

Prove that  $x^4 + 1$  is irreducible in  $\mathbb{Q}[x]$ .

A polynomial is irreducible in integers if it cannot be represented as a multiple of nonconstant integer polynomials.

$$\begin{array}{r} x^2 + 2x + 1 = (x+1)^2 \\ 2x + 1 \\ x^2 + 1 \end{array} \quad \begin{array}{l} \checkmark \\ \times \end{array} \quad \left. \vphantom{\begin{array}{r} x^2 + 2x + 1 \\ 2x + 1 \\ x^2 + 1 \end{array}} \right\} \text{in } \mathbb{Z}[x]$$

$K[x]$  is a set of polynomials composed of monomials with coefficients in the set  $K$ .

$\mathbb{R}[x] \Rightarrow$  the set of polynomials in real numbers

e.g.  $\sqrt{2}x^2 + \frac{2}{3}x + 19, \pi x^2$

$\mathbb{Q}[x] \Rightarrow$  " rational "

e.g.  $\frac{1}{3}x^3 + 2x - 3$

$\mathbb{Z}[x] \Rightarrow$  " integers "

e.g.  $2x^2 + 5x$

$\mathbb{C}[x] \Rightarrow$  " complex "

e.g.  $ix^2$

Prove that  $x^4 + 1$  is irreducible in  $\mathbb{Q}[x]$ .

P.F. 1)

Rational root theorem

If  $\frac{p}{q}$  ( $(p, q) = 1$ ) is a root of  $P(x)$ , then,  $p | a_0, q | a_n$ .

$$q = \pm 1, p = \pm 1$$

$\therefore$  rational root  $= \pm 1$  if it exists.

$x^q + 1 > 0$ ,  $x^q + 1$  has no solution over  $\mathbb{R}$

$(\Rightarrow)$

$x^q + 1$  cannot be written as a multiple of linear and cubic polynomial.

$$\therefore x^q + 1 = (ax^2 + bx + c)(dx^2 + ex + f)$$

$$ad = 1, cf = 1$$

$$a = d = \pm 1, c = f = \pm 1$$

$$\begin{aligned} x^q + 1 &= (x^2 + bx \pm 1)(x^2 + ex \pm 1) \\ &= x^4 + (b+e)x^3 + (be \pm 2)x^2 \pm (b+e)x + 1 \end{aligned}$$

$$\therefore b = -e$$

However,  $be = \pm 2$  is unobtainable since  $b, e \notin \mathbb{Q}$ .

Thus,  $x^q + 1$  is irreducible in  $\mathbb{Q}[z]$ . □

PF 2) Eisenstein's criterion.

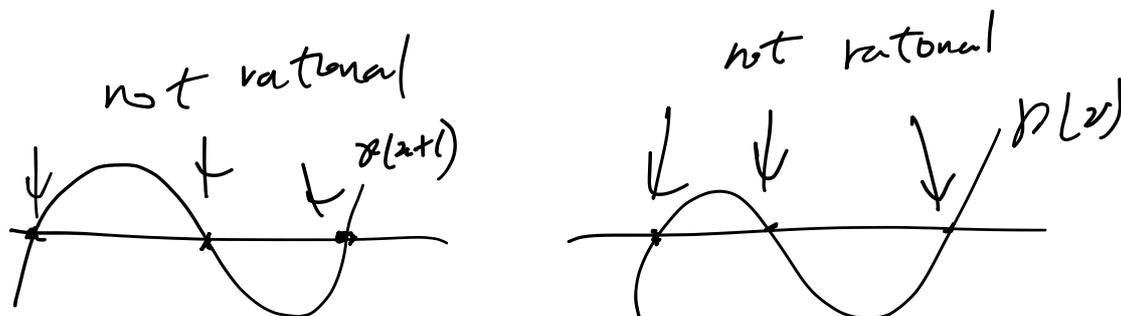
Let  $p(x) \in \mathbb{Z}[x]$  be defined as  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ .

$p(x)$  is irreducible in  $\mathbb{Q}[x]$  if there exists a prime  $p$  such that

- $p \nmid a_n$
- $p \mid a_i \quad \forall \quad 0 \leq i < n$
- $p^2 \nmid a_0$ .

$$\text{Let } p(x) = x^q + 1.$$

If  $p(x+1)$  is irreducible in  $\mathbb{Q}[x]$ ,  $p(x)$  is irreducible in  $\mathbb{Q}[x]$ .



$$p(x+1) = (x+1)^q + 1 = x^q + \binom{q}{1}x^{q-1} + \binom{q}{2}x^{q-2} + \binom{q}{3}x^{q-3} + \dots + 2$$

Consider  $p=2$ .

- $p \mid a_i \quad \forall 0 \leq i < n$
- $p \nmid a_n$
- $p^2 \nmid a_0$

Therefore, by Eisenstein's criterion,  $x^q + 1$  is irreducible in  $\mathbb{Q}[x]$ .

D