

## polinomi irriducibili su $Q$ e $Z$

**TEOREMA 1** Siano  $p$  un primo e  $f \in Z[x]$  con  $\deg(f) > 0$ . Sia  $\bar{f} \in Z_p[x]$  il polinomio ottenuto da  $f$  riducendo i suoi coefficienti modulo  $p$ . Allora, se  $\bar{f}$  é irriducibile su  $Z_p$  e  $\deg(\bar{f}) = \deg(f)$ , il polinomio  $f$  é irriducibile su  $Q$ .

**DIM.** Supponiamo per assurdo  $f$  riducibile su  $Q$  e quindi su  $Z$ , per cui abbiamo

$$f = gh \quad \text{con} \quad g, h \in Z[x], \quad 1 \leq \deg(g), \deg(h) < \deg(f).$$

Riducendo modulo  $p$  i coefficienti di  $f, g, h$ , in  $Z_p[x]$  otteniamo

$$\bar{f} = \bar{g}\bar{h}$$

e, essendo  $\deg(f) = \deg(\bar{f})$ , deve essere

$$\deg(\bar{g}) = \deg(g) < \deg(\bar{f}), \quad \deg(\bar{h}) = \deg(h) < \deg(\bar{f}).$$

Quanto provato é assurdo perché  $\bar{f}$  é irriducibile su  $Z_p$ .

**OSSERVAZIONE 2** Se  $\bar{f}$  é riducibile su  $Z_p$ , per qualche primo  $p$ , non é detto che  $f$  sia riducibile su  $Q$ . Per esempio, prendiamo

$$f(x) = 21x^3 - 3x^2 + 2x + 8 \in Z[x].$$

Se riduciamo  $f$  modulo 2 otteniamo il polinomio

$$\bar{f}(x) = x^3 + x^2 = x^2(x + 1)$$

riducibile su  $Z_2$ . Se riduciamo  $f$  modulo 5 otteniamo il polinomio

$$\bar{f}(x) = x^3 + 2x^2 + 2x + 3$$

il quale, essendo di terzo grado e non avendo radici in  $Z_5$ , é irriducibile su  $Z_5$ . Da ciò segue che  $f$  é irriducibile su  $Q$ .

## Irriducibilità di polinomi ciclotomici

Se  $p$  è un primo positivo, il polinomio

$$\xi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1$$

si chiama  $p$ -esimo polinomio ciclotomico.

**TEOREMA 3** Per ogni primo  $p$ , il  $p$ -esimo polinomio ciclotomico è irriducibile su  $\mathbb{Q}$ .

**DIM.** Il polinomio

$$\begin{aligned} f(x) &= \xi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{p-2}x + p \end{aligned}$$

è irriducibile su  $\mathbb{Q}$  per il criterio di Eisenstein. Supponiamo che esista una fattorizzazione non banale

$$\xi_p(x) = g(x)h(x)$$

di  $\xi_p(x)$  su  $\mathbb{Q}$ . Allora

$$f(x) = \xi_p(x+1) = g(x+1)h(x+1)$$

è una fattorizzazione non banale su  $\mathbb{Q}$  di  $f$  e ciò è assurdo. Ne segue che il polinomio  $\xi_p(x)$  è irriducibile su  $\mathbb{Q}$ .

**ESERCIZIO 4** Sia  $p$  un intero primo positivo. Tenendo presente che

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

provare che non esiste alcun numero reale algebrico su  $\mathbb{Q}$  e avente come polinomio minimo il polinomio ciclotomico  $\xi_p(x)$ .

## fattorizzazione unica in $Z[x]$

**TEOREMA 5** Sia  $f(x) \in Z[x]$  un polinomio non nullo diverso da  $-1$  e da  $1$ . Allora  $f(x)$  può essere scritto nella forma

$$f(x) = b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x), \quad (1)$$

ove i  $b_i$  sono numeri primi e i  $p_i(x)$  sono polinomi irriducibili in  $Z[x]$ .

**DEFINIZIONE 6** Una decomposizione di  $f$  del tipo (1) si chiama *fattorizzazione di  $f$  in polinomi irriducibili*.

**TEOREMA 7** Siano

$$b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x)$$

e

$$c_1 c_2 \cdots c_t q_1(x) q_2(x) \cdots q_n(x)$$

due fattorizzazioni di  $f(x) \in Z[x]$  in polinomi irriducibili. Allora risulta  $s = t$ ,  $m = n$  ed esistono una permutazione  $\sigma \in S_s$  e una  $\tau \in S_m$  tali che

$$b_1 = \pm c_{\sigma(1)}, \dots, b_s = \pm c_{\sigma(s)},$$

$$p_1(x) = \pm q_{\tau(1)}(x), \dots, p_m(x) = \pm q_{\tau(m)}(x).$$