Math 320 Lecture
March 24, 2020

Last time: introduced polynomial rings

Let R be a ring,

$R[x]$ = ring of polynomials with coefficients in R

$$= \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : a_i \in R, n \geq 0\}$$

$R[x]$ has usual polynomial addition and mult.

- If R is commutative, then so is $R[x]$
- the zero element of $R[x]$ is 0_R
- the elements of R form a subring of $R[x]$; call them the

constant polynomials

- If R has identity, then so does $R[x]$, and $1_{R[x]} = 1_R$

- the degree of a polynomial is that largest exponent that appears

- finished with a theorem:

If R is an integral domain and $f(x), g(x)$ are nonzero polynomials in $R[x]$, then

$$\deg[f(x)g(x)] = \deg f(x) + \deg g(x)$$

- Note: the constant polys have degree 0, and 0_R does not have a degree.

Why? If we give 0_R a degree, it will break the above theorem:

Ex: In $\mathbb{Z}[x]$, $\deg(x+1) = 1$

By the Thm (4.2), if $\deg 0 = 0$, then,

$$0 = \deg 0 = \deg(0 \cdot (x+1))$$
$$= \deg 0 + \deg(x+1)$$
$$= 0 + 1 = 1$$
$$\Rightarrow 0 = 1 \quad \text{X}$$

Cor 4.3: If R is an integral domain, then so is $R[x]$.

Pf: Let $f(x), g(x) \in R[x]$ and nonzero. Then, $\deg f(x), \deg g(x) \geq 0$.

By Thm 4.2,

$$\deg f(x)g(x) = \deg f(x) + \deg g(x)$$
$$\geq 0 + 0$$
$$\geq 0.$$

$\Rightarrow$ $f(x), g(x)$ are at least nonzero constants, i.e. they're

nonzero. □

Cor 4.4: In general, in $R[x]$,

$$\deg f(x)g(x) \leq \deg f(x) + \deg g(x)$$

This is true even when R is not an integral domain.

Ex: (1) in $\mathbb{Z}_4[x]$,

$$(2x^2)(2x^3) = 4x^5 = 0 \cdot x^5 = 0.$$

This shows that $\mathbb{Z}_4[x]$ is not an integral domain.

(2) in $\mathbb{Z}_4[x]$,

$$\underbrace{(2x^2+1)}_{\deg 2}\underbrace{(2x^3)}_{\deg 3} = \underbrace{2x^3}_{\deg 3}$$

$$3 \leq 2+3 = 5 \quad \checkmark$$

Satisfies Cor 4.4.

Cor 4.5: Let R be an integral domain and $f(x) \in R[x]$. Then, $f(x)$ is a unit iff $f(x)$ is a constant that is a unit in R.

i.e. the units of $R[x]$ are the units of R.

Pf:

"$\Leftarrow$" if $f(x)$ is a constant and a unit in R, then it's a unit in $R[x]$.

Here, $f(x) = u \in R$ where u is a unit. So, $\exists\, u^{-1} \in R$ s.t. $u \cdot u^{-1} = 1_R$.

But, $R \subset R[x]$, so $u, u^{-1} \in R[x]$ so they're units in $R[x]$ as well.

"$\Rightarrow$" If $f(x)$ is a unit in $R[x]$, then it's constant and a unit in R.

Suppose $f(x)$ has inverse $g(x)$ in $R[x]$, i.e. $f(x) \cdot g(x) = 1_R$.

Then, by Theorem 4.2,

$$0 = \deg 1_R = \deg[f(x) \cdot g(x)]$$
$$= \deg f(x) + \deg g(x)$$

degrees are nonnegative, so this implies that

$$\deg f(x) = \deg g(x) = 0$$

$\Rightarrow$ $f(x)$, $g(x)$ are units

$\Rightarrow$ $f(x) = a$, $g(x) = b$ where $a, b \in R$, and $ab = 1_R$, so a is a unit. $\square$

Remark: If F is a field, then the units of $F[x]$ are the nonzero elements of F.

When R is not an integral domain, we may have units that are non-constant.

Ex: $1+3x$ in $\mathbb{Z}_9[x]$ is a unit.

use the fact that $9=0$ in $\mathbb{Z}_9$:

$$(1+3x)(1-3x) = 1-9x^2$$
$$= 1+0x^2$$
$$= 1 \checkmark$$

$\Rightarrow 1+3x$ is a unit, and

$$(1+3x)^{-1} = 1-3x = 1+6x.$$

Division Algorithm for Polynomials:

Thm 4.6: Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0_F$.

