Math 320 Lecture
March 26, 2020

Divisibility in Polynomial Rings

For this lecture, F will denote a field.

Last time: Let $a(x), b(x) \in F[x]$, and $b(x) \neq 0_F$. We say $b(x)$ divides $a(x)$, denoted $b(x) \mid a(x)$, if $\exists$ an $h(x) \in F[x]$ such that $a(x) = b(x)h(x)$

Also: the gcd of $a(x), b(x) \in F[x]$ is the polynomial $d(x) \in F[x]$ s.t.

(1) $d(x) \mid a(x)$ and $d(x) \mid b(x)$.

(2) if $c(x) \mid a(x)$ and $c(x) \mid b(x)$, then $\deg c(x) \leq \deg d(x)$

(recall: degree in $F[x]$ is analogous to order in $\mathbb{Z}$)

(3) $d(x)$ is monic

where monic means that the leading coefficient is 1 $_f$.

Examples:

(1) Consider $x^2-1 \in \mathbb{Q}[x]$.

what are the divisors of x^2-1 in $\mathbb{Q}[x]$?

$x-1$ and $x+1$ (these are both monic)

However, these aren't the only divisors

$2x-2 \mid x^2-1$, since

$$x^2-1 = (2x-2)\left(\tfrac{1}{2}x+\tfrac{1}{2}\right)$$

Also, $\frac{1}{3}x+\frac{1}{3} \mid x^2-1$ since

$$x^2-1 = \left(\tfrac{1}{3}x+\tfrac{1}{3}\right)(3x-3)$$

This shows that x^2-1 has infinitely many divisors.

However, note that they're just constant multiples of $x-1$, $x+1$,

i.e. they're of the form

$c(x-1)$ or $c(x+1)$, where $c \in \mathbb{Q}$.

So, it suffices to just mention the monic divisors, which here are $1, x-1, x+1$. (1 is always a divisor)

(2) What is the gcd of x^2-1 and x^3-1?

The (monic) divisors of x^2-1 are

$1, (x-1), x+1$

The monic divisors of x^3-1 are

$1, (x-1), x^2+x+1$

The common divisors are

$1, x-1$.

$x-1$ is the highest-degree common divisor, so

$$\boxed{(x^2-1, x^3-1) = x-1.}$$

(3) Find $(\underbrace{4x^2-16}_{f(x)}, \underbrace{8x^3-12x^2+6x-1}_{g(x)})$

Notice, $f(x) = 4(x-2)(x+2)$

$g(x) = (2x-1)^3 = 8(x-\frac{1}{2})^3$

The monic divisors of $f(x)$ are:

(1) $x-2$, $x+2$

The monic divisors of $g(x)$ are

(1) $x-\frac{1}{2}$

$\Rightarrow (f(x), g(x)) = 1$, i.e. they're relatively prime.

Thm 4.8 Just like in $\mathbb{Z}$, we can write the gcd $d(x)$ of $a(x)$ and $b(x)$ as a linear combo of $a(x)$ and $b(x)$.

That is, $\exists\ u(x), v(x) \in F[x]$ s.t.

$d(x) = a(x)u(x) + b(x)v(x)$.

Cor 4.9: $a(x), b(x) \in F[x]$, not both zero. Then, $d(x) \in F[x]$ is their gcd iff

(1) $d(x) \mid a(x)$ and $d(x) \mid b(x)$

(2) If $c(x) \mid a(x)$ and $c(x) \mid b(x)$, then $c(x) \mid d(x)$.

(This is pretty much exacty Cor 1.3)

Pf (the same as for Cor 1.3)

"$\Rightarrow$" if $d(x)$ is gcd, then $d(x)$ satisfies (1) and (2).

If $d(x)$ is the gcd, then it of course satisfies (1)

Now, suppose $c(x) \mid a(x)$ and $c(x) \mid b(x)$.

Want to show: $c(x) \mid d(x)$.

To do this, use a linear combo:

$\exists\ u(x), v(x)$ s.t.

$$d(x) = a(x)u(x) + b(x)v(x)$$

Since $c(x)$ is a common divisor of $a(x), b(x)$, $\exists\ q(x), k(x) \in F[x]$ s.t.

$$a(x) = q(x)c(x), \quad b(x) = k(x)c(x).$$

Just substitute:

$$d(x) = (q(x)c(x))u(x) + (k(x)c(x))v(x)$$
$$= c(x)(q(x)u(x) + k(x)v(x)) \checkmark$$
$$\Rightarrow c(x) \mid d(x)$$

"$\Leftarrow$" If $d(x)$ satisfies (1) and (2), then $d(x) = (a(x), b(x))$

By (1), we know that $d(x) \mid a(x)$ and $d(x) \mid b(x)$.

Next, suppose $c(x) \mid a(x)$ and $c(x) \mid b(x)$.

By def. of gcd, we want to show that $\deg c(x) \leq \deg d(x)$.

By (2), we know that $c(x) \mid d(x)$ so $d(x) = c(x)p(x)$ f.s. $p(x) \in F[x]$.

Then, we can use Thm 4.2:

$$\deg c(x) \le \deg c(x) + \deg p(x) = \deg [c(x)\, p(x)]$$
$$= \deg d(x) \quad \blacksquare$$

Recall Thm 1.4: Let $a, b, c \in \mathbb{Z}$.
If $a \mid bc$ and $(a,b) = 1$, then $a \mid c$.

