FATTORIZZARE POLINOMI

Note Title 12/6/2017

Lavoriamo in $\mathbb{Z}/2\mathbb{Z}[x]$. Determinare tutti i polinomi irriducibili di grado ≤ 3

deg 1 : x, $x+1$

deg 2 : $x^2 + ax + b$ $\quad a, b \in \mathbb{Z}/2\mathbb{Z}$

IRRIDUCIBILE → $x^2 + x + 1$

RIDUCIBILE → $x^2 + 1 = (x-1)(x+1)$

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

deg = 3 $\quad x^3 + ax^2 + bx + 1$ $\quad p(x) = (x-1)q(x)$ $\Rightarrow p(1) = 0$

RIDUCIBILE $\quad x^3 + \quad + 1$

IRRIDUCIBILE $\quad x^3 + x^2 \quad + 1$

IRRIDUCIBILE $\quad x^3 + \quad x + 1$

RIDUCIBILE $\quad x^3 + x^2 + x + 1$

Fattorizzare $x^4 + x^2 + 1$ in $\mathbb{Z}/2\mathbb{Z}[x]$

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

Esempio in $\mathbb{Q}[x]$

$f(x) = x^3 + nx + 1$ è irrid. in $\mathbb{Q}[x]$

per (a) n intero positivo
(b) n intero dispari

(a) $f(x)$ rid. in $\mathbb{Q}[x] \Rightarrow$ rid. anche in $\mathbb{Z}[x]$

CRITERIO PER LE RADICI RAZIONALI

Sia $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$

Se $z = a/b$ ($(a,b) = 1$) è una radice razionale di $f(x)$

allora $a \mid a_0$, $b \mid a_n$

Dim $f(a/b) = 0 \overset{\text{Ruffini}}{\Rightarrow} (x - \frac{a}{b}) \mid f(x)$ in $\mathbb{Q}[x]$

$$f(x) = (x - \tfrac{a}{b})\, g(x) \qquad g(x) \in \mathbb{Q}[x]$$
$$= (bx - a) \cdot \frac{g(x)}{b} \qquad \frac{g(x)}{b} \in \mathbb{Z}[x]$$

$\Rightarrow$ (lemma di Gauss) $(bx - a) \mid f(x)$ in $\mathbb{Z}[x]$

$$\Rightarrow f(x) = (bx - a)(c_{n-1} x^{n-1} + \dots + c_0)$$

Confrontando il termine di grado max:

$$a_n = b\, c_{n-1} \Rightarrow b \mid a_n$$

In grado 0: $a_0 = -a c_0 \Rightarrow a \mid a_0$ ∎

$$\{\text{Radici razionali di } f(x)=0\} \subseteq \{\pm 1\}$$

$$f(1) = 1 + n + 1 > 0$$

$$f(-1) = -1 - n + 1 < 0$$

Quindi $f(x)$ non ha radici razionali

$\Rightarrow f(x)$ irriducibile $(\deg f = 3)$

(b) Supponiamo ora n dispari.

$f(x) = X^3 + nx + 1$ irrid in $\mathbb{Z}[x]$?

Se $f(x) = g(x)\, h(x)$ in $\mathbb{Z}[x]$

$\Downarrow$

$\overline{f}(x) = \overline{g}(x)\, \overline{h}(x)$ in $\mathbb{Z}/2\mathbb{Z}[x]$

$\overline{f}(x) = X^3 + X + 1$ è irrid. in $\mathbb{Z}/2\mathbb{Z}[x]$

per l'esercizio precedente.

