

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

**DEFINIZIONE 1** Un polinomio  $f \in Z[x]$  si dice *primitivo* se il massimo comune divisore dei suoi coefficienti non nulli é 1.

**PROPOSIZIONE 2 (lemma di Gauss)** *Il prodotto di due polinomi primitivi é un polinomio primitivo.*

**DIM.** Siano  $f, g \in Z[x]$  primitivi e supponiamo per assurdo che  $fg$  non lo sia. Esiste allora un primo  $p$  che divide il massimo comune divisore dei coefficienti non nulli di  $fg$  e possiamo considerare i polinomi  $\bar{f}, \bar{g}, \overline{fg} \in Z_p[x]$  riducendo modulo  $p$  i coefficienti di  $f, g, fg$ .

Dall'essere  $Z_p[x]$  un dominio di integritá, avendosi  $\bar{f}\bar{g} = \overline{fg} = 0$ , ricaviamo che o  $\bar{f} = 0$  oppure  $\bar{g} = 0$ . Ne segue che  $p$  divide tutti i coefficienti di  $f$  oppure tutti i coefficienti di  $g$  e ció é assurdo.

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

**TEOREMA 3** Sia  $f \in Z[x]$ . Se  $f$  é riducibile su  $Q$ , allora é riducibile anche su  $Z$ .

**DIM.** Supponiamo  $f = gh$  con  $g, h \in Q[x]$  e osserviamo che non é restrittivo supporre che  $f$  sia primitivo.

• Denotiamo con  $a$  un minimo comune multiplo dei denominatori dei coefficienti di  $g$  e con  $b$  quello dei denominatori dei coefficienti di  $h$ . Allora,  $abf = (ag)(bh)$ , e  $ag, bh \in Z[x]$ .

• Denotiamo con  $c_1$  il *MCD* dei coefficienti di  $ag$  e con  $c_2$  quello dei coefficienti di  $bh$ . Allora,  $ag = c_1g_1$  e  $bh = c_2h_1$ , ove  $g_1, h_1 \in Z[x]$ , sono polinomi primitivi, e abbiamo

$$abf = c_1c_2g_1h_1.$$

• Poiché  $f$  é primitivo, il massimo comune divisore dei coefficienti di  $abf$  é  $ab$ . Analogamente, poiché  $g_1h_1$  é primitivo (per il lemma di Gauss), il massimo comune divisore dei coefficienti di  $c_1c_2g_1h_1$  é  $c_1c_2$ . Ne segue che

$$ab = c_1c_2.$$

• Possiamo ora concludere che é

$$f = g_1h_1 \quad \text{con} \quad g_1h_1 \in Z[x]$$

e l'asserto é dimostrato.

**OSSERVAZIONE 4** Notiamo che la proposizione precedente non puó invertirsi. Per esempio, il polinomio  $5(x^2+1)$  é riducibile su  $Z$ , perché  $5$  e  $x^2+1$  sono elementi irriducibili di  $Z[x]$ , ma é irriducibile su  $Q$ .

**ESERCIZIO 5** Sia  $f(x) \in Z[x]$  un polinomio primitivo. Provare che  $f(x)$  é irriducibile su  $Z$  se, e solo se, é irriducibile su  $Q$ .

**TEOREMA 6 (criterio di Eisenstein)** Sia

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

un polinomio a coefficienti interi ed esista un primo  $p$  tale che

$$p|a_0, p|a_1, \dots, p|a_{n-1}; \quad p \nmid a_n; \quad p^2 \nmid a_0.$$

Allora  $f$  é irriducibile su  $Q$ .

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

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

Poniamo

$$g(x) = b_0 + \cdots + b_r x^r \quad \text{e} \quad h(x) = c_0 + \cdots + c_s x^s.$$

•  $p$  divide uno soltanto degli interi  $b_0, c_0$  perché  $p|a_0 = b_0c_0$  e  $p^2 \nmid a_0$ . Supponiamo

$$p|b_0 \quad \text{e} \quad p \nmid c_0.$$

Inoltre

$$p \nmid b_r$$

perché  $p \nmid a_n = b_r c_s$ .

• Sia  $t$  il piú piccolo intero tale che  $p \nmid b_t$  e osserviamo che é  $t > 0$ . Il coefficiente

$$a_t = b_t c_0 + b_{t-1} c_1 + \cdots + b_1 c_{t-1} + b_0 c_t$$

non é divisibile per  $p$  perché  $b_t c_0$  non é divisibile per  $p$ , mentre tutti gli altri addendi lo sono. Allora deve essere  $t = n$ . Questo significa che  $g$  ha grado  $n$  e ció é assurdo.

**ESERCIZIO 7** Sia  $n$  un intero positivo. Provare che il polinomio  $x^n - 2$  é irriducibile sul campo razionale e riducibile su quello reale.