0.1 Riducibilità di polinomi

Concludiamo lo studio degli anelli di polinomi affrontandone il problema della riducibilità.

Definizione

Sia R un dominio di integrità e sia $f(x) \in R[x]$ un polinomio non invertibile[1] e non nullo. Allora, $f(x)$ si dice irriducibile in $R[x]$ se ogni volta che esprimiamo $f(x)$ come un prodotto $f(x) = g(x)h(x)$ di polinomi $g(x), h(x) \in R[x]$, almeno uno fra $g(x)$ e $h(x)$ è invertibile. Se $f(x)$ non è irriducibile in $R[x]$, diciamo che $f(x)$ è riducibile in $R[x]$.

La riducibilità di un polinomio non è un fatto generale, ma dipende dal particolare dominio di integrità preso in esame: non ha alcun senso parlare di "polinomio irriducibile" senza specificare quale sia il dominio d'integrità considerato.

Esempio. Il polinomio $f(x) = 2x + 4$ è irriducibile in $\mathbb{Q}[x]$ ma riducibile in $\mathbb{Z}[x]$. Infatti, se fosse $f(x) = g(x)h(x)$, per la *Proposizione 1.1.1* si avrebbe $\deg^\star(f) = 1 = \deg^\star(g) + \deg^\star(h)$. Dunque, almeno uno fra $g(x)$ e $h(x)$ ha grado 0 e risulta quindi invertibile essendo $\mathbb{Q}$ un campo, da cui $f(x)$ è irriducibile in $\mathbb{Q}[x]$. D'altra parte, $2x + 4 = 2(x + 2)$ e né 2 né $x + 2$ sono elementi invertibili in $\mathbb{Z}[x]$, quindi $f(x)$ è riducibile in $\mathbb{Z}[x]$. $\square$

Nel caso in cui il dominio di integrità sia un campo $\mathbb{K}$, poiché ogni elemento non nullo di $\mathbb{K}$ è invertibile, un polinomio non costante $f(x) \in \mathbb{K}[x]$ è riducibile in $\mathbb{K}[x]$ se e solo se può essere espresso come prodotto di due polinomi non costanti di grado minore di $\deg^\star(f)$.

Esempio. Il polinomio $f(x) = x^2 + 1$ è irriducibile in $\mathbb{R}[x]$ ma riducibile in $\mathbb{C}[x]$. Infatti, se $f(x)$ fosse riducibile in $\mathbb{R}[x]$, per quanto appena detto esso sarebbe il prodotto di due termini di grado 1, il che è impossibile poiché $f(x)$ non ha radici reali. D'altra parte, sappiamo che $x^2 + 1 = (x + i)(x - i)$, dunque $f(x)$ è riducibile in $\mathbb{C}[x]$. $\square$

In generale, stabilire se un polinomio sia o meno irriducibile in un certo dominio di integrità è un problema complesso. Tuttavia, esistono alcuni casi particolari in cui ciò è molto semplice.

Teorema 1.5.1: Criterio del grado

Sia $\mathbb{K}$ un campo e sia $f(x) \in \mathbb{K}[x]$ un polinomio di grado 2 o 3. Allora, $f(x)$ è riducibile in $\mathbb{K}[x]$ se e solo se $f(x)$ ha una radice in $\mathbb{K}$.

Dimostrazione. Supponiamo che $f(x)$ sia riducibile in $\mathbb{K}[x]$. Allora, per definizione esistono $g(x), h(x) \in \mathbb{K}[x]$ non costanti di grado minore di $\deg^\star(f)$ tali che $f(x) = g(x)h(x)$. Poiché per ipotesi $\deg^\star(g) + \deg^\star(h) = \deg^\star(f) \leq 3$, almeno uno fra $g(x)$ e $h(x)$ ha grado 1, e senza perdita di generalità sia esso $g(x) = ax + b$. Essendo $\mathbb{K}$ un campo, $\alpha = -a^{-1}b \in \mathbb{K}$, da cui $g(\alpha) = a(-a^{-1}b) + b = 0_{\mathbb{K}}$. Dunque, $f(\alpha) = g(\alpha)h(\alpha) = 0_{\mathbb{K}}$, cioè α è una radice di $f(x)$.