Domanda flash: fattorizzare (in $\mathbb{Q}[x]$)

$$f(x) = x^4 - 2x^3 + x - 1$$

- $f(x)$ non ha radici
- $\overline{f}(x) \in \mathbb{Z}/2\mathbb{Z}[x]$ è irriducibile

  $\overline{f}$ non ha radici

$\Rightarrow$ se si fattorizzasse, sarebbe prodotto di irriducibili di grado 2

$\Rightarrow$ sarebbe $\overline{f} = (x^2 + x + 1)^2$, che non è vero

Eisenstein $f = a_n x^n + \dots + a_0$, p primo. Se: $a_i \in \mathbb{Z}[x]$

- $p \nmid a_n$
- $p \mid a_{n-1}, p \mid a_{n-2}, \dots, p \mid a_0$
- $p^2 \nmid a_0$

$\Rightarrow f(x)$ irriducibile

$f(x) = x^n - 2$ è un esempio al quale questo criterio si applica! $(p = 2)$

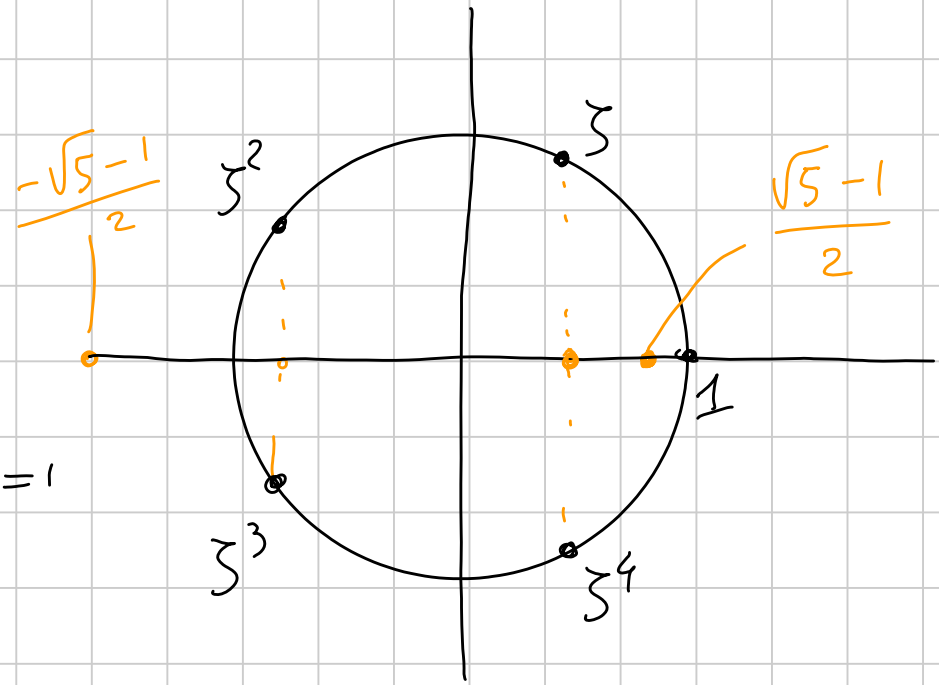
Esempio non banale p primo,

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

Dim. che $f(x)$ è irriducibile

Parentesi $\quad x^p - 1 = (x-1)(x^{p-1} + \dots + 1)$

Radici in $\mathbb{C}$:



Sia $\zeta \in \mathbb{C}$, $\zeta^p = 1$.
Allora

$$(\zeta^k)^p = (\zeta^p)^k = 1^k = 1$$

$$\zeta^4 = \bar{\zeta}$$

$$\bar{\zeta} = \zeta^{-1}$$

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

$$f(x+1) = \frac{\sum_{k=0}^{p} \binom{p}{k} x^k - 1}{x} = \frac{\sum_{k=1}^{p} \binom{p}{k} x^k}{x}$$

$$= \sum_{k=1}^{p} \binom{p}{k} x^{k-1}$$

Posso applicare Eisenstein con il primo p!

