4-21-2018

Quotient Rings

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 $\dfrac{R}{I}$ 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 $\dfrac{R}{I}$ 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 "$\dfrac{R}{I}$" 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 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

$$\begin{aligned} r+I&=r'+I, \quad \text{so} \quad r=r'+a, \quad a\in I \\ s+I&=s'+I, \quad \text{so} \quad s=s'+b, \quad b\in I \end{aligned}$$

Then

$$(r+I)(s+I)=rs+I=(r'+a)(s'+b)+I=r's'+r'b+as'+ab+I=r's'+I=(r'+I)(s'+I).$$

The next-to-last equality is derived as follows: $r'b+as'+ab\in I$, because I is an ideal; hence $r'b+as'+ab+I=I$. Note that this uses the multiplication axiom for an ideal; in a sense, it explains why the multiplication axiom requires that an ideal be closed under multiplication *by ring elements on the left and right.*

Thus, 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. □

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 $\dfrac{R}{I}$ 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 so is $r + I$, and $(r + I)^{-1} = r^{-1} + I$.

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**) The set of even integers $\langle 2 \rangle = 2\mathbb{Z}$ is an ideal in $\mathbb{Z}$. Form the quotient ring $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

Construct the addition and multiplication tables for the quotient ring.

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:

$+$	$0 + 2\mathbb{Z}$	$1 + 2\mathbb{Z}$
$0 + 2\mathbb{Z}$	$0 + 2\mathbb{Z}$	$1 + 2\mathbb{Z}$
$1 + 2\mathbb{Z}$	$1 + 2\mathbb{Z}$	$0 + 2\mathbb{Z}$

$\times$	$0 + 2\mathbb{Z}$	$1 + 2\mathbb{Z}$
$0 + 2\mathbb{Z}$	$0 + 2\mathbb{Z}$	$0 + 2\mathbb{Z}$
$1 + 2\mathbb{Z}$	$0 + 2\mathbb{Z}$	$1 + 2\mathbb{Z}$

You can see that $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ is isomorphic to $\mathbb{Z}_2$.

In general, $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ is isomorphic to $\mathbb{Z}_n$. I've been using "$\mathbb{Z}_n$" informally to mean the set $\{0, 1, \ldots, n - 1\}$ with addition and multiplication mod n, and taking for granted that the usual ring axioms hold. This example gives a formal contruction of $\mathbb{Z}_n$ as the quotient ring $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. $\square$

Example. $\mathbb{Z}_3[x]$ is the ring of polynomials with coefficients in $\mathbb{Z}_3$. Consider the ideal $\langle 2x^2 + x + 2 \rangle$.

(a) How many elements are in the quotient ring $\dfrac{\mathbb{Z}_3[x]}{\langle 2x^2 + x + 2 \rangle}$?

(b) Reduce the following product in $\dfrac{\mathbb{Z}_3[x]}{\langle 2x^2+x+2\rangle}$ to the form $(ax+b)+\langle 2x^2+x+2\rangle$:

$$(2x+1+\langle 2x^2+x+2\rangle)\cdot(x+1+\langle 2x^2+x+2\rangle).$$

(c) Find $[x+2+\langle 2x^2+x+2\rangle]^{-1}$ in $\dfrac{\mathbb{Z}_3[x]}{\langle 2x^2+x+2\rangle}$.

The ring $\dfrac{\mathbb{Z}_3[x]}{\langle 2x^2+x+2\rangle}$ is analogous to $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{\langle n\rangle}$. In the case of $\mathbb{Z}_n$, you do computations mod n: To "simplify", you divide the result of a computation by the modulus n and take the remainder. In $\dfrac{\mathbb{Z}_3[x]}{\langle 2x^2+x+2\rangle}$, the polynomial $2x^2+x+2$ acts like the "modulus". To do computations in $\dfrac{\mathbb{Z}_3[x]}{\langle 2x^2+x+2\rangle}$, you divide the result of a computation by $2x^2+x+2$ and take the remainder.

