

divisibilità in anelli di polinomi

ESERCIZIO 1 Sia D un dominio di integrità unitario, $c \in D$ una costante non nulla e $f \in D[x]$ un polinomio che divide c . Allora f è costante.

PROPOSIZIONE 2 Sia D un dominio di integrità unitario. Allora l'insieme degli elementi invertibili di $D[x]$ coincide con l'insieme $U(D)$ degli elementi invertibili di D .

DIM. Poiché D e $D[x]$ hanno la stessa unità, abbiamo $U(D) \subseteq U(D[x])$. D'altra parte abbiamo:

$$f \in U(D[x]) \Rightarrow \text{esiste } g \in D[x] \text{ tale che } fg = 1 \Rightarrow f|1 \text{ e } g|1.$$

Ne segue che f, g sono costanti non nulle e, quindi, elementi invertibili in D .

OSSERVAZIONE 3 Le due precedenti proprietà non sono in generale vere se D non è un dominio di integrità. Per esempio, in $Z_4[x]$ abbiamo

$$(2x + 1)(2x + 1) = 4x^2 + 4x + 1 = 1 \Rightarrow (2x + 1)^{-1} = 2x + 1,$$

cioè $2x + 1$, che non è una costante, divide la costante 1 ed è invertibile.

PROPOSIZIONE 4 Siano f, g due polinomi non nulli associati a coefficienti in un dominio di integrità unitario D . Allora f e g hanno lo stesso grado.

DIM. Abbiamo:

$$g = fh \text{ e } f = gh' \Rightarrow f = fhh' \Rightarrow hh' = 1$$

$$\Rightarrow h \text{ è una costante non nulla} \Rightarrow \deg(f) = \deg(g).$$

divisibilità in anelli di polinomi

OSSERVAZIONE 5 Anche la precedente proposizione non é in generale invertibile, nel senso che polinomi dello stesso grado possono non essere associati. Per esempio in $Z[x]$ i polinomi x^2 e $5x^2$ non sono associati.

Osserviamo che x^2 e $5x^2$ sono, invece, associati in $Q[x]$.

ESERCIZIO 6 Sia K un campo. Generalizzare al caso dei polinomi su K l'algoritmo di Euclide delle divisioni successive per il calcolo di un massimo comune divisore.

OSSERVAZIONE 7 L'anello dei polinomi su un anello principale puó non essere principale. Un esempio a proposito é dato dall'anello Z degli interi. Consideriamo infatti in $Z[x]$ l'ideale

$$I = \{2b + xa(x) \quad : \quad a(x) \in Z[x], b \in Z\}$$

e supponiamo $I = (h(x))$. In queste ipotesi abbiamo

$$2 = h(x)f(x) \quad \text{e} \quad x = h(x)g(x);$$

$$0 = \deg(2) = \deg(h) + \deg(f) \Rightarrow \deg(h) = \deg(f) = 0 \Rightarrow h, f \in Z.$$

D'altra parte

$$2 = hf \Rightarrow h = \pm 1 \quad \text{oppure} \quad h = \pm 2$$

e, poiché $1 \notin I$, deve essere $h = \pm 2$. Le ultime uguaglianze implicano che $x = \pm 2g(x)$, che é un assurdo; cosí I non puó essere principale.

radici di un polinomio

Sia A un anello commutativo unitario e

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

un polinomio di grado n a coefficienti in A .

DEFINIZIONE 8 Un'equazione del tipo $f(x) = 0$ si chiama *equazione algebrica di grado n* e un elemento $c \in A$ si dice *radice* o *zero* di f se risulta $f(c) = 0$.

PROPOSIZIONE 9 (teorema del resto) Siano f un polinomio a coefficienti in un anello commutativo unitario A e c un elemento di A . Allora esiste un unico polinomio $q \in A[x]$ tale che $f = (x - c)q + f(c)$.

DIM. Poiché $(x - c)$ ha coefficiente direttore 1, che è invertibile in A , possiamo dividere f per $(x - c)$ e da ciò segue facilmente l'asserto.

COROLLARIO 10 (teorema di Ruffini) Sia f un polinomio a coefficienti in anello commutativo unitario A . Allora c è una radice di f se, e solo se, $(x - c)$ divide f .

