4-12-2020

Quotient Rings of Polynomial Rings

In this section, I'll look at quotient rings of polynomial rings.

Let F be a field, and suppose $p(x) \in F[x]$. $\langle p(x) \rangle$ is the set of all multiples (by polynomials) of $p(x)$, the **(principal) ideal generated by** $p(x)$. When you form the quotient ring $\dfrac{F[x]}{\langle p(x) \rangle}$, it is as if you've set multiples of $p(x)$ equal to 0.

If $a(x) \in F[x]$, then $a(x) + \langle p(x) \rangle$ is the **coset** of $\langle p(x) \rangle$ represented by $a(x)$.

Define $a(x) = b(x) \pmod{p(x)}$ ($a(x)$ is **congruent** to $b(x)$ mod $p(x)$) to mean that

$$p(x) \mid a(x) - b(x).$$

In words, this means that $a(x)$ and $b(x)$ are congruent mod $p(x)$ if they differ by a multiple of $p(x)$. In equation form, this says $a(x) - b(x) = k(x) \cdot p(x)$ for some $k(x) \in F[x]$, or $a(x) = b(x) + k(x) \cdot p(x)$ for some $k(x) \in F[x]$.

Lemma. Let R be a commutative ring, and suppose $a(x), b(x), p(x) \in R[x]$. Then $a(x) = b(x) \pmod{p(x)}$ if and only if $a(x) + \langle p(x) \rangle = b(x) + \langle p(x) \rangle$.

Proof. Suppose $a(x) = b(x) \pmod{p(x)}$. Then $a(x) = b(x) + k(x) \cdot p(x)$ for some $k(x) \in R[x]$. Hence,

$$a(x) + \langle p(x) \rangle = b(x) + k(x) \cdot p(x) + \langle p(x) \rangle = b(x) + \langle p(x) \rangle.$$

Conversely, suppose $a(x) + \langle p(x) \rangle = b(x) + \langle p(x) \rangle$. Then

$$a(x) \in a(x) + \langle p(x) \rangle = b(x) + \langle p(x) \rangle.$$

Hence,

$$a(x) = b(x) + k(x) \cdot p(x) \quad \text{for some} \quad k(x) \in R[x].$$

This means that $a(x) = b(x) \pmod{p(x)}$. $\square$

Depending on the situation, I may write $a(x) = b(x) \pmod{p(x)}$ or $a(x) + \langle p(x) \rangle = b(x) + \langle p(x) \rangle$.

Example. (**A quotient ring of the rational polynomial ring**) Take $p(x) = x - 2$ in $\mathbb{Q}[x]$. Then two polynomials are congruent mod $x - 2$ if they differ by a multiple of $x - 2$.

(a) Show that $2x^2 + 3x + 5 = x^2 + 4x + 7 \pmod{x - 2}$.

(b) Find a rational number r such that $x^3 - 4x^2 + x + 11 = r \pmod{x - 2}$.

(c) Prove that $\dfrac{\mathbb{Q}[x]}{\langle x - 2 \rangle} \approx \mathbb{Q}$.

(a)

$$(2x^2+3x+5)-(x^2+4x+7) = x^2 - x - 2 = (x+1)(x-2), \quad \text{so} \quad 2x^2+3x+5 = x^2+4x+7 \pmod{x-2}. \quad \square$$

(b) By the Remainder Theorem, when $f(x) = x^3 - 4x^2 + x + 11$ is divided by $x - 2$, the remainder is

$$f(2) = 2^3 - 4 \cdot 2^2 + 2 + 11 = 5.$$

Thus,

$$\begin{aligned} x^3 - 4x^2 + x + 11 &= (x-2)q(x) + 5 \\ x^3 - 4x^2 + x + 11 &= 5 \pmod{x-2} \end{aligned} \quad \square$$

(c) I'll use the First Isomorphism Theorem. Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}$ by

$$\phi(f(x)) = f(2).$$

That is, ϕ evaluates a polynomial at $x = 2$. Note that

$$\phi(f(x) + g(x)) = f(2) + g(2) = \phi(f(x)) + \phi(g(x)) \quad \text{and} \quad \phi(f(x)g(x)) = f(2)g(2) = \phi(f(x))\,\phi(g(x)),$$

It follows that ϕ is a ring map.

I claim that $\ker\phi = \langle x - 2\rangle$. Now $f(x) \in \ker\phi$ if and only if

$$f(2) = \phi(f(x)) = 0.$$

That is, $f(x) \in \ker\phi$ if and only if 2 is a root of f. By the Root Theorem, this is equivalent to $x - 2 \mid f(x)$, which is equivalent to $f(x) \in \langle x - 2\rangle$.

