Math 320 April 7, 2020

Last time: irreducibility of polynomials

Recall: Let $f(x), g(x) \in F[x]$

(F will always denote a field)

We say $f(x)$ is an <u>associate</u> of $g(x)$ if $f(x) = c \cdot g(x)$ for some constant $c \in F$. $(c \neq 0_F)$

Note: this also implies $g(x)$ is an associate of $f(x)$, since

$$g(x) = c^{-1} f(x).$$

Ex: (1) $x^2 - 1$ and $3x^2 - 3$ are associates in $\mathbb{Q}[x]$ since

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

(2) $ix + 1$ and $x - i$ are associates in $\mathbb{C}[x]$, since $ix + 1 = i(x - i)$

(3) $(2-i)x + 5$ and $x + (2+i)$ are associates in $\mathbb{C}[x]$, since

$$(2-i)x + 5 = (2-i)(x + (2+i))$$

Defined irreducible polynomials:
We say say $p(x) \in F[x]$ (nonconstant) is called <u>irreducible</u> (in $F[x]$) if its only divisors are its associates and the nonzero constants.

That is, the only divisors of $p(x)$ are of the form

$$c, \text{ and } d \cdot f(x), \text{ where}$$

$$c, d \in F \text{ (nonzero)}$$

(this is the analogue of prime integers)

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

Ex: (1) $x^2 - 4x + 4$ is reducible in $\mathbb{Q}[x]$, since

$$\underbrace{x^2 - 4x + 4}_{\deg 2} = \underbrace{(x-2)}_{\deg 1}\underbrace{(x-2)}_{\deg 1}$$

This satisfies Theorem 4.11

(2) $x^4 + x^2 - 6$ is reducible in $\mathbb{Q}[x]$, since

$$\underbrace{x^4 + x^2 - 6}_{\deg 4} = \underbrace{(x^2+3)}_{\deg 2}\underbrace{(x^2-2)}_{\deg 2}$$

(3) $x^n - 1$ $(n \geq 2)$ is reducible in $\mathbb{Q}[x]$, and

$$\underbrace{x^n - 1}_{\deg n} = \underbrace{(x-1)}_{\deg 1}\underbrace{(x^{n-1} + x^{n-2} + \cdots + x + 1)}_{\deg (n-1)}$$

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

(4) x^2+1 is...

- irreducible in $\mathbb{Q}[x]$, $\mathbb{R}[x]$
- reducible in $\mathbb{C}[x]$, since

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

- also reducible in $\mathbb{Z}_2[x]$:

$$x^2+1 = (x+1)^2 \quad \text{in } \mathbb{Z}_2[x]$$

Why?

$$(x+1)^2 = x^2 + \cancel{2x} + 1 = x^2+1.$$

Thm 4.12: Let $p(x) \in F[x]$ be nonconstant. Then TFAE (the following are equivalent):

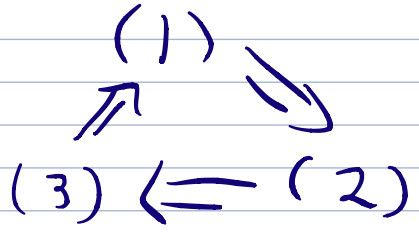
(1) $p(x)$ is irreducible

(2) If $b(x), c(x) \in F[x]$ and $p(x) \mid b(x)c(x)$, then

$$p(x) \mid b(x) \text{ or } p(x) \mid c(x)$$

(3) If $r(x), s(x) \in F[x]$ and $p(x) = r(x)\,s(x)$, then $r(x)$ or $s(x)$ is a nonzero constant.

Pf:



(1) $\Rightarrow$ (2) "If $p(x)$ is irreducible, then property (2) is true"

If $p(x)$ is irreducible, then its only divisors are constants and associates.

Let's look at $b(x)$. Since $p(x)$ is irreducible, the only possible common divisors of $p(x)$ and $b(x)$ are constants or of the form $c \cdot p(x)$, where $c \in F$.

$c \cdot p(x)$ ↝ associates of $p(x)$.

If $cp(x) \mid b(x)$, then $p(x) \mid b(x)$ and we're done.