Viceversa, supponiamo che esista $\alpha \in \mathbb{K}$ tale che $f(\alpha) = 0_{\mathbb{K}}$. Per il *Teorema di Ruffini* sappiamo che $(x - \alpha)$ divide $f(x)$, cioè $f(x) = (x - \alpha)q(x)$ per un opportuno $q(x) \in \mathbb{K}[x]$. Poiché $\deg^\star(q) = \deg^\star(f) - \deg^\star(x - \alpha) \geq 2 - 1 = 1$, si ha che $f(x)$ è riducibile in $\mathbb{K}[x]$. $\blacksquare$

Tale teorema è particolarmente comodo nel caso dei campi finiti, poiché per stabilire la riducibilità di $f(x) \in \mathbb{F}_p[x]$ è sufficiente verificare se $f(n) \equiv 0 \pmod{p}$ per $n = 0, 1, \dots, p - 1$.

Esempio. Il polinomio $f(x) = x^3 + x + 1$ è irriducibile in $\mathbb{F}_2[x]$ ma riducibile in $\mathbb{F}_3[x]$. Infatti, $f(0) \equiv f(1) \equiv 1 \not\equiv 0 \pmod{2}$ in $\mathbb{F}_2$, ma $f(1) = 3 \equiv 0 \pmod{3}$ in $\mathbb{F}_3$. $\square$

[1] Si intende rispetto al prodotto, cioè per la *Proposizione 1.1.2* prendiamo $f(x) \notin R^\times$.

Osserviamo che il *Teorema 1.5.1* vale solo nei campi, dunque non è applicabile in $\mathbb{Z}$. Inoltre, esistono polinomi riducibili di grado maggiore o uguale a 4 che non hanno radici.

Esempio. Entrambi i polinomi $f(x) = x^4 + 1$ e $g(x) = x^6 + 1$ non ammettono chiaramente radici reali. Tuttavia, osserviamo che $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$ e possiamo scomporre $x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$, dunque $f(x)$ e $g(x)$ sono riducibili in $\mathbb{R}[x]$. $\square$

Di qui in seguito ci concentreremo principalmente sul problema della riducibilità in $\mathbb{Z}[x]$.

Definizione

Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ un polinomio non nullo. Si definisce contenuto di f il valore di $\mathrm{MCD}(a_0, \dots, a_n)$. Un polinomio si dice primitivo se il suo contenuto è 1.

Esempio. Il polinomio $f(x) = 2x^2 + 3x + 4$ è primitivo perché $\mathrm{MCD}(2, 3, 4) = 1$. D'altra parte, il polinomio $g(x) = 2x^2 + 4$ non è primitivo poiché $\mathrm{MCD}(2, 0, 4) = 2 \neq 1$. $\square$

Osserviamo che presi i due polinomi primitivi $f(x) = x + 1$ e $g(x) = 2x + 3$, anche il loro prodotto $f(x)g(x) = 2x^2 + 5x + 3$ è primitivo, poiché il suo contenuto è $\mathrm{MCD}(2, 5, 3) = 1$. Questo è un fatto generale, come dimostrato dal lemma seguente.

Lemma 1.5.2: Lemma di Gauss

Il prodotto di due polinomi primitivi è un polinomio primitivo.