Thm 4.10 (very similar to 1.4): Let
$a(x), b(x), c(x) \in F[x]$. If $a(x) \mid b(x)c(x)$
and $(a(x), b(x)) = 1_F$, then
$a(x) \mid c(x)$.

Pf: Again, this will be nearly identical to the integer version.

Since $(a(x), b(x)) = 1_F$, $\exists\ u(x), v(x) \in F[x]$
s.t.
$$a(x)u(x) + b(x)v(x) = 1_F.$$

Multiply both sides by $c(x)$:

$$c(x)a(x)u(x) + b(x)c(x)v(x) = c(x).$$

Since $a(x) \mid b(x)c(x)$, $\exists\ q(x) \in F[x]$ s.t.

$$b(x)c(x) = a(x)q(x).$$

Substitute:

$$a(x)(c(x)u(x)) + a(x)q(x)v(x) = c(x)$$

$$\Rightarrow \quad a(x)\big(c(x)u(x) + q(x)v(x)\big) = c(x)$$

$$\Rightarrow \quad a(x) \mid c(x). \quad \blacksquare$$

Side note: There's a Euclidean Algorithm for polynomials, that's pretty much the same as for integers. (see Exercises 5 and 6 in 4.2)

Section 4.3 Irreducibles and Unique Factorization

Regarding divisibility, $\mathbb{Z}$ and $F[x]$ have a lot in common

Correspondence:

$\mathbb{Z}$		$F[x]$
order	$\longleftrightarrow$	degree
primes	$\longleftrightarrow$	irreducibles

We'll discuss irreducible polynomials, which take the place of prime integers.

Associates:

Def: Let R be a commutative ring w/ identity, and let $a, b \in R$.

We say that a is an <u>associate</u> of b if there exists a unit $u \in R$ such that

$$a = bu.$$

Here, b is also an associate of a, since

$$b = au^{-1}.$$

Back to polynomials: Recall, the units of $F[x]$ are just the nonzero constants. So, this means that $f(x) \in F[x]$ is an associate of $g(x) \in F[x]$ iff $f(x) = cg(x)$ for some constant $c \in F$

Ex: (1) in $\mathbb{Q}[x]$, $x-3$ is an associate of $4x-12$.

(2) in $\mathbb{C}[x]$, $x-i$ is an associate of $ix+1$ (so sometimes associates are not obvious)

If $f(x)$ and $g(x)$ are associates we can think of them as "basically the same" when it comes to factorization.

Irreducibility:

Def: A <u>nonconstant</u> poly $p(x) \in F[x]$ is said to be <u>irreducible</u> if its only divisors are its associates and the nonzero constants.

A nonconstant polynomial that is not irreducible is called <u>reducible</u>.

That is, if $p(x)$ is irreducible, then all of its divisors are

of the form:

c, or $cp(x)$, where $c \in F$.

(c: constants; $cp(x)$: associate)

If we don't look at multiplying by constants, then the "only" divisors of $p(x)$ are 1_F and itself.

very similar to the definition of a prime integer.

Examples:

(1) every degree-1 polynomial in $F[x]$ is irreducible.

A degree-1 poly is of the form $ax+b$, where $a, b \in F$.

The only divisors of $ax+b$ can be constants or of the form $c(ax+b)$, where $c \in F$.

(2) $x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$

(3) Let's look at $x^2 + 1$.

Notice that the coefficient field is important!

In $\mathbb{R}[x]$ and $\mathbb{Q}[x]$, $x^2 + 1$ is irreducible

But, in $\mathbb{C}[x]$, $x^2 + 1 = (x - i)(x + i)$

$x - i$ is neither a constant nor an associate of $x^2 + 1$, so $x^2 + 1$ is reducible in $\mathbb{C}[x]$

↑ important to note the ring

Thm 4.11: A nonzero poly $f(x) \in F[x]$ is reducible in $F[x]$ iff $f(x)$ can be written as a product of two nonconstant polys of lower degree.

Pf: "$\Rightarrow$" Assume that $f(x)$ is reducible. Then, it has a divisor $g(x)$ that is neither constant nor an associate.

So, $f(x) = g(x) \cdot h(x)$ f.s. $h(x) \in F[x]$.

By Thm 4.2

$$\deg f(x) = \deg g(x) + \deg h(x).$$

If $\deg h(x) = 0$, then it's constant. But, if $h(x)$ is constant, then $g(x)$ would be an associate. So this can't happen.

$\Rightarrow$ $g(x)$, $h(x)$ are nonconstant, so

$$\deg g(x), \deg h(x) \geq 1.$$

$\Rightarrow 0 < \deg g(x) < \deg g(x) + \deg h(x) = \deg f(x)$

Similarly, $\deg h(x) < \deg f(x)$.

"$\Leftarrow$" Suppose $f(x) = g(x)h(x)$, where $g(x)$, $h(x)$ are nonconstant and lower degree than $f(x)$.

If they're both nonconstant, then they both cannot be associates.

If, say $g(x)$ were an associate of $f(x)$, then $f(x) = c\,g(x)$ f.s. $c \in F$. But then

$$c\,g(x) = h(x)\,g(x)$$
$$c = h(x)$$
$\Rightarrow h(x)$ constant $\times$ contradiction

So, $f(x)$ is reducible. ∎