Class 23

April 18, 2024

Last class we talked about the division theorem. Recall: Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exists unique $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x) g(x) + r(x)$$

and such that $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. We have a few direct consequences of this theorem.

Cor 1

Let F be a field. Then $f(a)$ is the remainder term in

$$\frac{f(x)}{(x-a)}$$

pf

By the division theorem:

$$f(x) = q(x) g(x) + r(x)$$

$$f(x) = q(x)(x-a) + r(x)$$

for some $q(x), r(x)$. Suppose we plug in $x = a$. Then

$$f(a) = q(x)(a-a) + r(a) = r(a)$$

but as $\deg(g(x)) = 1$, then $\deg(r(x)) = 0$ and $r(x) = r(a) = f(a)$.

Cor 2

Let F be a field and $f(x) \in F[x]$. Then a is a zero of $f(x)$ if and only if $(x-a)$ is a factor of $f(x)$.

pf

First, suppose $f(a) = 0$. Then by **Cor 1**,

$$r(x) = f(a) = 0$$

So

$$f(x) = q(x)(x-a) + 0 = q(x)(x-a)$$

Now, suppose $(x-a)$ is a factor of $f(x)$. Then

$$f(x) = q(x)(x-a)$$

so

$$f(a) = q(a)(a-a) = 0$$

Reducibility

Let D be an integral domain. A polynomial $f(x) \in D[x]$ is said to be irreducible over D if $\forall g(x), h(x) \in D[x]$ such that

$$f(x) = g(x) h(x)$$

either $g(x)$ or $h(x)$ is a unit in $D[x]$. If $D[x]$ is not irreducible, it is said to be reducible. In particular, if D is a field, then $\deg(g(x)), \deg(h(x)) < \deg(f(x))$.

Ex 1

Consider the polynomial $f(x) = 2x^2 + 8$ in various integral domains. Let $D_1 = \mathbb{Z}$, $D_2 = \mathbb{Q}$, $D_3 = \mathbb{R}$, $D_4 = \mathbb{C}$. Then

$$f(x) = 2\left(x^2 + 4\right)$$

As 2 is not a unit in D_1, then $f(x)$ is reducible in $\mathbb{Z}[x]$. As 2 is a unit in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, then we cannot make any conclusions about reducibility in these fields. In we allow factoring over complex numbers, then

$$f(x) = 2(x + 2i)(x - 2i)$$

As the unique (up to units) factorization of $f(x)$. As $2i \in \mathbb{C}$, then $f(x)$ is reducible over $\mathbb{C}$, but is irreducible over $\mathbb{Q}, \mathbb{R}$ since there is not a further factorization over the reals or rationals.

Theorem

Let F be a field, and let $f(x) \in F[x]$. If $\deg(f(x)) \geq 2$ and $f(a) = 0$ for some $a \in F$, then $f(x)$ is reducible over F.

pf

By **Cor 2**, $(x - a)$ is a factor of $f(x)$. Thus

$$f(x) = q(x)(x - a)$$

for some $q(x) \in F[x]$. For polynomials of degree 4 or higher, we can find reducible polynomials with no roots in F. For example, consider $\mathbb{R}[x]$. Then

$$f(x) = x^4 + 2x^2 + 1 = \left(x^2 + 1\right)\left(x^2 + 1\right)$$

but the roots of $f(x)$ are $\pm i$, so $f(x)$ has no roots in $\mathbb{C}$.

Ex 2

Determine if $2x^2 + 2$ is reducible over $\mathbb{Z}_5$,$\mathbb{Z}_7$, $\mathbb{Z}_{11}$.

For $\mathbb{Z}_5$,

$$2x^2 + 2 = 0$$

$$2x^2 = 2x^2 + 2 + 3 = 0 + 3 = 3$$

and as $2^{-1} = 3$ when working mod 5, then

$$3 * 2x^2 = x^2 = 3 * 3 = 4$$

and as $2^2 = 4 \pmod 5$, then $2x^2 + 2$ is reducible over $\mathbb{Z}_5$.

For $\mathbb{Z}_7$,

$$2x^2 + 2 = 0$$

$$2x^2 = 2x^2 + 2 + 5 = 0 + 5 = 5$$

and as $2^{-1} = 4$ when working mod 7, then

$$4 * 2x^2 = x^2 = 4 * 5 = 6$$

If we try each number in $\mathbb{Z}_7$, we see

$$0^2 = 0$$

$$1^2 = 1$$

$$2^2 = 4$$

$$3^2 = 2$$

$$4^2 = 2$$

$$5^2 = 4$$

$$6^2 = 1$$

None of them satisfy the equation, so there are no roots for this polynomial in $\mathbb{Z}_7$. As the polynomial is degree 2, then the polynomial cannot be reduced.

For $\mathbb{Z}_{11}$,

$$2x^2 + 2 = 0$$

$$2x^2 = 2x^2 + 2 + 9 = 0 + 9 = 9$$

and as $2^{-1} = 6$ when working mod 11, then

$$6 * 2x^2 = x^2 = 6 * 9 = 3$$

If we try each number in $\mathbb{Z}_{11}$, we see

$$0^2 = 0$$

$$1^2 = 1$$

$$2^2 = 4$$

$$3^2 = 9$$

$$4^2 = 5$$

$$5^2 = 3$$

$$6^2 = 3$$

$$7^2 = 5$$

$$8^2 = 9$$

$$9^2 = 4$$

$$10^2 = 1$$

None of them satisfy the equation, so there are no roots for this polynomial in $\mathbb{Z}_{11}$. As the polynomial is degree 2, then the polynomial cannot be reduced.

