MA542 Lecture

Timothy Kohl

Boston University

February 14, 2025

Quotient/Factor Rings

For a ring R with ideal $I \subseteq R$ we considered the cosets $a + I$ for $a \in R$ and observed that, similar to what one sees in group theory, there is an algebraic structure to be placed on the set of cosets.

We are interested in whether the collection of cosets $\{r + I\}$ has the structure of a ring.

We know that, R is an abelian group under addition, and that since $I \subseteq R$ is an ideal it is a subgroup and that it is a normal subgroup of the abelian group $(R, +)$ which means that R/I is well defined as an abelian group.

Theorem

For R a ring with unity and $I \subseteq R$ an ideal, the set of cosets R/I is a ring where $(r+I)+(s+I)=(r+s)+I$ and $(r+I)(s+I)=(rs)+I$. Moreover the additive identity is $0+I$ and R/I has unity element $1+I$ for 1 the unity element of R.

PROOF: Basic group theory gives us part of the structure already in that since I is an ideal, it is automatically a normal subgroup of R with respect to addition (since any subgroup of an abelian group is normal) and so the addition of cosets is well defined.

That is, if $r+I=r'+I$ and $s+I=s'+I$ then
$(r+I)+(s+I)=(r'+I)+(s'+I)$ and that $0+I$ is the additive identity.

What remains to be shown is that R/I has a multiplicative structure as stated.
We shall see that the ideal property of I (and not just that it is a subring) is what makes this work.

PROOF (continued) The definition $(r+I)(s+I) = (rs)+I$ is straightforward, but it is a matter of verifying that the definition does not depend on the choice of coset representative.

So say $r+I = r'+I$ and $s+I = s'+I$ then the question is whether $rs+I = r's'+I$, namely that $rs - r's' \in I$.

Well $r+I = r'+I$, and $s+I = s'+I$ means that $r' = r+a$ and $s' = s+b$ for $a, b \in I$ which means

$$r's' - rs = (r+a)(s+b) - rs = rs + rb + as + ab - rs = rb + as + ab$$

and since $b \in I$, $rb \in I$ and $a \in I$ implies $as \in I$ and certainly $ab \in I$ (think!) and so $rb + as + ab \in I$, namely $rs - r's' \in I$.

PROOF (continued) As to things like the associativity of coset multiplication, and the distributive law holding in R/I, namely that

$$(r+I)[(s+I)+(t+I)] = (r+I)(s+I)+(r+I)(t+I)$$

these are straightforward exercises, as is the proof that $1+I$ is the multiplicative identity of R/I. $\square$

When one is asked to 'determine' the structure of R/I, this starts with the enumeration of the distinct cosets *in* R/I.

One of the key facts to bear in mind is (like one learns in group theory) the cosets in R/I represent a partition of R.

Examples of Quotient Rings

Basic: $R = \mathbb{Z}$, $I = n\mathbb{Z}$ for some $n > 1$.

Since $r + n\mathbb{Z} = s + n\mathbb{Z}$ iff $r - s \in n\mathbb{Z}$ (i.e. $r - s = nk$ for some k) then $r + n\mathbb{Z} = s + n\mathbb{Z}$ iff $r \equiv s (mod\ n)$.

Ergo, the distinct cosets (elements!) of $\mathbb{Z}/n\mathbb{Z}$ are

$$\{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

since for every integer $x \in \mathbb{Z}$

$$x + n\mathbb{Z} = r + n\mathbb{Z}$$

for *exactly one* $r \in \{0, 1, \ldots, n-1\}$ by the division algorithm.

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

Moreover, one can see that

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} = r + n\mathbb{Z}$$

where r is the remainder when $a + b$ is divided by n.

e.g. In $\mathbb{Z}/5\mathbb{Z}$,

$$(3 + 5\mathbb{Z}) + (4 + 5\mathbb{Z}) = 7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}$$

since $7 = 1 \cdot 5 + 2$.

And similarly for multiplication

$$(3 + 5\mathbb{Z})(2 + 5\mathbb{Z}) = 6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}$$

Moreover, it's quite clear that we have an isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ which is given by the function $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ where $\phi(r + n\mathbb{Z}) = r$.

It's easy to verify that this is a homomorphism, and that it is one-to-one and onto. (Exercise.)

Here is a familiar example, whose analysis begins with the enumeration of the *distinct* cosets in R/I.

Here $R = \mathbb{Z}[x]$ and $I = \langle x \rangle$ and we begin by realizing that

$$\begin{aligned} I &= \langle x \rangle \\ &= \{xf(x) \mid f(x) \in R\} \\ &= \{h(x) \in R \mid h(0) = 0\} \\ &= \{c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x \mid c_i \in \mathbb{Z}\} \end{aligned}$$

and it is the last characterization of I that is the key, namely the set of polynomials *whose constant term is* 0.

So what are the distinct cosets in R/I?

Well, $f(x) + I = g(x) + I$ iff $f(x) - g(x) \in I$ which means that for $h(x) = f(x) - g(x)$ one has $h(0) = 0$, but this means the constant term of $f(x) - g(x)$ is zero, which means that if

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

then $f(x) + I = g(x) + I$ iff $a_0 = b_0$.

What this also implies is that if $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ and $g(x) = a_0$ (i.e. a constant polynomial) then

$$f(x) + I = g(x) + I$$

or more succinctly for any polynomial $f(x)$ one has $f(x) + I = f(0) + I$.

Moreover, if one has two constant polynomials 'a' and 'b' then $a + I = b + I$ iff $a - b \in I$ iff $a = b$!

The conclusion is that the distinct cosets in R/I are $\{a + I \mid a \in \mathbb{Z}\}$.

So what is the ring structure of R/I ?

Since the distinct cosets are $\{a + I \mid a \in \mathbb{Z}\}$ then the ring structure is given by

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

where $0 + I$ is the additive identity and $1 + I$ is the multiplicative identity (unity) element.

And so one can define a map $\phi : \mathbb{Z} \to R/I$ given by $\phi(a) = a + I$ which we can verify is not only a homomorphism, but also one-to-one and onto, and thus $R/I \cong \mathbb{Z}$.

One of the ways to 'interpret' the quotient construction is that it 'collapses' or 'condenses' the ring.

In the first example, $\mathbb{Z}/n\mathbb{Z}$ all the elements with the same remainder are aggregated together in the same coset, resulting in a quotient ring which is **finite.**

In contrast, in $\mathbb{Z}[x]/\langle x \rangle$ it's almost as if were making all occurrences of 'x' in a given polynomial equal to zero.

Indeed, this is consistent with our observation that for a polynomial $f(x) \in \mathbb{Z}[x]$ one has that

$$f(x) + \langle x \rangle = f(0) + \langle x \rangle$$

where for $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ one has $f(0) = a_0$ of course.

The other point to note is that $\mathbb{Z}[x]/\langle x \rangle$ is infinite, so that shows that a the quotient of an infinite ring may or may not be infinite.

Note also, that we can repeat the argument we used to deduce the structure of $\mathbb{Z}[x]/\langle x \rangle$ to show that for any commutative ring A, one has that $A[x]$ is a ring, and that $\langle x \rangle \subseteq A[x]$ is an ideal and that

$$A[x]/\langle x \rangle \cong A$$

for the exact same reason, namely that $f(x) + \langle x \rangle = f(0) + \langle x \rangle$.