University

February 18, 2025

Operational Facts About Quotients

If one is trying to work out the structure of a quotient ring R/I, there are a number of (seemingly) low level facts one can use.

- $x + I = y + I$ implies $x + z + I = y + z + I$
- $x + I = 0 + I$ iff $x \in I$
- $(x + I)^n = x^n + I$ for all $n \geq 1$

And we use these, for example, to take a 'complicated' coset and 'replace' it with a simpler coset.

We saw this in the example the other day with $\mathbb{Z}[x]/\langle x\rangle$ where we realized that $f(x) + \langle x\rangle = f(0) + \langle x\rangle$.

Here is an example where we use these techniques to analyze a quotient ring.

Let $R = \mathbb{Z}[i]$ and $I = \langle 2 - i \rangle$.

First, observe that $2 - i + I = 0 + I$ which implies that

$$\begin{gathered} 2 - i + i + I = 0 + i + I \\ \downarrow \\ 2 + I = i + I \end{gathered}$$

This implies, in particular that $a + bi + I$ (a 'typical' coset) can be 'rewritten' as

$$a + bi + I = a + 2b + I$$

where, in particular, $a + 2b$ is simply an integer.

Moreover, we can deduce other conclusions

$$
\begin{array}{c}
2 + I = i + I \\
\downarrow \\
4 + I = -1 + I \text{ since } 2^2 = 4 \text{ and } i^2 = -1 \\
\downarrow \\
4 + 1 + I = -1 + 1 + I \\
\downarrow \\
5 + I = 0 + I
\end{array}
$$

i.e. $5 \equiv 0 (mod\ I)$.

So we have that $(a + bi) + I = (a + 2b) + I$ where $5 + I = 0 + I$, so for example $1 + 2i + I = 0 + I$

Claim: The cosets $\{0 + I, 1 + I, 2 + I, 3 + I, 4 + I\}$ are all distinct in $\mathbb{Z}[i]/I$ and every coset $(a + bi) + I$ is equal to one of these.

PROOF: First, if for integers a, b we have $a + I = b + I$ then $a - b \in I$ so $(a - b) = (x + iy)(2 - i)$.

So $a - b = (2x + y) + (2y - x)i$ which means $2x + y = a - b$ and $2y - x = 0$ so $x = 2y$ and so $2x + y = 5y = a - b$ meaning $5 \mid a - b$ which means $a \equiv b(mod\ 5)$.

But for $a, b \in \{0, 1, 2, 3, 4\}$ this is impossible unless $a = b$.

And since $(a + bi) + I = (a + 2b) + I$ and $5 + I = 0 + I$ then $(a + bi) + I$ equals $r + I$ for exactly one $r \in \{0, 1, 2, 3, 4\}$. $\square$

So we've just shown is that $\mathbb{Z}[i]/\langle 2-i\rangle \cong \mathbb{Z}_5$.

This is interesting and important in that this quotient ring is a field, even though the ring that it's a quotient of, $\mathbb{Z}[i]$, is not a field, but only a domain.

What this comes from is the relationship between the ideal and the ring.

More on this later.

Homomorphisms and Ideals

Before exploring more specific examples of quotient ring structures, we consider a basic source of ideals (and in a sense where *all* ideals arise from) namely ring homomorphisms.

Recall that for rings R, S, a function $\phi : R \to S$ is a *ring homomorphism* if

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$$
$$\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$$

Let's go over some basic properties of homomorphisms.

Proposition

If $\phi : R \to S$ is a ring homomorphism then
(a) $\phi(0_R) = 0_S$
(b) $\phi(-r) = -\phi(r)$
(c) if $R' \subseteq R$ *is a subring then* $\phi(R')$ *is a subring of* S
(d) if S' *is a subring of* S *then* $\phi^{-1}(S') = \{r \in R \mid \phi(r) \in S'\}$ *is a sub-ring of* R
(e) if R *has unity* 1_R *then* $\phi(1_R)$ *is a unity for* $\phi(R)$ *(but not necessarily for* S*).*
(f) if I *is an ideal of* R *then* $\phi(I)$ *is an ideal of* $\phi(R)$
(g) if J *is an ideal of* S *then* $\phi^{-1}(J)$ *is an ideal of* R.

PROOF: We shall discuss the proofs of some of these statements.

PROOF (a): For any $r \in R$, $r + 0_R = r$ of course, so $\phi(r + 0_R) = \phi(r)$ where now $\phi(r + 0_R) = \phi(r) + \phi(0_R)$, which means $\phi(r) = \phi(r) + \phi(0_R)$ so if we subtract $\phi(r)$ from both sides we get $0_S = \phi(0_R)$.

PROOF (c) If $R' \subseteq R$ is a subring then $\phi(R')$ consists of elements of the form $\phi(r)$ for $r \in R$ of course, so we need to apply the subring test to $\phi(R')$. First, we have $\phi(r_1) - \phi(r_2) = \phi(r_1 - r_2) \in \phi(R')$ since $r_1 - r_2 \in R'$ and $\phi(r_1)\phi(r_2) = \phi(r_1 r_2) \in \phi(R')$ since $r_1 r_2 \in R'$ if $r_1, r_2 \in R'$.