(a) By the Division Algorithm, any $f(x)\in\mathbb{Z}_3[x]$ can be written as

$$f(x) = (2x^2+x+2)q(x)+r(x), \quad \text{where} \quad \deg r(x) < \deg(2x^2+x+2).$$

This means that $r(x) = ax+b$, where $a, b\in\mathbb{Z}_3$. Then

$$f(x)+\langle 2x^2+x+2\rangle = [(2x^2+x+2)q(x)+r(x)]+\langle 2x^2+x+2\rangle = (ax+b)+\langle 2x^2+x+2\rangle.$$

Since there are 3 choices for a and 3 choices for b, there are 9 cosets. □

(b) First, multiply the coset representatives:

$$(2x+1)(x+1) = 2x^2+1.$$

Dividing $2x^2+1$ by $2x^2+x+2$, I get

$$2x^2+1 = (2x^2+x+2)(1)+(2x+2).$$

Then

$$2x^2+1+\langle 2x^2+x+2\rangle = [(2x^2+x+2)(1)+(2x+2)]+\langle 2x^2+x+2\rangle = 2x+2+\langle 2x^2+x+2\rangle. \quad \square$$

(c) To find multiplicative inverses in $\mathbb{Z}_n$, you use the Extended Euclidean Algorithm. The same idea works in quotient rings of polynomial rings.

$2x^2+x+2$	-	$2x$
$x+2$	$2x$	1
2	$2x+1$	0

$$(1)(2x^2+x+2)-(2x)(x+2) = 2$$
$$(1)(2x^2+x+2)+(x)(x+2) = 2$$
$$(2)(2x^2+x+2)+(2x)(x+2) = 1$$
$$(2)(2x^2+x+2)+(2x)(x+2)+\langle 2x^2+x+2\rangle = 1+\langle 2x^2+x+2\rangle$$
$$(2x)(x+2)+\langle 2x^2+x+2\rangle = 1+\langle 2x^2+x+2\rangle$$

Thus,

$$[x+2+\langle 2x^2+x+2\rangle]^{-1} = 2x+\langle 2x^2+x+2\rangle. \quad \square$$

Example. (a) List the elements of the cosets of $\langle(2,2)\rangle$ in the ring $\mathbb{Z}_4 \times \mathbb{Z}_6$.

(b) Is the quotient ring $\dfrac{\mathbb{Z}_4 \times \mathbb{Z}_6}{\langle(2,2)\rangle}$ an integral domain?

(a) If x is an element of a ring R, the ideal $\langle x\rangle$ consists of all multiples of x by elements of R. It is not necessarily the same as the additive subgroup generated by x, which is

$$\{\ldots, -3x, -2x, -x, 0, x, 2x, 3x, \ldots\}.$$

In this example, the additive subgroup generated by $(2,2)$ is

$$\{(0,0), (2,2), (0,4), (2,0), (0,2), (2,4)\}.$$

As usual, I get it by starting with the zero element $(0,0)$ and the generator $(2,2)$, then adding $(2,2)$ until I get back to $(0,0)$.

This set is *contained* in the ideal $\langle(2,2)\rangle$; I need to check whether it is *the same* as the ideal.

If $(a,b) \in \mathbb{Z}_4 \times \mathbb{Z}_6$, then

$$(a,b) \cdot (2,2) = (2a, 2b).$$

Thus, an element of the ideal $\langle(2,2)\rangle$ consists of a pair $(2a, 2b)$, where each component is even. There are two even elements in $\mathbb{Z}_4$ (namely 0 and 2) and 3 even elements in $\mathbb{Z}_6$ (namely 0, 2, and 4), so there are $2 \cdot 3 = 6$ such pairs. Thus, the ideal $\langle(2,2)\rangle$ has a maximum of 6 elements. Since the additive subgroup above already has 6 elements, it must be the same as the ideal.