Next, I'll show that ϕ is surjective. Let $q \in \mathbb{Q}$. I can think of q as a constant polynomial, and doing so, $\phi(q) = q$. Therefore, ϕ is surjective.

Using these results,

$$\frac{\mathbb{Q}[x]}{\langle x - 2\rangle} = \frac{\mathbb{Q}[x]}{\ker\phi} \approx \operatorname{im}\phi = \mathbb{Q}.$$

The first equality follows from the fact that $\langle x - 2\rangle = \ker\phi$. The isomorphism follows from the First Isomorphism Theorem. The second equality follows from the fact that ϕ is surjective. $\square$

In the last example, $\dfrac{F[x]}{\langle p(x)\rangle}$ was a field. The next result says that this is the case exactly when $p(x)$ is irreducible.

Theorem. $\dfrac{F[x]}{\langle p(x)\rangle}$ is a field if and only if $p(x)$ is irreducible.

Proof. Since $F[x]$ is a commutative ring with identity, so is $\dfrac{F[x]}{\langle p(x)\rangle}$.

Suppose $p(x)$ is irreducible. I need to show that $\dfrac{F[x]}{\langle p(x)\rangle}$ is a field. I need to show that nonzero elements are invertible.

Take a nonzero element of $\dfrac{F[x]}{\langle p(x)\rangle}$ — say $a(x) + \langle p(x)\rangle$, for $a(x) \in F[x]$. What does it mean for $a(x) + \langle p(x)\rangle$ to be nonzero? It means that $a(x) \notin \langle p(x)\rangle$, so $p(x) \nmid a(x)$.

Now what is the greatest common divisor of $a(x)$ and $p(x)$? Well, $(a(x), p(x)) \mid p(x)$, but $p(x)$ is irreducible — its only factors are units and unit multiples of $p(x)$.

Suppose $(a(x), p(x)) = k \cdot p(x)$, where $k \in F$ and $k \neq 0$. Then $k \cdot p(x) \mid a(x)$, i.e. $k \cdot p(x)b(x) = a(x)$ for some $b(x)$. But then $p(x)[k \cdot b(x)] = a(x)$ shows that $p(x) \mid a(x)$, contrary to assumption.

The only other possibility is that $(a(x), p(x)) = k$, where $k \in F$ and $k \neq 0$. So I can find polynomials $m(x)$, $n(x)$, such that

$$a(x)m(x) + p(x)n(x) = k.$$

Then

$$a(x) \cdot \left(\frac{1}{k}m(x)\right) + p(x) \cdot \left(\frac{1}{k}n(x)\right) = 1.$$

Hence,

$$\begin{aligned} a(x) \cdot \left(\frac{1}{k}m(x)\right) + p(x) \cdot \left(\frac{1}{k}n(x)\right) + \langle p(x)\rangle &= 1 + \langle p(x)\rangle \\ a(x) \cdot \left(\frac{1}{k}m(x)\right) + \langle p(x)\rangle &= 1 + \langle p(x)\rangle \\ \left(a(x) + \langle p(x)\rangle\right)\left(\frac{1}{k}m(x) + \langle p(x)\rangle\right) &= 1 + \langle p(x)\rangle \end{aligned}$$

This shows that $\frac{1}{k}m(x) + \langle p(x) \rangle$ is the multiplicative inverse of $a(x) + \langle p(x) \rangle$. Therefore, $a(x) + \langle p(x) \rangle$ is invertible, and $\dfrac{F[x]}{\langle p(x) \rangle}$ is a field.

Going the other way, suppose that $p(x)$ is *not* irreducible. Then I can find polynomials $c(x)$, $d(x)$ such that $p(x) = c(x)d(x)$, where $c(x)$ and $d(x)$ both have smaller degree than $p(x)$.

Because $c(x)$ and $d(x)$ have smaller degree than $p(x)$, they're not divisible by $p(x)$. In particular,

$$c(x) + \langle p(x) \rangle \neq 0 \quad \text{and} \quad d(x) + \langle p(x) \rangle \neq 0.$$

But $p(x) = c(x)d(x)$ gives

$$\begin{aligned} p(x) + \langle p(x) \rangle &= c(x)d(x) + \langle p(x) \rangle \\ 0 &= \left(c(x) + \langle p(x) \rangle\right)\left(d(x) + \langle p(x) \rangle\right) \end{aligned}$$

This shows that $\dfrac{F[x]}{\langle p(x) \rangle}$ has zero divisors. Therefore, it's not an integral domain — and since fields are integral domains, it can't be a field, either. $\square$

Example. (**A quotient ring which is not an integral domain**) Prove that $\dfrac{\mathbb{Q}[x]}{\langle x^2 - 1 \rangle}$ is not an integral domain by exhibiting a pair of zero divisors.

