Irreducibility

(1) For primitive polynomials,

irreducibility in $\mathbb{Z}[x]$ = irred. in $\mathbb{Q}[x]$.

(2) Irred. in $\mathbb{Z}[x]$.

$f(x) \in \mathbb{Z}[x]$ leading term not div by p

$f(x)$ primitive & $\bar{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ irreducible

$\Rightarrow$ $f(x)$ is irreducible.

Pf: Say $f(x) = g(x) \cdot h(x)$ reduce mod p

$\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$ trivial mod p

$\Downarrow$

original also trivial.

Ex: $\cos(20°)$ satisfies

$$\cos(60°) = 4\cos(20)^3 - 3\cos(20)$$

$$\frac{1}{2} = 4x^3 - 3x \qquad 4x^3 - 3x - \frac{1}{2} = 0$$

$$8x^3 - 6x - 1 = 0$$

mod 5

$\underline{3x^3 - x - 1}$ irreducible? $\Longleftrightarrow$ no roots?

✓ $\quad$ $0, 1, 2, 3, 4$.

None is a root

Warning: There are $f(x) \in \mathbb{Z}[x]$ which are reducible mod every p but irreducible in $\mathbb{Z}[x]$!

primitive

Thm (Eisenstein): Let $f(x) \in \mathbb{Z}[x]$ be such that a prime p does not divide the leading coeff of f, divides every other coeff, but p^2 does not divide the constant term, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Ex: $x^3 - 5$ irreducible in $\mathbb{Z}[x]$ $\mathbb{Q}[x]$

$x^n \pm p$ — " —

Pf: Say $f(x) = g(x) \cdot h(x)$. & $f(x)$ leading term not div by p

↳ non-trivial. all other div by p.

$f(x)$ primitive.

Let's prove the constant term of $f(x)$ must be div. by p^2.

$$\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x) \quad \text{in } \mathbb{Z}/p\mathbb{Z}[x]$$

$$\| $$

$$c \cdot x^n \Rightarrow \begin{array}{l} \bar{g}(x) = \text{const} \cdot x^m \\ \bar{h}(x) = \text{const} \cdot x^{n-m} \end{array} \quad 0 \le m \le n$$

$m=0 \Rightarrow \deg \bar{h}(x) = n = \deg \bar{f}(x) = \deg f(x)$

$\Rightarrow \deg h(x) = n$ so $g(x)$ is a constant.

$\Rightarrow g(x) \cdot h(x)$ is a trivial factorisation.

not possible. So $m > 0$.

similarly $\Rightarrow n-m > 0$

$$\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$$

$\bar{g}(x) = \text{const. } x^m$, $\quad \bar{h}(x) = \text{const } x^{n-m}$

$\Rightarrow$ const. terms of $g(x)$ & $h(x)$ div by p.

$\Rightarrow$ const. term of $f(x)$ div. by p^2

$\square$.

<u>Moral.</u> $\quad f(x) \xrightarrow{\text{mod } p} \bar{f}(x)$

factorisation. $\xleftarrow{\text{Constrains}}$ ~~understand~~. Factorisation

Example: $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Q}[x]$ **irreducible.**

$$= \frac{x^p - 1}{x - 1}$$

$\Rightarrow$ ξ_p has degree $(p-1)$ over $\mathbb{Q}$.

Look at $f(x+1) = \dfrac{(x+1)^p - 1}{x}$

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

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-1} x^0$$

irred by Eisenstein.

deg 4 poly. in $\mathbb{Z}[x]$ primitive.

mod 3

(Linear) $\times$ (cubic).

mod 5

(quadratic) $\times$ (quadratic)