Infatti:

- termine di grado max: x^{p-1}
- gli altri coeff. sono $\binom{p}{k}$ con $1 \le k \le p-1$

$$\Rightarrow p \mid \binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$

- il termine noto è $\binom{p}{1} = p \not\equiv 0 \ (p^2)$

Guardiamo meglio $x^n - 2$. Come si fattorizza in $\mathbb{C}[x]$? E in $\mathbb{R}[x]$ (con $n=5$)?

$$p(x) = x^n - 2 = (x - \sqrt[n]{2})(x - \zeta\sqrt[n]{2}) \cdots (x - \zeta^{n-1}\sqrt[n]{2})$$

dove $\zeta = \exp\left(\frac{2\pi i}{n}\right)$

$$p(\sqrt[n]{2} \cdot x) = (\sqrt[n]{2}\,x)^n - 2 = 2x^n - 2 = 2(x^n - 1)$$

$$p(x) = x^5 - 2 \overset{\text{in } \mathbb{C}[x]}{=} (x - \sqrt[5]{2})(x - \zeta\sqrt[5]{2})(x - \zeta^2\sqrt[5]{2})(x - \zeta^3\sqrt[5]{2})(x - \zeta^4\sqrt[5]{2})$$

In $\mathbb{R}[x]$: $x - \sqrt[5]{2}$, $(x^2 - x\sqrt[5]{2}(\zeta + \zeta^4) + \sqrt[5]{4})$

$(x^2 - x\sqrt[5]{2}(\zeta^2 + \zeta^3) + \sqrt[5]{4})$

Oss. $1+\zeta+\zeta^2+\zeta^3+\zeta^4=0$

$\zeta^5-1=0 \qquad (\zeta-1)(1+\dots+\zeta^4)=0$

$\Rightarrow \quad \frac{1}{\zeta^2}+\frac{1}{\zeta}+1+\zeta+\zeta^2=0$

$1+\left(\zeta+\frac{1}{\zeta}\right)+\left(\zeta+\frac{1}{\zeta}\right)^2-2=0$

$(\zeta+\zeta^4)+(\zeta+\zeta^4)^2=1$

$$\left\{\begin{matrix}\zeta+\zeta^4,\\ \zeta^2+\zeta^3\end{matrix}\right\}=\left\{\frac{-1\pm\sqrt{5}}{2}\right\}$$

Un anello quoziente

$f(x)=x^3-5x^2+7x-3 \in \mathbb{Z}/5\mathbb{Z}[x]$

$A=\frac{\mathbb{Z}/5\mathbb{Z}[x]}{(f(x))}$ è uno s.v. su $\mathbb{Z}/5\mathbb{Z}$ di dimensione $=3$

- $\#A$ (come s.v. $A\simeq(\mathbb{Z}/5\mathbb{Z})^3$) $\#A=125$
- $\#A^\times$
- $\#\{a\in A \text{ divisori di zero}\}$
- $\#\{a\in A \text{ nilpotente}\}$

DEF A anello. $a \in A$ è detto NILPOTENTE se

$$\exists\, n \geq 0 \quad \text{t.c.} \quad a^n = 0$$

PROP Sia A un anello con $\#A < \infty$. Allora

$$A = A^\times \cup \{ a \in A \text{ divisore di } 0 \}$$

Dim. Prendiamo $a \in A$ non divisore di 0.

Consideriamo $a, a^2, a^3, a^4, \ldots$

$$\exists\, h < k \quad \text{t.c.} \quad a^h = a^k \quad \text{(qui si usa } A \text{ finito)}$$

$$\Rightarrow \quad a^h \cdot \left(1 - a^{k-h}\right) = 0 \quad \text{in } A$$

$$\Rightarrow \quad 1 - a^{k-h} = 0 \Rightarrow \quad a \cdot a^{k-h-1} = 1,$$

$$(a) \cdot \underbrace{\left(a \cdot \ldots \cdot a \cdot \left(1 - a^{k-h}\right)\right)}_{0,\ \text{perché } a \text{ non è div. di } 0} = 0$$

quindi a è invertibile, con inverso a^{k-h-1} ∎

Come sono fatti gli invertibili?