Fraction Fields

Recall the definition of the rational numbers. Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then $\frac{a}{b}$ is a rational number. Two rational numbers $\frac{a}{b}, \frac{c}{d}$ are equal if

$$ad = bc$$

We define sums of rational numbers as

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

and products of rational numbers as

$$\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}$$

If we replace $\mathbb{Z}$ with any integral domain, we can get a field.

Def

Let D be an integral domain. Then $\text{Frac}\,(D) = \left\{\frac{a}{b} | a, b \in D, b \neq 0\right\}$ with $\frac{a}{b} = \frac{c}{d}$ if $ad = bc$. This is called the fraction field of D. Let's prove this is a field!

Pf

First, let's show we have closure under addition and multiplication. Let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \text{Frac}\,(D)$. Then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

then $bd \neq 0$, and $ad + bc, bd \in D$, so $\frac{a}{b} + \frac{c}{d} \in \text{Frac}\,(D)$. Similarly for multiplication:

$$\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}$$

and as $bd \neq 0$ and $ac, bd \in D$, then

$$\frac{ac}{bd} \in \text{Frac}\,(D)$$

Now that we now we have closure under multiplication and addition, we can show the field axioms. First, additive identity. Consider $\frac{0}{b} \in \text{Frac}\,(D)$ where $b \neq 0$. Then

$$\frac{0}{b} + \frac{c}{d} = \frac{0d + bc}{bd} = \frac{bc}{bd} = \frac{c}{d}$$

as $bdc = bdc$ (This is the reduction rule. We will assume this for the rest of the proof). In particular, note b is arbitrary as

$$\frac{0}{b} = \frac{0}{c} = 0$$

since

$$0b = 0 = 0c$$

For the additive inverse:

$$-\left(\frac{a}{b}\right) = \frac{-a}{b}$$

as

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab - ab}{b^2} = \frac{0}{b^2} = 0$$

Now for associativity of addition:

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \left(\frac{cf + de}{df}\right) = \frac{adf + bcf + bde}{bdf} = \left(\frac{ad + bc}{bd}\right) + \frac{e}{f} = \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f}$$

And for commutativity of addition:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{cb+da}{db}=\frac{c}{d}+\frac{a}{b}$$

Associativity of multiplication:

$$\left(\frac{a}{b}*\frac{c}{d}\right)*\frac{e}{f}=\left(\frac{ac}{bd}\right)*\frac{e}{f}=\frac{ace}{bdf}=\frac{a}{b}*\left(\frac{ce}{df}\right)=\frac{a}{b}*\left(\frac{c}{d}*\frac{e}{f}\right)$$

Distributive laws:

Note, if the left distributive law is shown and $\mathrm{Frac}(D)$ is commutative, then we do not need to show the right distributive law.

$$\frac{a}{b}*\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}*\left(\frac{cf+de}{df}\right)=\frac{acf+ade}{bdf}$$

As

$$\frac{a+b}{c}=\frac{(a+b)\,c}{c^2}=\frac{ac+bc}{c^2}=\frac{a}{c}+\frac{b}{c}$$

then we can split up the fraction at the numerator as

$$\frac{acf+ade}{bdf}=\frac{acf}{bdf}+\frac{ade}{bdf}=\frac{ac}{bd}+\frac{ae}{bf}=\frac{a}{b}*\frac{c}{d}+\frac{a}{b}*\frac{e}{f}$$

For commutativity under multiplication:

$$\frac{a}{b}*\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}*\frac{a}{b}$$

Unity:

$$\frac{1}{1}\in\mathrm{Frac}(D)$$

and

$$\frac{1}{1}*\frac{a}{b}=\frac{1a}{1b}=\frac{a}{b}$$

Units:

Suppose $\frac{a}{b}\neq 0$. Then $a,b\neq 0$, thus $\frac{b}{a}\in\mathrm{Frac}(D)$ and

$$\frac{a}{b}*\frac{b}{a}=\frac{ab}{ba}=\frac{1}{1}$$

as

$$ab1=ab=ba=1ba$$

and thus, $\mathrm{Frac}(D)$ is a field.

Properties

In particular, if $D=F[x]$ for some field, we can get rational expressions of polynomials. This is why our cancellation laws work when working with rational expressions of polynomials. We have a few nice properties of rational expressions. Let $\frac{a}{b},\frac{c}{d}\in\mathrm{Frac}(D)$. Then

1. $\frac{a}{1}*\frac{c}{d}=\frac{ac}{d}$
2. $\left(\left(\frac{a}{b}\right)^{-1}\right)^{-1}=\frac{a}{b}$
3. If F is a field, $\mathrm{Frac}(F)\approx F$
4. The relation $\frac{a}{b}=\frac{c}{d}$ if $ad=bc$ is an equivalence relation.
5. D is isomorphic to a subring of $\mathrm{Frac}(D)$
6. $\mathrm{Frac}(\mathbb{Z}[i])\approx\mathbb{Q}[i]$
7. $\mathrm{Frac}(\mathbb{Z}[x])\approx\mathbb{Q}[x]$

These are given without proof. Try proving them for practice!