Dimostrazione. Siano $f(x)$, $g(x) \in \mathbb{Z}[x]$ polinomi primitivi, e supponiamo per assurdo che $f(x)g(x)$ non sia primitivo. Allora, esiste p primo che divide tutti i coefficienti di $f(x)g(x)$, cioè $f(x)g(x) \equiv 0$ in $\mathbb{F}_p[x]$. Poiché $\mathbb{F}_p[x]$ è un dominio di integrità, deve essere $f(x) \equiv 0$ oppure $g(x) \equiv 0$, da cui p divide tutti i coefficienti di almeno uno fra $f(x)$ e $g(x)$, e tale polinomio risulta quindi non primitivo, assurdo. Dunque, $f(x)g(x)$ è primitivo. $\blacksquare$

Esiste una stretta relazione tra la riducibilità in $\mathbb{Z}[x]$ e quella in $\mathbb{Q}[x]$.

Teorema 1.5.3

Sia $f(x) \in \mathbb{Z}[x]$ un polinomio irriducibile in $\mathbb{Z}[x]$. Allora, $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

Dimostrazione. Supponiamo per assurdo che $f(x)$ sia riducibile in $\mathbb{Q}[x]$. Allora, esistono $g(x)$, $h(x) \in \mathbb{Q}[x]$ non costanti tali che $f(x) = g(x)h(x)$, dove, a meno di dividere $g(x)$ per il contenuto di f, possiamo assumere senza perdita di generalità che $f(x)$ sia primitivo. Siano a e b il minimo comune multiplo dei denominatori dei coefficienti di $g(x)$ e $h(x)$, rispettivamente, così che $ag(x)$ e $bh(x)$ siano polinomi a coefficienti interi. Detti c_1 e c_2 il contenuto di $ag(x)$ e $bh(x)$, rispettivamente, si ha che $ag(x) = c_1 g'(x)$ e $bh(x) = c_2 h'(x)$, dove $g'(x)$ e $h'(x)$ sono polinomi primitivi. Poiché $abf(x) = ag(x)\, bh(x) = c_1 c_2\, g'(x)h'(x)$ e per il *Lemma 1.5.2* anche $g'(x)h'(x)$ è primitivo, deve essere $ab = c_1 c_2$. Dunque, si ha che $f(x) = g'(x)h'(x)$ dove $g'(x)$, $h'(x) \in \mathbb{Z}[x]$, cioè $f(x)$ è riducibile in $\mathbb{Z}[x]$, assurdo. $\blacksquare$

Sebbene $\mathbb{Q}$ sia un campo più grande di $\mathbb{Z}$, tale teorema mostra che esso non è abbastanza grande per permettere di scomporre in $\mathbb{Q}[x]$ un polinomio irriducibile in $\mathbb{Z}[x]$, ed è quindi necessario passare a campi ancora più grandi quali $\mathbb{R}$ e $\mathbb{C}$. Inoltre, la dimostrazione mostra che se un polinomio $f(x) \in \mathbb{Z}[x]$ è riducibile in $\mathbb{Q}[x]$, allora esso è riducibile anche in $\mathbb{Z}[x]$.

Esempio. Sia $f(x) = 6x^2 - 5x + 1 = (3x - \frac{3}{2})(2x - \frac{2}{3})$ un polinomio riducibile in $\mathbb{Q}[x]$. Utilizzando la notazione del *Teorema 1.5.3*, definiamo $g(x) = (3x - \frac{3}{2})$ e $h(x) = (2x - \frac{2}{3})$. Allora, $a = 2$ e $b = 3$, da cui $ag(x) = 6x - 3$ e $bh(x) = 6x - 2$. Dunque, $c_1 = \mathrm{MCD}(6, 3) = 3$ e $c_2 = \mathrm{MCD}(6, 2) = 2$, da cui $g'(x) = 2x - 1$ e $h'(x) = 3x - 1$ sono polinomi primitivi e $f(x) = g'(x)h'(x) = (2x - 1)(3x - 1)$ risulta quindi riducibile in $\mathbb{Z}[x]$. $\square$

Sketch del capitolo: riduzione mod p, Eisenstein, polinomi ciclotomici, tanti esempi, e tutto quello che Weigel dà per scontato sia stato fatto ad Algebra 1.