Then, there exist <u>unique</u> polys $q(x), r(x) \in F[x]$ with

$$f(x) = g(x)q(x) + r(x), \text{ and}$$

$r(x) = 0_R$ OR $\deg r(x) < \deg g(x)$.

This is similar to the Division Algorithm for integers: $\forall a, b \in \mathbb{Z}$ w/ $b \neq 0$, $\exists$ unique $q, r \in \mathbb{Z}$ s.t. $a = bq + r$, $0 \leq r < b$.

In the polynomial version, degree takes the place of order.

To find $q(x)$ and $r(x)$, need polynomial long division.

Examples:

(1) find $q(x)$, $r(x)$ as in the Division Algorithm when dividing $x^4 - 7x + 1$ by $2x^2 + 1$ in $\mathbb{Q}[x]$.

note: $q(x)$ is called the quotient and $r(x)$ the remainder

$\frac{1}{2}x^2 - \frac{1}{4}$ ← $q(x)$

$2x^2+1 \;\big|\; x^4 + 0x^3 + 0x^2 - 7x + 1$

$-\left(x^4 \qquad + \frac{1}{2}x^2\right)$

$-\frac{1}{2}x^2 + 7x + 1$

$-\left(-\frac{1}{2}x^2 \qquad - \frac{1}{4}\right)$

$7x + \frac{5}{4}$ ← $r(x)$

$$\Rightarrow \underbrace{x^4 - 7x + 1}_{f(x)} = \underbrace{(2x^2+1)}_{g(x)}\underbrace{\left(\frac{1}{2}x^2 - \frac{1}{4}\right)}_{q(x)} + \underbrace{\left(7x + \frac{5}{4}\right)}_{r(x)}$$

Notice: • $\deg q(x) = \deg\left(\frac{1}{2}x^2 - \frac{1}{4}\right) = 2$

• $\deg r(x) = \deg\left(7x + \frac{5}{4}\right) = 1$ ✓

(2) Same thing, but divide $2x^4 + x^2 - x + 1$ by $2x - 1$ in $\mathbb{Z}_5[x]$.

$$
\begin{array}{r}
x^3 + 3x^2 + 2x + 3 \quad \leftarrow q(x) \\
2x-1 \;\overline{)\; 2x^4 + 0x^3 + x^2 - x + 1} \\
-(2x^4 - x^3) \\
\hline
x^3 + x^2 - x + 1 \\
-(x^3 - 3x^2) \\
\hline
4x^2 - x + 1 \\
-(4x^2 - 2x) \\
\hline
x + 1 \\
-(x - 3) \\
\hline
4 \quad r(x)
\end{array}
$$

$$
\Rightarrow \underbrace{2x^4 + x^2 - x + 1}_{f(x)} = \underbrace{(2x-1)}_{g(x)}\underbrace{(x^3 + 3x^2 + 2x + 3)}_{q(x)} + \underbrace{4}_{r(x)}
$$

Here, $\deg q(x) = 3$, $\deg r(x) = 0$. ✓

Section 4.2: Divisibility in $F[x]$.

Note: Throughout this section, F will be a field.

Def: Let F be a field, $a(x), b(x) \in F[x]$, with $b(x)$ nonzero. We say that $b(x)$ <u>divides</u> $a(x)$, and write $b(x) \mid a(x)$ if there exists $h(x) \in F[x]$ such that

$$a(x) = b(x) \cdot h(x).$$

Very similar to divisibility in $\mathbb{Z}$.

Examples: (1) $x-1$ divides x^2-1 in $\mathbb{Z}[x]$, since

$$\underbrace{x^2-1}_{a(x)} = \underbrace{(x-1)}_{b(x)} \cdot \underbrace{(x+1)}_{h(x)}$$

note: $b(x) \mid a(x)$ when the

remainder when dividing $b(x)$ by $a(x)$ is 0_F.

(2) In $\mathbb{Q}[x]$, consider $x^3 - 3x + 1$.

Every element of $\mathbb{Q}$ divides $x^3 - 3x + 1$.

$$x^3 - 3x + 1 = \left(\frac{1}{7}\right)\left(7x^3 - 3x + 1\right)$$

$$\left(x^3 - 3x + 1\right) = \left(\frac{2}{5}\right)\left(\frac{5}{2}x^3 - \frac{15}{2}x + \frac{5}{2}\right)$$

In general, every nonzero element of F divides $f(x) \in F[x]$, because if $c \in F$, then

$$\underbrace{f(x)}_{a(x)} = \underbrace{(c)}_{b(x)}\underbrace{\left(c^{-1}f(x)\right)}_{h(x)}$$

i.e. you can always divide by constants.