Quando accade che $\overline{a_0 + a_1 X + a_2 X^2} \in A$ è invertibile?

$\Leftrightarrow \quad \left(a_0 + a_1 X + a_2 X^2,\ f(X)\right) = 1 \quad \text{in } \mathbb{Z}/5\mathbb{Z}[X]$

$f(X) = (X-1)(X+2)(X-1) \quad \text{in } \mathbb{Z}/5\mathbb{Z}[X]$

$\| \quad X^3 - 5X^2 + 7X - 3 = X^3 + 2X + 2$

$f(X) \equiv (X-1)^2 (X+2) \quad \text{in } \mathbb{Z}/5\mathbb{Z}[X]$

$p(X) = a_0 + a_1 X + a_2 X^2$ è invertibile $\Leftrightarrow$

$\left(p(X), X-1\right) = \left(p(X), X+2\right) = 1$

$\Leftrightarrow \quad p(1) \not\equiv 0 \ (5), \quad p(-2) \not\equiv 0 \ (5)$

$\{\text{Divisori di } 0 \text{ in } A\} = \{p(X) : p(1) \equiv 0 \ (5)\}$

$\cup$

$\{p(X) : p(-2) \equiv 0 \ (5)\}$

$\#\{p(X) : p(1) = 0\} = 25$

$\#\{p(X) : p(-2) = 0\} = 25$

} spazi vettoriali di dimensione 2 su $\mathbb{Z}/5\mathbb{Z}$

$\#\{p(X) : p(1) = p(-2) = 0\} = 5$

$\quad \llcorner\ (X-1)(X+2) \cdot K \qquad K = 0, 1, 2, 3, 4$

$\#\{\text{Div. di } 0 \text{ in } A\} = 25 + 25 - 5 = 45$

$$\# A^\times = 125 - 45 = 80$$

Parentesi 2 $\quad (p(x), f(x)) = 1 \text{ in } K[x]$

Bézout $\Longrightarrow \quad 1 = a(x)p(x) + b(x)f(x) \text{ in } K[x]$

modulo $f(x) \Longrightarrow \quad 1 = \overline{a(x)} \cdot \overline{p(x)} \text{ in } K[x]/(f)$

Restano da contare i nilpotenti.

$p(x)$ t.c. si abbia

$$\exists n: \overline{p(x)}^n = 0 \iff \exists n: p(x)^n \in (f)$$

$$\iff \exists n: (x-1)^2(x+2) \mid p(x)^n$$

se $\deg p(x) \leq 2$ $\iff x-1, x+2 \mid p(x)$

$\iff p(x) = k \cdot (x-1)(x+2)$

Quindi ci sono 5 elementi nilpotenti

Algoritmo di Euclide fra polinomi

$$(x^4+x^3+1,\ x^2+1) \quad \text{in} \quad \mathbb{Q}[x]$$

$$x^4+x^3+1 = (x^2+1)(x^2+x-1) - x + 2$$

$$x^4+x^3-x^2+x^2+x-1$$

$$x^2+1 = (2-x)(\ \ \ \ ) + 5$$

$$-x-2$$

$$5 = (x^2+1) - (2-x)(-x-2)$$

$$= (x^2+1) - \Big((x^4+x^3+1) - (x^2+1)(x^2+x-1)\Big)(-x-2)$$

$$= (x^2+1)\Big(1 - (x+2)(x^2+x-1)\Big) - (x^4+x^3+1)$$

$$\Longrightarrow \quad 1 = (x^2+1)\left(\frac{1-(x+2)(x^2+x-1)}{5}\right) + \left(-\frac{1}{5}\right)(x^4+x^3+1)$$

Conclusione: in $\dfrac{\mathbb{Q}[x]}{(x^4+x^3+1)}$ la classe di x^2+1

è invertibile, e il suo inverso è la classe di

$$\left(\frac{1-(x+2)(x^2+x-1)}{5}\right)$$