COROLLARIO 11 Siano

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

un polinomio di grado positivo n a coefficienti in un anello commutativo unitario A , e

$$q(x) = q_0 + q_1x + q_2x^2 + \cdots + q_{n-1}x^{n-1}$$

il quoziente della divisione di f per $(x - c)$, $c \in A$. Allora risulta:

$$q_{n-1} = a_n, \quad q_{n-2} = a_{n-1} + cq_{n-1}, \quad \dots,$$

$$q_1 = a_2 + cq_2, \quad q_0 = a_1 + cq_1, \quad a_0 + cq_0 = f(c).$$

divisione veloce

OSSERVAZIONE 12 Il corollario 11 permette di semplificare l'algoritmo della divisione di f per $(x - c)$. Si può infatti eseguire sinteticamente questa divisione usando lo schema seguente

$$\begin{array}{c|cccc|c}
 & a_n & a_{n-1} & \cdots & a_1 & a_0 \\
 c & & cq_{n-1} & \cdots & cq_1 & cq_0 \\
 \hline
 & a_n = q_{n-1} & a_{n-1} + cq_{n-1} = q_{n-2} & \cdots & a_1 + cq_1 = q_0 & a_0 + cq_0 = f(c)
 \end{array}$$

Per esempio, lo schema da usare per trovare il quoziente $q(x)$ e il resto $r(x)$ della divisione fra $x^3 - 3x^2 + 7x - 10$ e $x - 4$ é

$$\begin{array}{c|ccc|c}
 & 1 & -3 & 7 & -10 \\
 4 & & 4 & 4 & 44 \\
 \hline
 & 1 & 1 & 11 & 34
 \end{array}$$

da cui si ricava $q(x) = x^2 + x + 11$ e $r(x) = 34$.

divisibilità in anelli di polinomi

PROPOSIZIONE 13 Siano D un dominio di integrità unitario, $f \in D[x]$ e c_1, c_2, \dots, c_n radici a due a due distinte di f . Allora

$$(x - c_1)(x - c_2) \cdots (x - c_n) \text{ divide } f.$$

DIM. Per $n = 1$ l'asserto é vero, riducendosi al teorema di Ruffini. Se supponiamo $n > 1$ e procediamo per induzione su n , abbiamo:

$$f = (x - c_1)q \text{ e, per ogni } i > 1, f(c_i) = (c_i - c_1)q(c_i) = 0$$

$$\Rightarrow q(c_i) = 0 \Rightarrow q = (x - c_2)(x - c_3) \cdots (x - c_n)h, h \in D[x]$$

$$\Rightarrow f = (x - c_1)(x - c_2) \cdots (x - c_n)h.$$

COROLLARIO 14 Siano D un dominio di integrità unitario, $f \in D[x]$ e $\deg(f) = n > 0$. Allora f possiede al più n radici in D .

DIM. Se c_1, c_2, \dots, c_m sono radici distinte di f abbiamo

$$(x - c_1)(x - c_2) \cdots (x - c_m) \mid f \Rightarrow m \leq \deg(f).$$

OSSERVAZIONE 15 Nelle due proposizioni precedenti, l'ipotesi che D sia dominio di integrità é essenziale. Per esempio, se consideriamo il polinomio

$$f(x) = x^2 + x \in Z_6[x],$$

abbiamo:

- $f(0) = f(3) = 0$ e f non é del tipo $f(x) = x(x - 3)g(x)$;
- oltre alle radici 0 e 3, f ha anche le radici 2 e 5.

principio d'identità dei polinomi

ESERCIZIO 16 Trovare in Z_6 tutte le radici del polinomio $x^2 + 2x + 4$.

ESERCIZIO 17 Provare che nel campo Z_p , p primo, 1 e $p - 1$ sono gli unici elementi che coincidono col proprio inverso.

TEOREMA 18 (principio di identità dei polinomi) Se D è un dominio di integrità unitario infinito, allora in $D[x]$ vale il principio di identità dei polinomi; cioè, se $f, g \in D[x]$, allora $f = g$ se, e solo se, la funzione polinomiale di f è uguale a quella di g .

DIM. La prima implicazione è ovvia. Per la seconda, se supponiamo $f \neq g$, abbiamo:

$$\bar{f} = \bar{g} \Rightarrow f(a) = g(a) \text{ per ogni } a \in D$$

$$\Rightarrow (f - g)(a) = f(a) - g(a) = 0 \text{ per ogni } a \in D \Rightarrow$$

esistono in D un numero di radici di $f - g$ maggiore di $\deg(f - g)$

$$\Rightarrow f - g = 0 \Rightarrow f = g \Rightarrow \text{assurdo.}$$

polinomi irriducibili e primi

Sia D un dominio di integritá unitario.

DEFINIZIONE 19 Sia f un polinomio non nullo a coefficienti in D . Si dice che f é *irriducibile su D* se f é un elemento irriducibile di $D[x]$, cioè se non é invertibile in $D[x]$ e

$$f = gh \text{ con } g, h \in D[x] \Rightarrow g \text{ o } h \text{ e' invertibile in } D[x].$$

Se f non é irriducibile, si dice *riducibile*. Analogamente, si dice che f é *primo su D* se f é un elemento primo di $D[x]$, cioè se non é invertibile in $D[x]$ e

$$f \mid gh \text{ con } g, h \in D[x] \Rightarrow f \mid g \text{ o } f \mid h.$$

PROPOSIZIONE 20 Sia K un campo. Allora un polinomio $f \in K[x]$ é irriducibile su K se, e solo se, é un elemento primo dell'anello $K[x]$.

TEOREMA 21 Siano K un campo e $f \in K[x]$. Allora (f) é un ideale massimale in $K[x]$ se, e soltanto se, f é irriducibile su K .

