Factorization of Polynomials

Wednesday, 16 March 2022 14:09

Recap: A polynomial is a "formal" expression involving "scalar" from R and indeterminate x.

We compare, add, muleiply them by a set of rules.

Hence can't say "plug $x=2$ into $3x^2-1$" or "solve $x^2-3x+1=0$"

Main motivation for evaluation homomorphism

$ev_\alpha : F[x] \to E \quad (\overset{\mathbb{R}}{F} \leq \overset{\mathbb{C}}{E} \ni \alpha)$

$ev_\alpha(a_0 + a_1 x + \dots + a_n x^n)$

$= a_0 + a_1\alpha + \dots + a_n\alpha^n$

$\mathbb{R}[x] / \ker(ev_i) \cong im(ev_i) = \mathbb{C}$ — $\circledast$

Reverse engineer this process: "Guess" what should be $\ker(ev_i) = I$

Guess $I = \{(x^2+1)p(x) : p(x) \in \mathbb{R}[x]\}$

<u>Define</u> $\mathbb{C}$ as $\mathbb{R}[x]/I$

Define $\sqrt{2}$ using $\mathbb{Q}[x] / \underbrace{\{(x^2-2)p(x)\}}_{I}$, etc

$x^2-2 \in I$

$(x^2-2)+I = I$

$(x+I)^2 = 2+I$

The mapping perspective is essential.

$F[x]$ polynomial ring over field F.

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

Application: Solve equations

Division algorithm

Thm: Let $f(x), g(x) \in F[x]$, $\deg g \geq 0$. Then there exist $q(x), r(x) \in F[x]$ s.t.

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

and $\deg r < \deg g$ or $r = 0$.

Example: $f(x) = x^3$, $g(x) = x - 1$

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

$$\deg r = 0 < 1 = \deg g$$

"Proof": Do long division

$$\left.\begin{aligned} f(x) &= x^4 - 3x^3 + 2x^2 + 4x - 1 \\ g(x) &= x^2 - 2x + 3 \end{aligned}\right\} \mathbb{R}[x]$$

$$\begin{array}{r|l}
 & \phantom{x^4 - 3x^3 + {}} x^2 - x - 3 \\ \hline
x^2 - 2x + 3 & x^4 - 3x^3 + 2x^2 + 4x - 1 \\
 & x^4 - 2x^3 + 3x^2 \\ \hline
 & - x^3 - x^2 + 4x \\
 & - x^3 + 2x^2 - 3x \\ \hline
 & - 3x^2 + 7x - 1 \\
 & - 3x^2 + 6x - 9 \\ \hline
 & \phantom{x^4 - x^3 - 3x^2 + {}} x + 8
\end{array}$$

$q(x) = x^2 - x - 3$, $r(x) = x + 8$

Why long division always work?

(1) We can always proceed as long as what's left is of deg $\geq$ deg g: we are working in a field, so

$$f(x) = ax^n + \cdots \qquad (n \geq m)$$
$$g(x) = bx^m + \cdots$$

$$\Rightarrow \frac{a}{b}x^{n-m}g(x) = ax^n + \cdots$$

Non-example: $f(x) = x$, $g(x) = 2$ in $\mathbb{Z}[x]$.

(2) The long division always stops: every step, the degree of what's left decreases by at least 1, so in at most deg f many steps, the division stops.

Uniqueness of $q(x), r(x)$:

$$f(x) = q_1(x) \cdot g(x) + r_1(x)$$

$$= q_2(x) \cdot g(x) + r_2(x)$$

$$\Rightarrow \underbrace{\underbrace{g(x)}_{\deg g} \underbrace{(q_1(x) - q_2(x))}_{\text{either } 0 \text{ or } \deg \geq 0}}_{\text{either } 0 \text{ or } \deg \geq \deg g} = \underbrace{r_2(x) - r_1(x)}_{\deg < \deg g.}$$

$\leftarrow$ only feasible one

$$\Rightarrow q_1(x) - q_2(x) = 0$$

$$\Rightarrow r_2(x) = r_1(x)$$

We used the assumption that F is a field

$$(\overset{\neq 0}{a} x^n + \ldots)(\overset{\neq 0}{b} x^m + \ldots)$$

$$= (\underset{\neq 0}{ab} x^{n+m} + \ldots \_\_)$$

$\square$

Prop: If $a \in F$ is a root of $f(x) \in F[x]$, then $x-a$ is a factor of $f(x)$.