Thm 4.7: Let F be a field, and $a(x), b(x) \in F[x]$, w/ $b(x) \neq 0_F$.

(1) If $b(x) \mid a(x)$, then $cb(x) \mid a(x)$ for all nonzero $c \in F$.

(2) Every divisor of $a(x)$ has degree $\leq \deg a(x)$ ☆

(2) is similar to the case in $\mathbb{Z}$, where if $b \mid a$ in $\mathbb{Z}$, then $-a \leq b \leq a$.

Pf: (1) If $b(x) \mid a(x)$, then $a(x) = b(x)h(x)$ f.s. $h(x) \in F[x]$. Then

$$a(x) = b(x)h(x) = (c \cdot c^{-1})\, b(x)\, h(x)$$
$$= (cb(x))(c^{-1}h(x))$$

$\Rightarrow cb(x) \mid a(x)$.

(2) F is a field, so F is an integral domain. So, we can use Thm 4.2 from last section.

Again, if $b(x) | a(x)$, then $a(x) = b(x)h(x)$ f.s. $h(x) \in F[x]$. Then by Thm 4.2,

$$\deg a(x) = \deg [b(x)h(x)]$$

$$\deg a(x) = \underline{\deg b(x)} + \underline{\deg h(x)}$$

degrees are nonnegative, so

$$\deg b(x) \leq \deg b(x) + \deg h(x) = \deg a(x)$$

$$\Rightarrow \boxed{\deg b(x) \leq \deg a(x)}$$ ∎

Exercise from the book (4.2.4):

Let $f(x), g(x) \in F[x]$. If $f(x) | g(x)$ and $g(x) | f(x)$, show that $f(x) = c \cdot g(x)$ for some nonzero $c \in F$.

Pf: If $f(x) \mid g(x)$, then $g(x) = h(x) \cdot f(x)$ f.s. $h(x) \in F[x]$. If $g(x) \mid f(x)$, then $f(x) = k(x)\, g(x)$, f.s. $k(x) \in F[x]$. Then,

$$f(x) = k(x)\, g(x) = (k(x)\, h(x)) f(x)$$

$$f(x) = \underbrace{(k(x)\, h(x))}\, f(x)$$

want to show this is constant

we know $F[x]$ is an integral domain, so we may cancel the $f(x)$'s to get

$$1_F = k(x)\, h(x)$$

$\Rightarrow k(x)$ is constant ✓

Alternatively, use thm 4.2:

$$\deg f(x) = \deg(k(x) h(x) f(x))$$

$$\deg f(x) = \deg(k(x) \cdot h(x)) + \deg f(x)$$

$$0 = \deg k(x) + \deg h(x)$$

$\Rightarrow \deg k(x) = 0 \Rightarrow k(x)$ is a

constant $c \in F$

$\Rightarrow f(x) = k(x)g(x) = c \cdot g(x)$.

furthermore, $h(x) = c^{-1}$, since

$k(x) \cdot h(x) = 1_F$.

Def: The <u>leading coefficient</u> of a polynomial is the coefficient of its highest-degree term.

Ex: leading coefficient of $3x^3 - 4x + 2$ is 3.

· We say a polynomial in $F[x]$ is monic if its leading coefficient is 1_F.

Greatest Common Divisors:

Def: $a(x), b(x) \in F[x]$, not both zero. The <u>greatest common divisor</u> of $a(x)$ and $b(x)$, denoted $(a(x), b(x))$,

is the monic polynomial of highest degree that divides both $a(x)$ and $b(x)$.

So, $d(x)$ is the gcd of $a(x)$ and $b(x)$ if

(1) $d(x)$ is monic

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

(3) If $c(x) \mid a(x)$ and $c(x) \mid b(x)$, then $\deg c(x) \leq \deg d(x)$.

Note: 1_F is monic and divides every polynomial, so $a(x)$ and $b(x)$ have at least one common monic divisor

We say two polynomials $a(x)$ and $b(x)$ in $F[x]$ are <u>relatively prime</u> if their gcd is 1_F.

Remark: to show $d(x)$ and $b(x)$ are relatively prime, you just need to show that the only common divisors are constants.

Thm 4.8: $a(x), b(x) \in F[x]$, not both zero. Then, there exists a unique gcd $d(x)$ of $a(x)$ and $b(x)$

Furthermore, there exist (not necessarily unique) $u(x)$ and $v(x)$ s.t.

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