$(x - 1) + \langle x^2 - 1 \rangle$ and $(x + 1) + \langle x^2 - 1 \rangle$ are zero divisors, because

$$(x - 1)(x + 1) = x^2 - 1 = 0 \pmod{x^2 - 1}. \quad \square$$

Example. (**A quotient ring which is a field**) (a) Show that $\dfrac{\mathbb{Q}[x]}{\langle x^2 + 2x + 2 \rangle}$ is a field.

(b) Find the inverse of $(x^3 + 1) + \langle x^2 + 2x + 2 \rangle$ in $\dfrac{\mathbb{Q}[x]}{\langle x^2 + 2x + 2 \rangle}$.

(a) Since $x^2 + 2x + 2 = (x + 1)^2 + 1 > 0$ for all $x \in \mathbb{Q}$, it follows that $x^2 + 2x + 2$ has no rational roots. Hence, it's irreducible, and the quotient ring is a field. $\square$

(b) Apply the Extended Euclidean algorithm to $x^3 + 1$ and $x^2 + 2x + 2$:

$x^3 + 1$	-	$\dfrac{x^2}{2} - \dfrac{5x}{4} + \dfrac{3}{2}$
$x^2 + 2x + 2$	$x - 2$	$\dfrac{x}{2} - \dfrac{1}{4}$
$2x + 5$	$\dfrac{x}{2} - \dfrac{1}{4}$	1
$\dfrac{13}{4}$	$\dfrac{8x}{13} + \dfrac{20}{13}$	0

Therefore,

$$\frac{13}{4} = \left(\frac{x^2}{2} - \frac{5x}{4} + \frac{3}{2}\right)(x^2 + 2x + 2) - \left(\frac{x}{2} - \frac{1}{4}\right)(x^3 + 1).$$

Hence,

$$1 = \frac{4}{13}\left(\frac{x^2}{2} - \frac{5x}{4} + \frac{3}{2}\right)(x^2 + 2x + 2) - \frac{4}{13}\left(\frac{x}{2} - \frac{1}{4}\right)(x^3 + 1).$$

Reducing mod $x^2 + 2x + 2$, I get

$$1 + \langle x^2 + 2x + 2\rangle = -\frac{4}{13}\left(\frac{x}{2} - \frac{1}{4}\right)(x^3 + 1) + \langle x^2 + 2x + 2\rangle$$
$$1 + \langle x^2 + 2x + 2\rangle = \left(-\frac{4}{13}\left(\frac{x}{2} - \frac{1}{4}\right) + \langle x^2 + 2x + 2\rangle\right)\left((x^3 + 1) + \langle x^2 + 2x + 2\rangle\right)$$

Thus, $-\frac{4}{13}\left(\frac{x}{2} - \frac{1}{4}\right) + \langle x^2 + 2x + 2\rangle$ is the inverse of $(x^3 + 1) + \langle x^2 + 2x + 2\rangle$. □

Example. (**A field with 4 elements**) (a) Prove that $\dfrac{\mathbb{Z}_2[x]}{\langle x^2 + x + 1\rangle}$ is a field.

(b) Find $ax + b \in \mathbb{Z}_2[x]$ so that

$$(x^4 + x^3 + 1) + \langle x^2 + x + 1\rangle = (ax + b) + \langle x^2 + x + 1\rangle.$$

(c) Construct addition and multiplication tables for $\dfrac{\mathbb{Z}_2[x]}{\langle x^2 + x + 1\rangle}$.

(a) Let $f(x) = x^2 + x + 1$. Then $f(0) = 1$ and $f(1) = 1$. Since f has no roots in $\mathbb{Z}_2$, it's irreducible. Hence, $\dfrac{\mathbb{Z}_2[x]}{\langle x^2 + x + 1\rangle}$ is a field. □

(b) By the Division Algorithm,

$$x^4 + x^3 + 1 = (x^2 + x + 1)(x^2 + 1) + x.$$

This equation says that $x^4 + x^3 + 1$ and x differ by a multiple of $x^2 + x + 1$, so they represent the same coset mod $x^2 + x + 1$.