If $c\,p(x) \mid b(x)$ then $b(x) = c\,p(x)\cdot h(x)$
$= p(x)(ch(x))$

$\Rightarrow p(x) \mid b(x)$.

Otherwise, the only common divisors are constants. This means $p(x)$ and $b(x)$ are relatively prime.

So we have $p(x) \mid b(x)\,c(x)$ and $(p(x), b(x)) = 1$,

$\Rightarrow p(x) \mid c(x)$ (Thm 4.10)

↑

poly version of Thm 1.4

This proves (2).

(2) $\Rightarrow$ (3) "If $p(x)$ satisfies (2), then $p(x)$ satisfies (3)"

Suppose $p(x) = r(x)\cdot s(x)$ This implies $p(x) \mid r(x)\cdot s(x)$. Then by (2)

$p(x) \mid r(x)$ or $p(x) \mid s(x)$.

If $p(x) \mid r(x)$, then $r(x) = p(x)a(x)$

so,

$$p(x) = r(x)s(x) = p(x) \cdot a(x) \cdot s(x)$$

(cancel $p(x)$'s:

$$1_F = a(x) \cdot s(x)$$

The degrees of both sides must be equal:

$$0 = \deg 1_F = \deg [a(x)s(x)]$$
$$= \deg a(x) + \deg s(x)$$

$\Rightarrow \deg s(x) = 0 \Rightarrow s(x)$ is constant.

Similarly, if $p(x) \mid s(x)$, then $r(x)$ is constant (same proof as above, just switch the $r(x)$'s and $s(x)$'s)

This proves (3)

(3) $\Rightarrow$ (1) "If $p(x)$ has property (3) then $p(x)$ is irreducible."

We want to show the only divisors are constants and associates

To do this, start with an arbitrary divisor $d(x)$ of $p(x)$.

We'll show $d(x)$ = constant or an associate of $p(x)$.

If $d(x) \mid p(x)$, then

$$p(x) = d(x) \cdot h(x)$$

We're going to use (3) here.

Property (3) says $d(x)$ or $h(x)$ is constant.

If $d(x)$ is constant, then we're done.

If $h(x)$ is constant, then $h(x) = c \in F$.

So, $p(x) = c \cdot d(x)$ or

$$\boxed{d(x) = c^{-1} \cdot p(x)}$$

$\Rightarrow$ $d(x)$ is an associate of $p(x)$.

Since $d(x)$ is arbitrary, this implies $p(x)$ is irreducible. ∎

Remark: This is similar to Thm 1.5: p is prime iff whenever $p \mid bc$, $p \mid b$ or $p \mid c$.

Cor 4.13: If $p(x) \mid a_1(x) \cdots a_n(x)$ and $p(x)$ is irreducible, then $p(x)$ divides at least one of the $a_i(x)$'s.

Proof uses property 2 of Thm 4.12 (basically the same as Cor 1.6)

Unique factorization for Polynomials:
Every polynomial (nonconstant) $f(x) \in F[x]$ is a product of irreducibles in $F[x]$.

This factorization is unique in the following sense: if

$$f(x) = p_1(x)\, p_2(x) \cdots p_r(x)$$

and

$$f(x) = q_1(x)\, q_2(x) \cdots q_s(x)$$

where each $p_i(x)$ and $q_j(x)$ are irreducible, then $r = s$ and after possible re-ordering and re-labeling, each $p_i(x)$ is an associate of $q_i(x)$.

Ex: $x^2 - 1$ can be factored into irreducibles in $\mathbb{Q}[x]$:

(1) $\underbrace{(x-1)}_{p_1(x)}\underbrace{(x+1)}_{p_2(x)}$

(2) $\underbrace{(3x-3)}\underbrace{\left(\frac{1}{3}x+\frac{1}{3}\right)}$

$q_1(x)$ $q_2(x)$

see how $q_1(x) = 3 \cdot p_1(x)$ and

$q_2(x) = \frac{1}{3} \cdot p_2(x)$.

These factorizations are "basically the same."

Section 4.4

Roots and Reducibility

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$

be a polynomial in $F[x]$.