There exists $h(x) \in F[x]$ s.t. $f(x) = (x-a)\,h(x)$.

Proof: Apply long division to $f(x)$, $g(x) = x-a$ and get $f(x) = (x-a)q(x) + r(x)$.

Since $\deg r < \deg(g)$ or $r = 0$, $r(x)$ is constant.

Now $\overset{=0}{f(a)} = \underbrace{(a-a)q(a)}_{0} + \underset{0}{r(a)}$

So $r(x) = r(a) = 0$ $\square$

Corollary: A degree n polynomia[l] in $F[x]$ can have at most n roots in F. 1

Proof: Let $f(x)$ be of deg n

Let $a_1, \ldots, a_d$ be the distinct roots of $f(x)$.

By factor thm,

$$f(x) = (x - a_1)\, g_1(x)$$

Now $0 = f(a_2) = (a_2 - a_1)\, g_1(a_2)$

$\Rightarrow$ a_2 is a root of $g_1(x)$

b/c F is an integral domain

$$f(x) = (x-a_1)(x-a_2)\, g_2(x)$$
$$= (x-a_1)(x-a_2)(x-a_3)\, g_3(x)$$
$$= \cdots$$

Because the degrees of $f(x), g_1(x), g_2(x), \ldots$ are strictly decreasing by 1 everytime, so at worst

$$f(x) = (x-a_1)\ldots(x-a_n)\underbrace{g_n(x)}_{\deg 0}$$

Now a_{n+1} (if any) can't be a root of $f(x)$. $\square$

Non-example: (The one we did in class was incorrect, will do again tmr)

Corollary: Let F be a finite field (e.g. $\mathbb{Z}_p$). Then $(F^\times, \cdot)$ is cyclic.

$\mathbb{Z}_{17}$ is a finite field

$(\mathbb{Z}_{17}^{\times}, \cdot)$ is a group of size 16.

Proof: Suppose $(F^{\times}, \cdot)$ ← abelian as $\cdot$ is commutative

$\cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_d}$

Let $m = \operatorname{lcm}(n_1, \dots, n_d)$. Then $\forall g \in F^{\times}$

$g = (g_1, \dots, g_d)$

$\Rightarrow g^m = (g_1^m, \dots, g_d^m)$ Using multiplicative notation for $\mathbb{Z}_{n_i}$ as we are think of $\cdot$

$\Rightarrow g^m = \left((g_1^{n_1})^{m/n_1}, \dots, (g_d^{n_d})^{m/n_d}\right)$.

$= (e, \dots, e)$ Identity in $F^{\times} \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_d}$

$= 1 \in F$

$\Rightarrow g^m = 1$ for every $g \in F^\times$

$\Rightarrow x^m - 1 = 0$ has

$|F^\times|$ many sol'n in F.

$\Rightarrow \operatorname{lcm}(n_1, \ldots, n_d) = m \geq |F^\times| = n_1 n_2 \ldots n_d$

$\Rightarrow n_1, \ldots, n_d$ are relatively prime

$\Rightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_d} \cong \mathbb{Z}_{n_1 \ldots n_d}$

$\Rightarrow (F^\times, \cdot) \cong \mathbb{Z}_{n_1 \ldots n_d}$ is cyclic.

Example: In $(\mathbb{Z}_5^\times, \cdot)$,

$2, 4, 3, 1$ is cyclic $\cong \mathbb{Z}_4$

$$\begin{array}{cccc} 2, & 4, & 3, & 1 \\ \parallel & \parallel & \parallel & \parallel \\ 2^1 & 2^2 & 2^3 & 2^4 \end{array} \text{ in } \mathbb{Z}_5$$