PROOF (e) If 1_R is the unity element of R then if $\phi(r) \in \phi(R)$ then $\phi(1_R)\phi(r) = \phi(1_R r) = \phi(r)$ and since *all* elements of $\phi(R)$ are (by definition) of the form $\phi(r)$ for $r \in R$ then $\phi(1_R)$ acts like a unity element for $\phi(R)$.

Is $\phi(1_R) = 1_S$ for the multiplicative identity $1_S \in S$?

Actually no, here is an example, define $\phi : \mathbb{R} \to M_2(\mathbb{R})$ by $x \mapsto \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$, where $1 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ which is not the 2x2 identity matrix.

Part (g) above, implies that $\phi^{-1}(0_S)$ is an ideal of R.

Definition

For a ring homomorphism $\phi : R \to S$, the kernel is
$Ker(\phi) = \{r \in R \mid \phi(r) = 0_S\}$.

The importance of the kernel of a homomorphism is that it quantifies to what degree a homomorphism fails to be one-to-one.

Recall that $\phi : R \to S$ is one-to-one if $\phi(r_1) = \phi(r_2)$ only if $r_1 = r_2$.

This implies that $\phi(r_1) - \phi(r_2) = 0$ only if $r_1 - r_2 = 0$, where we observe that $\phi(r_1) - \phi(r_2) = \phi(r_1 - r_2)$.

Proposition

If $\phi : R \rightarrow S$ is a homomorphism then ϕ is one-to-one if and only if $Ker(\phi) = \{0_R\}$.

Proof.

If ϕ is one-to-one then let $x \in Ker(\phi)$ then $\phi(x) = 0_S$, but we already know that $\phi(0_R) = 0_S$ so by the one-to-one property, it must be that $x = 0_R$.
If $Ker(\phi) = \{0\}$ then suppose $\phi(r_1) = \phi(r_2)$ then $\phi(r_1 - r_2) = \phi(0_R) = 0_S$ which means $r_1 - r_2 \in Ker(\phi) = \{0\}$, but this means $r_1 - r_2 \in Ker(\phi) = \{0_R\}$ so $r_1 = r_2$, i.e. ϕ is one-to-one. $\square$

As observed above, for $\phi : R \rightarrow S$ a ring homomorphism, $Ker(\phi)$ is the inverse image of the zero ideal in S, and is therefore an ideal of R.

So we ask a reasonably natural question, what can we say about $R/Ker(\phi)$?

Theorem (First Isomophism Theorem for Rings)

If $\phi : R \rightarrow S$ is a ring homomorphism then $R/Ker(\phi) \cong \phi(R)$ where $\phi(R) \subseteq S$ is the image of R. □

PROOF:
Given $\phi : R \rightarrow S$, let's define $\Phi : R/Ker(\phi) \rightarrow \phi(R)$ by
$\Phi(x + Ker(\phi)) = \phi(x)$.

Observe first, that if $x + Ker(\phi) = y + Ker(\phi)$ then
$\Phi(x + Ker(\phi)) = \phi(x)$ and $\Phi(y + Ker(\phi)) = \phi(y)$ so we must check that these are equal in order to show that Φ is well defined.

However, this is easy since $\phi(x) = \phi(y)$ iff $\phi(x - y) = 0_S$ which is equivalent to $x - y \in Ker(\phi)$, but this is exactly equivalent to
$x + Ker(\phi) = y + Ker(\phi)$.

Φ is a homomorphism since
$\Phi((r_1 + Ker(\phi)) + (r_2 + Ker(\phi))) = \Phi(r_1 + r_2 + Ker(\phi)) = \phi(r_1 + r_2)$
which is the same as $\Phi(r_1 + Ker(\phi)) + \Phi(r_2 + Ker(\phi))$, and the multiplicative property is proved similarly.

PROOF (continued)
We note that Φ is clearly onto since if $\phi(r) \in \phi(R)$ then $\phi(r) = \Phi(r + Ker(\phi))$. To prove that Φ is one-to-one, let's consider $Ker(\Phi)$.

Note that $x + Ker(\phi) \in Ker(\Phi)$ if $\Phi(x + Ker(\phi)) = \phi(x) = 0$ which is true iff $x \in Ker(\phi)$ and so $Ker(\Phi) = \{0 + Ker(\phi)\}$!

i.e. $Ker(\Phi)$ is trivial, so Φ is one-to-one, and therefore an isomorphism.

As to $\phi(R)$ vs. S, we have the following.

Corollary

If $\phi : R \to S$ is onto, namely $\phi(R) = S$ then $R/Ker(\phi) \cong S$.

Also we note this too.

Corollary

If $\phi : R \to S$ is one-to-one then $R \cong \phi(R)$.

To show this, we note that $Ker(\phi) = \{0\}$ and so $R/Ker(\phi) = R/\{0\}$ and one can show that $R \cong R/\{0\}$ via the function $x \mapsto x + \{0\}$.