Therefore,

$$(x^4 + x^3 + 1) + \langle x^2 + x + 1\rangle = x + \langle x^2 + x + 1\rangle. \quad \square$$

(c) By the Division Algorithm, if $f(x) \in \mathbb{Z}_2[x]$, then

$$f(x) = (x^2 + x + 1)q(x) + (ax + b), \quad \text{where} \quad a, b \in \mathbb{Z}_2.$$

There are two possibilities for a and two for b, a total of 4. It follows that $\dfrac{\mathbb{Z}_2[x]}{\langle x^2 + x + 1\rangle}$ is a field with 4 elements. The elements are

$$0 + \langle x^2 + x + 1\rangle, 1 + \langle x^2 + x + 1\rangle, x + \langle x^2 + x + 1\rangle, (x + 1) + \langle x^2 + x + 1\rangle.$$

Here are the addition and multiplication tables for $\dfrac{\mathbb{Z}_2[x]}{\langle x^2 + x + 1\rangle}$:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

The addition table is fairly easy to understand: For example, $x+(x+1)=1$, because $2x=0 \pmod 2$. For the multiplication table, take $x \cdot x$ as an example. $x \cdot x = x^2$; I apply the Division Algorithm to get

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

So $x \cdot x = x+1 \pmod{x^2+x+1}$.

Alternatively, you can use the fact that in the quotient ring $x^2+x+1=0$ (omitting the coset notation), so $x^2 = x+1$ (remember that $-1 = 1$ in $\mathbb{Z}_s$). $\square$

Remark. In the same way, you can construct a field of order p^n for any prime n and any $n \geq 1$. Just take $\mathbb{Z}_p[x]$ and form the quotient ring $\dfrac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}$, where $f(x)$ is an irreducible polynomial of degree n.

Example. (**Computations in a quotient ring**) (a) Show that $\dfrac{\mathbb{Z}_3[x]}{\langle x^3+2x+1\rangle}$ is a field.

(b) How many elements are there in $\dfrac{\mathbb{Z}_3[x]}{\langle x^3+2x+1\rangle}$?

(c) Compute

$$\left[(x^2+x+2)+\langle x^3+2x+1\rangle\right]\left[(2x^2+1)+\langle x^3+2x+1\rangle\right].$$

Express your answer in the form $(ax^2+bx+c)+\langle x^3+2x+1\rangle$, where $a, b, c \in \mathbb{Z}_3$.

(d) Find $\left[(x^2+1)+\langle x^3+2x+1\rangle\right]^{-1}$.

(a) x^3+2x+1 has no roots in $\mathbb{Z}_3$:

x	0	1	2
$x^3+2x+1 \pmod 3$	1	1	1

Since x^3+2x+1 is a cubic, it follows that it's irreducible. Hence, $\dfrac{\mathbb{Z}_3[x]}{\langle x^3+2x+1\rangle}$ is a field. $\square$

(b) By the Division Algorithm, every element of $\dfrac{\mathbb{Z}_3[x]}{\langle x^3+2x+1\rangle}$ can be written in the form

$$(ax^2+bx+c)+\langle x^3+2x+1\rangle, \quad \text{where} \quad a, b, c \in \mathbb{Z}_3.$$

There are 3 choices each for a, b, and c. Therefore, $\dfrac{\mathbb{Z}_3[x]}{\langle x^3+2x+1\rangle}$ has $3^3 = 27$ elements. $\square$

(c)

$$\left[(x^2+x+2)+\langle x^3+2x+1\rangle\right]\left[(2x^2+1)+\langle x^3+2x+1\rangle\right] = (2x^4+2x^3+2x^2+x+2)+\langle x^3+2x+1\rangle.$$

By the Division Algorithm,

$$2x^4+2x^3+2x^2+x+2 = (2x+2)(x^3+2x+1)+x^2.$$

Therefore,

$$(2x^4 + 2x^3 + 2x^2 + x + 2) + \langle x^3 + 2x + 1\rangle = x^2 + \langle x^3 + 2x + 1\rangle. \quad \square$$

(d) Apply the Extended Euclidean algorithm:

$x^3 + 2x + 1$	-	$x^2 + 2x + 1$
$x^2 + 1$	x	$x + 2$
$x + 1$	$x + 2$	1
2	$2x + 2$	0

$$(x^2 + 2x + 1)(x^2 + 1) - (x + 2)(x^3 + 2x + 1) = 2$$
$$(2x^2 + x + 2)(x^2 + 1) - (2x + 1)(x^3 + 2x + 1) = 1$$

Therefore,

$$\left[(2x^2 + x + 2) + \langle x^3 + 2x + 1\rangle\right]\left[(x^2 + 1) + \langle x^3 + 2x + 1\rangle\right] = 1 + \langle x^3 + 2x + 1\rangle.$$

Hence,

$$\left[(x^2 + 1) + \langle x^3 + 2x + 1\rangle\right]^{-1} = (2x^2 + x + 2) + \langle x^3 + 2x + 1\rangle. \quad \square$$