Let $c \in F$. Define $f(c)$ to be the following element of F:

$f(c) = a_n c^n + a_{n-1} c^{n-1} + \cdots + a_2 c^2 + a_1 c + a_0$.

We call c a <u>root</u> (or <u>zero</u>) of $f(x)$ if $f(c) = 0_F$.

Two important Theorems

Thm 4.15 (Remainder Theorem): Let $f(x) \in F[x]$ and $a \in F$. Then the remainder when $f(x)$ is divided by $x-a$ is $f(a)$. That is,

$$f(x) = (x-a)\,q(x) + f(a)$$

f.s. $q(x) \in F[x]$.

Pf: By the division algorithm,

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

where $r(x) = 0_F$ or

$$\deg r(x) < \deg (x-a) = 1$$

In either case, $r(x)$ is some constant c:

$$f(x) = q(x)\cdot(x-a) + c.$$

Then, plug in a:

$$f(a) = q(a)\cdot(a-a) + c = q(a)\cdot 0_F + c$$
$$= 0_F + c = c.$$

$\Rightarrow f(x) = q(x)\cdot(x-a) + f(a)$. ∎

remainder

Ex: What is the remainder when we divide $\underbrace{x^2-4x+4}_{f(x)}$ by $x-1$? (in $\mathbb{Q}[x]$)

By the Remainder Thm. it should be $f(1) = 1-4+4 = 1$.

Check:

$$\begin{array}{r} x-3 \\ x-1 \overline{)\, x^2-4x+4} \\ -(x^2-x) \\ \hline -3x+4 \\ -(-3x+3) \\ \hline 1 \end{array}$$

← quotient

← remainder

$x^2-4x+4 = (x-1)(x-3)+1$ ✓

Thm 4.16 (Factor Theorem): Let $f(x) \in F[x]$ and $a \in F$. Then a is a root of $f(x)$ if and only if $(x-a)$ divides $f(x)$. (i.e. $x-a$ is a factor of $f(x)$)

Pf:

"$\Rightarrow$" if a is a root, then $x-a \mid f(x)$.

By the Remainder Theorem,

$$f(x) = (x-a)\,q(x) + f(a)$$

If a is a root, then $f(a) = 0_F$, so

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

$$\Rightarrow (x-a) \mid f(x).$$

"$\Leftarrow$" if $(x-a) \mid f(x)$ then a is a root.

If $x-a \mid f(x)$, then $f(x) = (x-a)\cdot h(x)$.

Then, just plug in a:

$$f(a) = (a-a)\cdot h(a) = 0_F \cdot h(a) = 0_F$$

$\Rightarrow$ a is root. $\square$

Ex: (1) 2 is a root of x^2-4x+4 and $x^2-4x+4 = (x-2)(x+2)$

so $x-2 \mid x^2-4x+4$.

(2) 1 is clearly a root of x^n-1, and as we saw earlier,

$$x^n-1 = (x-1)(x^{n-1}+x^{n-2}+\dots+x+1)$$

so $x-1 \mid x^n-1$.

(3) When n is odd, -1 is a root of x^n+1 in $\mathbb{Q}[x]$, so $x+1 \mid x^n+1$. When n is even, this is not the case, since then

$$(-1)^n+1 = 2.$$

So when n is even, $x+1 \nmid x^n+1$.

Cor 4.17: Let F be a field and $f(x) \in F[x]$ be nonzero of degree n. Then $f(x)$ has at most n roots in F.

We'll prove this next time.

It's important that F is a field here.

Examples:

Consider $f(x) = x^2 + x$ in $\mathbb{Z}_6[x]$

$\mathbb{Z}_6$ is not a field, check for roots:

$f(0) = 0$ ✓

$f(1) = 2$ ✗

$f(3) = 9 + 3 = 12 = 0$ ✓

$f(4) = 16 + 4 = 20 = 4$ ✗

$f(2) = 6 = 0$ ✓

$f(5) = f(-1) = 1 - 1 = 0$ ✓

So, $x^2 + x$ has 4 roots in $\mathbb{Z}_6$ even though it's degree -2.

So when the coefficient ring is not a field you can get

more roots than the degree of the polynomial.