Factorization of Polynomials (II)

Thursday, 17 March 2022 12:08

Recall: A deg n polynomial $f(x)$ in $F[x]$ has at most n (distinct) roots. (F is a field)

Corollary: If F is a finite field, then $(F^\times, \cdot)$ is cyclic.

$(\mathbb{Z}_{12}^\times, \cdot) = (\{1, 5, 7, 11\}, \cdot)$

$\varphi(12) = |\mathbb{Z}_{12}^\times| = 4$

Claim: $x^2 \equiv 1 \pmod{12}$, $\forall x \in \mathbb{Z}_{12}^\times$.

Proof: (1) By direct calculation

(2) $a \equiv 1 \pmod{12}$

$\iff a \equiv 1 \pmod 3$ & $1 \pmod 4$

By Euler thm, $x^2 \equiv 1 \pmod 3$

$x^2 \equiv 1 \pmod 4$

Corollary: (1) $x^2-1=0$ has 4 soln in $\mathbb{Z}_{12}$

(2) $(\mathbb{Z}_{12}^\times, \cdot)$ is not cyclic.

$$\cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$$

Fact: $(\mathbb{Z}_n^\times, \cdot)$ is cyclic

$\Leftrightarrow$ $n = 1, 2, 4, p^k, 2\cdot p^k$ p odd prime

Irreducible polynomial over F.

Def: A polynomial $f(x) \in F[x]$ is <u>irreducible</u> over F if $f(x)$ can't be factorized as $g(x)h(x)$ for $\deg g, \deg h < \deg f$.

Example: • x^2+1 is irred over $\mathbb{R}$ but it is not irred over $\mathbb{C}$ b/c $x^2+1 = (x-i)(x+i)$

- x^2-2 is irred over $\mathbb{Q}$ but it is not irred over $\mathbb{R}$ or $\mathbb{C}$ b/c $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$.
- A polynomial is irred over $\mathbb{C}$ $\Leftrightarrow$ the polynomial has $\deg \leq 1$ b/c if a polynomial $f(x)$ $/\mathbb{C}$ has $\deg \geq 2$, then by TFTA, $f(x)$ has a root a, so by factor thm, $f(x)=(x-a)g(x)$ for some $\deg g < \deg f$.

Prop: A deg 2 or 3 polynomial $f(x)$ is irred$_{/F}$ $\Leftrightarrow$ it has no root $/F$.

Proof: If $f(x)=g(x)h(x)$, then

$0<\deg g, \deg h < \deg f = 2$ or 3

$\deg g + \deg h = \deg f = 2$ or 3

So either $\deg g = 1$ or $\deg h = 1$,

i.e., $g = ax + b$ (or $h = ax + b$).

So $\frac{-b}{a}$ is a root of $f(x)$.

Conversely, if α is a root of $f(x)$, then $f(x) = (x - \alpha) g(x)$. $\square$

Non-example:

$(x^2 + 4x + 5)(x^2 + 2x + 3)$ is not irred over $\mathbb{R}$, but it has no real roots.

Irreducible poly over $\mathbb{Q}$

Thm (Gauss lemma): Let $f(x)$ be a polynomial with integer coefficients clear denominators if necessary: $\frac{1}{2}x^2 + \frac{1}{3}x + 1 = \frac{1}{6}(3x^2 + 2x + 6)$

Then $f(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{Q}[x]$ implies $f(x) = \tilde{g}(x)\tilde{h}(x)$ for some $\tilde{g}, \tilde{h} \in \mathbb{Z}[x]$ and $\deg \tilde{g} = \deg g$, $\deg \tilde{h} = \deg h$.

Idea: $f(x) = \ldots\ldots + 3$

$$\left.\begin{aligned} g(x) &= \ldots\ldots + \tfrac{1}{10}x + \tfrac{1}{2} \\ h(x) &= \ldots\ldots + 5x + 6 \end{aligned}\right\} \begin{aligned} f(x) &= \ldots \\ &+ \left(\tfrac{3}{5} + \tfrac{5}{2}\right)x + 3 \end{aligned}$$

Thm (Eisenstein criterion):

Lee $f(x) \in \mathbb{Z}[x] = a_n x^n + \ldots + a_0$

If there exists a prime p s.t.