DIM. Supponiamo (f) massimale in $K[x]$ e $f = gh$ con $g, h \in K[x]$. In queste ipotesi abbiamo $(f) \subseteq (g)$ e quindi

$$(f) = (g) \quad \text{oppure} \quad (g) = K[x].$$

Nel primo caso abbiamo $\deg(f) = \deg(g)$ e h é una costante. Nel secondo caso g é una costante e $\deg(f) = \deg(h)$. Ne segue che f é irriducibile.

Supponiamo ora f irriducibile e sia $I = (g)$ un ideale di $K[x]$ che contiene (f) . Allora esiste $h \in K[x]$ tale che $f = gh$ e, essendo f irriducibile abbiamo

$$g = \text{costante} \quad \text{oppure} \quad h = \text{costante}.$$

Nel primo caso risulta $I = K[x]$, nel secondo $(f) = (g)$. Ne segue che I é massimale.

polinomi irriducibili e primi

ESERCIZIO 22 *Provare che un polinomio di primo grado a coefficienti in un campo K ha una radice in K ed é ivi irriducibile.*

PROPOSIZIONE 23 *Sia K un campo. Ogni polinomio di grado positivo a coefficienti in K é prodotto di polinomi irriducibili su K .*

PROPOSIZIONE 24 *Sia D un dominio di integritá unitario. Allora x é un elemento primo in $D[x]$.*

DIM. Supponiamo $x|fg$, con $f, g \in D[x]$ e

$$f(x) = a_0 + a_1x + \dots, \quad g(x) = b_0 + b_1x + \dots$$

Allora, deve essere $a_0b_0 = 0$ e essendo D un dominio di integritá, abbiamo $a_0 = 0$ o $b_0 = 0$. Nel primo caso $x|f$, nel secondo $x|g$ e resta cosí provato che x é primo.

PROPOSIZIONE 25 *Sia D un dominio di integritá unitario tale che (x) sia un ideale massimale di $D[x]$. Allora D é un campo.*

DIM. Sia $a \in D^*$ e osserviamo che

$$a \notin (x) = \{xf(x) : f \in D[x]\}$$

e quindi (x) é propriamente contenuto nell'ideale (a, x) , pertanto deve essere $(a, x) = A[x]$. Allora devono esistere due polinomi

$$h(x) = h_0 + h_1x + \dots \quad e \quad k(x) = k_0 + k_1x + \dots$$

tali che $1 = ah(x) + xk(x)$, da cui segue che $ah_0 = 1$, cioè a é invertibile.

PROPOSIZIONE 26 *Sia A un anello commutativo unitario tale che $A[x]$ sia principale. Allora A é un campo.*

DIM. A é sottoanello di $A[x]$ e quindi é un dominio di integritá. Allora l'ideale principale (x) , essendo x primo e $A[x]$ principale, risulta massimale in $A[x]$. Ne segue che A é un campo.

polinomi irriducibili e primi

PROPOSIZIONE 27 Siano K un campo ed $f \in K[x]$ un polinomio irriducibile di grado maggiore di 1. Allora K non contiene radici di f .

DIM. Supponiamo per assurdo che K contenga una radice c di f . Allora avremmo:

$$f = (x - c)q \Rightarrow \deg(f) = 1 + \deg(q) > 1 \Rightarrow \deg(q) > 0 \\ \Rightarrow f \text{ riducibile, un assurdo.}$$

ESERCIZIO 28 Provare che:

- il polinomio $x^2 - 2$ é irriducibile su \mathbb{Q} e riducibile su \mathbb{R} ;
- il polinomio $x^2 + 4$ é irriducibile su \mathbb{R} e su \mathbb{Q} .

OSSERVAZIONE 29 In generale, la proposizione 27 non si puó invertire; per esempio il polinomio $(x^2 - 2)(x^2 - 3)$, pur essendo riducibile sul campo \mathbb{Q} dei razionali, non ha radici razionali. Essa puó invece invertirsi nel caso dei gradi 2 e 3.

PROPOSIZIONE 30 Siano K un campo, $f \in K[x]$ di grado 2 o 3 e si supponga che f non abbia radici in K . Allora f é irriducibile su K .

DIM. Supponiamo per assurdo che f sia riducibile. Allora

$$f = gh \text{ con } \deg(g) > 0 \text{ e } \deg(h) > 0$$

$$\Rightarrow \deg(f) = \deg(g) + \deg(h) \in \{2, 3\}$$

$$\Rightarrow g \text{ o } h \text{ ha grado uguale ad 1, per esempio } g$$

$$\Rightarrow \text{esiste } c \in K \text{ tale che } g(c) = 0 \Rightarrow f(c) = 0,$$

un assurdo.

ESERCIZIO 31 Sia K un campo. Provare che un polinomio $f \in K[x]$ di grado 2 o 3 é riducibile su K se, e solo se, f ha una radice in K .