Rilun Rotman
Irr. Poly, 1.38

Take $f \in \mathbb{Q}[x]$, $f \neq 0$. $f = a_n x^n + \cdots + a_0$, $a_i \in \mathbb{Q}$

Clear denominators: Get (rational #)(polyn. w/ integer coefficients)

← take gcd of coefficients out

Example $f = \frac{2}{5}x^2 - \frac{4}{3}x + \frac{6}{15}$ $\operatorname{lcm}(5, 3, 15) = 15$

$f = \frac{1}{15}(6x^2 - 20x + 12)$ $\gcd(6, -20, 12) = 2$

$\in \mathbb{Z}[x]$, $\gcd(\text{coeff}) = 1$.

$f = \frac{2}{15}(3x^2 - 10x + 6) = c(f)\, f^*(x)$

$c(f) \in \mathbb{Q}$ content of $f$; $f^*(x)$ primitive

Can make $c(f) > 0$, $-f^*(x)$ still primitive

**Def** $f = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ is called primitive if gcd of its coefficients is 1.

**Prop** $\forall f(x) \in \mathbb{Q}[x]$, $f \neq 0$ has a unique factorization

$$f(x) = c(f) f^*(x)$$

$c(f) \in \mathbb{Q}_{>0}$ (positive) and $f^*(x) \in \mathbb{Z}[x]$ is primitive

**Proof** (uniqueness) $f = c f^*$ Assume $\exists$ another factorization $f = e\, h(x)$

$c f^* = e h$ let $\frac{e}{c} = \frac{u}{v}$, $u, v$ coprime, $v, u \in \mathbb{Z}_{>0}$. $e \in \mathbb{Q}_{>0}$ primitive

$\Rightarrow v f^*(x) = u h(x)$ holds $\Rightarrow v$ divides each coeff of $u h(x)$, $(u, v) = 1 \Rightarrow$

$v$ divides each coeff of $h(x)$. $\Rightarrow$ $v = 1$. Likewise, $u = 1$.

$\Rightarrow$ factorization unique

**Corollary** if $f(x) \in \mathbb{Z}[x]$ then $c(f) \in \mathbb{Z}$

**Proof** $c(f)$ then is the gcd of coefficients of $f$.

**Corollary** If $f(x) \in \mathbb{Q}[x]$, $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$ then

$$c(f) = c(g)c(h) \quad \text{and} \quad f^\vee(x) = g^\vee(x)h^\vee(x)$$

**Pf** $f(x) = g(x)h(x) = c(g)g^\vee(x)c(h)h^\vee(x) = (c(g)c(h))\, g^\vee(x)h^\vee(x)$

by uniqueness. $\quad \| \qquad \|$

$$f(x) = c(f) \quad f^\vee(x)$$

**Thm** (Gauss) If $p(x) \in \mathbb{Z}[x]$ is not a product of two polynomials in $\mathbb{Z}[x]$ of degree $<$ deg $p$, then $p(x)$ is irreducible in $\mathbb{Q}[x]$.

**Proof** if $p(x) = g(x)h(x)$ in $\mathbb{Q}[x] \Rightarrow p(x) = c(g)c(h)\, g^\vee(x)h^\vee(x)$

$g^\vee, h^\vee$ primitive in $\mathbb{Z}[x]$. $\qquad$ ↑ ↑ primitive polynomials

**Need lemma** The product of two primitive polynomials $f, g$ is itself primitive

**Proof** if $p \mid \gcd(\text{coeff of } fg)$ then $fg \pmod p \equiv 0$.

$\mathbb{Z} \xrightarrow{\gamma} \mathbb{Z}_p$ mod $p$ reduction homomorphism

$\mathbb{Z}[x] \xrightarrow{\gamma} \mathbb{Z}_p[x]$ $\quad f(x) \longrightarrow f(x) \bmod p$ coefficients.

↑ integral domain.

$\gamma(fg) = 0 \quad \gamma(f)\gamma(g) \equiv 0 \Rightarrow \gamma(f) \equiv 0$ or $\gamma(g) \equiv 0$.

$\Rightarrow p \mid \gcd(\text{coeff of } f)$ or $p \mid \gcd(\text{coeff of } g)$

$\Downarrow$ $f$ not primitive $\qquad$ $\Downarrow$ $g$ is not primitive $\qquad$ contradiction! lemma □

$\Rightarrow$ by Lemma $g^*(x)h^*(x)$ is primitive $\quad p(x) = c(g)c(h)\, g^*(x)h^*(x)$

$p(x) = d\, p^*(x)$ factorization $\qquad$ $c(g)c(h) = d$ $\qquad$ $g^*(x)h^*(x) = p^*(x) \in \mathbb{Z}[x]$

by uniqueness $=$ ↗

$\Rightarrow$ Can factor in $\mathbb{Z}[x]$ as $(c(g)c(h))\, g^*(x)\, h^*(x)$

Contradiction $\qquad$ $\in \mathbb{Z}[x]$ $\qquad$ $\in \mathbb{Z}[x]$

Enough to study factorizations in $\mathbb{Z}[x]$

$\mathbb{Z}[x] \xrightarrow{\gamma} \mathbb{Z}_p[x]$ $\qquad$ absence of factorizations in $\mathbb{Z}_p[x]$

$f = gh \Rightarrow \bar{f} = \bar{g}\bar{h}$ $\qquad$ implies absence of factorizations in $\mathbb{Z}[x]$

$\Rightarrow$ irreducibility of $f(x)$ in $\mathbb{Q}[x]$

Examples

1) $f(x) = x^3 + 5x^2 + 3x + 1$

mod 2 $\quad p=2 \qquad \bar{f}(x) = x^3 + x^2 + x + 1 = (x+1)(x^2+1) = (x+1)^3$ factors.