(1) $p \nmid a_n$;

(2) $p \mid a_i$, for $i = 0, \ldots, n-1$;

(3) $p^2 \nmid a_0$,

then $f(x)$ is irred over $\mathbb{Z}$ (also $\mathbb{Q}$)

Quick example! x^2-2 is irred.
b/c Eisenstein criterion with $p=2$.

Proof: Suppose $f(x)$ is reducible,

So $f(x) = (b_r x^r + \cdots + b_0) \cdot (c_s x^s + \cdots + c_0)$

Since $a_n = b_r c_s$, $p \nmid b_r$ and $p \nmid c_s$.

Since $a_0 = b_0 c_0$, p divides exactly one of b_0 and c_0. Say $p \nmid b_0$, $p \mid c_0$.

So there exists a smallest $m (\leq s < n)$ s.t. $p \nmid c_m$ but $p \mid c_i$ for $i = 0, \dots, m-1$.

$$a_m = \underbrace{\underbrace{\underset{\substack{\uparrow \\ \text{not div} \\ \text{by } p}}{b_0}\ \underset{\substack{\uparrow \\ \text{not div} \\ \text{by } p}}{c_m}}_{\text{not div by } p} + \underbrace{b_1 c_{m-1} + \cdots + b_m c_0}_{\text{divisible by } p}}_{\text{not divisible by } p.}$$

A contradiction. $\square$

Example: $25x^5 - 9x^4 - 3x^2 - 12$ is irred over $\mathbb{Z}$ b/c of the Eisenstein criterion w/ $p=3$

Corollary: Let p be a prime. Then $x^{p-1} + x^{p-2} + \ldots + 1$ is irred.

Proof: $x^{p-1} + x^{p-2} + \ldots + 1 = \dfrac{x^p - 1}{x-1}$.

Observation: $f(x)$ is irred iff $f(x+1)$ is irred.

Proof: If $f(x+1) = g(x)h(x)$, then $f(x) = g(x-1)h(x-1)$. $\square$

Use the observation on $x^{p-1} + \ldots + 1$.

$$(x+1)^{p-1} + \ldots + 1 = \frac{(x+1)^p - 1}{(x+1) - 1}$$

$$= \frac{(x+1)^p - 1}{x}$$

$$= \frac{\binom{p}{p}x^p + \binom{p}{p-1}x^{p-1} + \cdots + \binom{p}{1}x + 1 - 1}{x}$$

$$= \binom{p}{p}x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{1}.$$

Apply Einsenstein criteriom with p.

(1) $\binom{p}{p} = 1$ is not divisible by p

(3) $\binom{p}{1} = p$ is not divisible by p^2.

(2) Need to check $\binom{p}{i}$ is divisible by p for $i = 1, 2, \ldots, p-1$.

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \begin{array}{l} \leftarrow \text{divisible by } p \\ \leftarrow \text{not divisible by } p \end{array} \quad \square$$

Non-example: $x^5 + \ldots + 1$ $\quad 5 = 6-1$

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

In fact, $x^{n-1} + \ldots + 1$ is irred $\Leftrightarrow$ n is a prime

Uniqueness of factorization

Thm: Let $f(x) \in F[x]$.

Suppose $f(x) = p_1(x) \cdot \ldots \cdot p_r(x)$

$$= q_1(x) \cdots \cdot q_s(x)$$

are two factorizations with p_i, q_i are all irreducible.

Then $r = s$, and we can rearrange q_i's s.t. $p_i(x)$ and $q_i(x)$ are the same up to a non-zero scalar multiple.

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

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

Non-example: $R = \mathbb{Z}[\sqrt{-5}]$

$= \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$.

e.g. $(a+b\sqrt{-5})(c+d\sqrt{-5})$

$= (ac-5bd)+(ad+bc)\sqrt{-5}$

$6 = 2\times 3$

$= (1+\sqrt{-5})(1-\sqrt{-5})$

$x^n+y^n=z^n$ has no non-zero soln for $n\geq 3$

Pick $\xi^n=1$.

$(x+y)(x+\xi y)(x+\xi^2 y)\cdots(x+\xi^{n-1}y)$

$= z^n$

is a factorization in

$\mathbb{Z}[\xi] = \{a_0+a_1\xi+a_2\xi^2+\cdots+a_{n-1}\xi^{n-1}$

$a_0,\dots,a_{n-1}\in\mathbb{Z}\}$