I can list the elements of the cosets of the ideal as I would for subgroups.

$$\begin{aligned}
\langle(2,2)\rangle &= \{(0,0), (2,2), (0,4), (2,0), (0,2), (2,4)\} \\
(0,1) + \langle(2,2)\rangle &= \{(0,1), (2,3), (0,5), (2,1), (0,3), (2,5)\} \\
(1,0) + \langle(2,2)\rangle &= \{(1,0), (3,2), (1,4), (3,0), (1,2), (3,4)\} \\
(1,1) + \langle(2,2)\rangle &= \{(1,1), (3,3), (1,5), (3,1), (1,3), (3,5)\}
\end{aligned} \quad \square$$

(b) Note that

$$[(0,1) + \langle(2,2)\rangle][(1,0) + \langle(2,2)\rangle] = \langle(2,2)\rangle.$$

Hence, $\dfrac{\mathbb{Z}_4 \times \mathbb{Z}_6}{\langle(2,2)\rangle}$ is not an integral domain. $\square$

Example. In the ring $\mathbb{Z}_2 \times \mathbb{Z}_{10}$, consider the principal ideal $\langle(1,5)\rangle$.

(a) List the elements of $\langle(1,5)\rangle$.

(b) List the elements of the cosets of $\langle(1,5)\rangle$.

(c) Is the quotient ring $\dfrac{\mathbb{Z}_2 \times \mathbb{Z}_{10}}{\langle(1,5)\rangle}$ a field?

(a) Note that the additive subgroup generated by $(1,5)$ has only two elements. It's not the same as the ideal generated by $(1,5)$, so I can't find the elements of the ideal by taking additive multiples of $(1,5)$. I'll find the elements of the ideal $\langle(1,5)\rangle$ by multiplying $(1,5)$ by the elements of $\mathbb{Z}_2 \times \mathbb{Z}_{10}$, then throwing out duplicates. The computation is routine, if a bit tedious.

element	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$
$\cdot(1,5)$	$(0,0)$	$(0,5)$	$(0,0)$	$(0,5)$	$(0,0)$

element	$(0,5)$	$(0,6)$	$(0,7)$	$(0,8)$	$(0,9)$
$\cdot(1,5)$	$(0,5)$	$(0,0)$	$(0,5)$	$(0,0)$	$(0,5)$

element	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$
$\cdot(1,5)$	$(1,0)$	$(1,5)$	$(1,0)$	$(1,5)$	$(1,0)$

element	$(1,5)$	$(1,6)$	$(1,7)$	$(1,8)$	$(1,9)$
$\cdot(1,5)$	$(1,5)$	$(1,0)$	$(1,5)$	$(1,0)$	$(1,5)$

Removing duplicates, I have

$$\langle(1,5)\rangle = \{(0,0),(0,5),(1,0),(1,5)\}. \quad \square$$

(b) Since the ideal has 4 elements and the ring has 20, there must be 5 cosets.

$$\begin{aligned} \langle(1,5)\rangle &= \{(0,0),(0,5),(1,0),(1,5)\} \\ (0,1)+\langle(1,5)\rangle &= \{(0,1),(0,6),(1,1),(1,6)\} \\ (0,2)+\langle(1,5)\rangle &= \{(0,2),(0,7),(1,2),(1,7)\} \quad \square \\ (0,3)+\langle(1,5)\rangle &= \{(0,3),(0,8),(1,3),(1,8)\} \\ (0,4)+\langle(1,5)\rangle &= \{(0,4),(0,9),(1,4),(1,9)\} \end{aligned}$$

(c) Note that $(0,1)+\langle(1,5)\rangle$ is the identity.

$$[(0,2)+\langle(1,5)\rangle][(0,3)+\langle(1,5)\rangle] = (0,1)+\langle(1,5)\rangle.$$

$$[(0,4)+\langle(1,5)\rangle][(0,4)+\langle(1,5)\rangle] = (0,1)+\langle(1,5)\rangle.$$

Since every nonzero coset has a multiplicative inverse, the quotient ring is a field. $\square$