$p=3 \qquad \bar{f}(x) = x^3 + 2x^2 + 1 \qquad \bar{f}(0) \neq 0 \qquad \bar{f}(1) = 4 \neq 0 \pmod 3$

$\bar{f}(2) = 17 \neq 0 \pmod 3$

$\Rightarrow \bar{f}(x)$ is irreducible in $\mathbb{Z}/3[x] \Rightarrow f(x)$ does not factor in $\mathbb{Z}[x]$

$\Rightarrow f(x)$ is irreducible in $\mathbb{Q}$.

2) $f(x) = 6x^3 + x + 1$ not monic $2, 3 \mid 6$. cannot use $p = 2, 3$ due to drop in degree

try $p=5 \qquad \bar{f}(x) = x^3 + x + 1$. Check for roots

| $\alpha$ | 0 | 1 | 2 | 3 | 4 = −1 |
|---|---|---|---|---|---|
| $\bar{f}(\alpha)$ | 1 | 3 | 8+2+1 = 1 | 27+3+1 = 1 | −4−1+1 = −4 |

no roots, deg 3 $\Rightarrow \bar{f}(x)$ is irreducible over $\mathbb{F}_5$.

$\Rightarrow f(x)$ is irreducible / $\mathbb{Q}$.

**Thm** (Eisenstein criterion). Let $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$

If $\exists$ a prime $p$, $p \mid a_i \ \forall i < n$, $p \nmid a_n$, $p^2 \nmid a_0 \Rightarrow f(x)$

is irreducible in $\mathbb{Q}[x]$

$p \nmid a_n$ $\qquad$ $p^2 \nmid a_0$

$a_n x^n + \dots + a_1 x + a_0 \Rightarrow$ irreducible

$p \mid a_i \ \forall i < n$

$p = 5$

$f(x)$ $3x^4 + 5x^3 - 10x^2 - 15$

Satisfies the criterion, irreducible in $\mathbb{Q}[x]$

$5 \nmid 3$ $\quad 5 \mid (5, -10, 0, -15)$ $\quad 5^2 \nmid -15$.

**Proof** For such $f$ and $p$ consider homomorphism $\gamma$

$\gamma: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$.

$\begin{cases} g(x) = b_m x^m + \dots + b_0 \\ h(x) = c_{n-m} x^{n-m} + \dots + c_0 \end{cases}$

If $f$ reducible in $\mathbb{Q} \Rightarrow$ factors in $\mathbb{Z}$, $f = g(x)h(x)$ $\deg g, \deg h < n$

$\gamma(f) = \gamma(g)\gamma(h)$ $\qquad$ $\gamma(f) = a_n x^n + 0 + \dots + 0 = a_n x^n$

unique factorization in $\mathbb{Z}_p[x] \Rightarrow \gamma(g) = b_m x^m$ $\quad b_{m-1} \dots b_0 \equiv 0 \pmod p$

$\gamma(h) = c_{n-m} x^{n-m}$ $\quad c_{n-m-1}, \dots c_0 \equiv 0 \pmod p$

$a_0 = b_0 c_0$

$p \mid b_0, p \mid c_0 \Rightarrow p^2 \mid a_0$ contradiction

Example. Def $p$-th cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$$

Example $\Phi_3(x) = x^2 + x + 1$ $\quad \Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

Prop $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$ $\forall$ prime $p$.

Proof $f(x)$ is irreducible iff $f(x+c)$ irreducible, $c$ a constant (exercise).

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x + 1 - 1}{x}$$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1} \cdot 1$$

$p \mid \binom{p}{i}$ for $i = 1, 2, \ldots p-1$ $\qquad \binom{p}{p-1} = p$.

satisfies Eisenstein criterion $\Rightarrow$ irreducible $/\mathbb{Q}$.

$n$ not prime $\quad x^{n-1} + \cdots + 1$ factors. $\quad x^3 + x^2 + x + 1 \quad n = 4$.

$\exists$ $p$ prime $p \mid a$, $p^2 \nmid a$

Prop If $a \in \mathbb{Z}$, $a$ is not a perfect $p^{th}$ power $\Rightarrow x^n - a$ is irreducible in $\mathbb{Q}[x]$ $\forall n \geq 2$

$p \mid a \quad p^2 \nmid a$

$x^n - a$ $\qquad x^n - 2$, $x^n - 3$, $x^n - 10 \ldots$

$\Rightarrow \exists$ irreducible polyn $/\mathbb{Q}$ of any degree $n$ $\qquad x^n - 2$