

ideali di un anello

DEFINIZIONE 1 Un ideale sinistro (risp. destro, bilatero) H si dice *principale* se può essere generato da un solo elemento, cioè se esiste $x \in H$ tale che $(x)_s = H$ (risp. $(x)_d = H$, $(x) = H$).

DEFINIZIONE 2 Un dominio di integrità unitario A si chiama *anello principale* se tutti i suoi ideali sono principali.

DEFINIZIONE 3 Un ideale sinistro (risp. destro, bilatero) proprio H di A si dice *massimale* se non è propriamente contenuto in alcun ideale sinistro (risp. destro, bilatero) diverso da A .

TEOREMA 4 (teorema di Krull) Sia A un anello unitario. Allora ogni ideale sinistro proprio H è contenuto in almeno un ideale sinistro massimale.

DEFINIZIONE 5 Sia A un anello commutativo. Un ideale proprio H di A si dice *primo* se vale la seguente proprietà:

$$a, b \in A, \quad ab \in H \Rightarrow a \in H \quad \text{oppure} \quad b \in H .$$

ideali di $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Z}_n, +, \cdot)$

PROPOSIZIONE 6 Ogni ideale H di $(\mathbb{Z}, +, \cdot)$ é del tipo $m\mathbb{Z}$, ove m é il minimo fra gli interi non negativi contenuti in H . Ne segue che \mathbb{Z} é un anello principale.

DIM. Segue dall'osservazione che $m\mathbb{Z}$ é un ideale e che ogni ideale é un sottogruppo di $(\mathbb{Z}, +)$.

ESERCIZIO 7 Sia $m\mathbb{Z}$ un ideale dell'anello \mathbb{Z} degli interi. Provare che $m\mathbb{Z}$ é un ideale primo se, e solo se, m é un primo. Provare inoltre che un ideale di \mathbb{Z} é primo se, e solo se, é massimale.

PROPOSIZIONE 8 Ogni ideale H di $(\mathbb{Z}_n, +, \cdot)$ é del tipo

$$\langle h \rangle = \{0, h, 2h, \dots, (k-1)h\},$$

ove h e k sono interi tali che $n = hk$.

DIM. Segue dall'osservazione che $\langle h \rangle$ é un ideale e che ogni ideale é un sottogruppo di $(\mathbb{Z}_n, +)$.

anelli di polinomi

Sia A un anello commutativo unitario.

DEFINIZIONE 9 Si chiama *polinomio a coefficienti in A nella indeterminata x* un'espressione formale del tipo

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

ove $a_0, a_1, a_2, \dots, a_n$ sono elementi di A e si dicono *coefficienti* di $a(x)$. Il coefficiente a_0 si chiama anche *termine noto* di $a(x)$. Se a_n è diverso da zero, l'intero n prende il nome di *grado* di $a(x)$ e si denota con $\deg(a(x))$ o $\deg(a)$. Nel caso in cui il polinomio $a(x)$ ha grado n , l'elemento a_n si chiama *coefficiente* o *parametro direttore* di $a(x)$ e, se è $a_n = 1$, il polinomio si dice *monico*. L'insieme di tutti i polinomi a coefficienti in A si denota con $A[x]$.

Alcune osservazioni:

- gli elementi non nulli dell'anello A sono polinomi di grado zero;
- lo zero dell'anello A è un polinomio (*polinomio nullo*) e risulta l'unico polinomio per cui non è definito il grado;
- due polinomi

$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$
sono uguali se, e solo se,

$$n = m \quad \text{e} \quad a_0 = b_0, a_1 = b_1, a_2 = b_2, \dots, a_n = b_n,$$

in particolare un polinomio è il polinomio nullo se, e solo se, tutti i suoi coefficienti sono uguali a zero.

funzioni polinomiali

DEFINIZIONE 10 Se $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ é un polinomio a coefficienti in A , la funzione

$$\bar{a} : A \rightarrow A$$

definita da

$$\bar{a}(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n, \quad \text{per ogni } c \in A,$$

si chiama *funzione polinomiale di $a(x)$* . Di solito, se $a(x)$ é un polinomio e c un elemento di A , con abuso di notazione, si scrive $a(c)$ in luogo di $\bar{a}(c)$ e si dice che l'elemento $a(c)$ é il *valore di $a(x)$ su c* . Si dice, poi, che in $A[x]$ vale il *principio di identità dei polinomi* se accade che due polinomi di $A[x]$ sono uguali se, e solo se, sono uguali le loro funzioni polinomiali.

OSSERVAZIONE 11 Il Lettore ricorderá dal corso di *Analisi matematica I* che in $Z[x]$, $Q[x]$, $R[x]$, $C[x]$ vale il principio di identità dei polinomi. Proveremo nel seguito che tale principio vale in $A[x]$, per ogni dominio d'integritá unitario infinito K .

OSSERVAZIONE 12 Il polinomio $x^2 - x$ a coefficienti in Z_2 ha funzione polinomiale nulla, pur non essendo il polinomio nullo. Abbiamo cosí che in $Z_2[x]$ non vale il principio di identità dei polinomi.

anelli di polinomi

Se

$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ e $b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$,
sono elementi di $A[x]$, poniamo

$a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_t + b_t)x^t$,
ove t é il piú grande fra gli interi n e m , e

$$a(x)b(x) = \sum_{h=0}^{n+m} \left(\sum_{i+j=h} a_i b_j \right) x^h.$$

DEFINIZIONE 13 La struttura algebrica $A[x] = (A[x], +, \cdot)$ é un anello commutativo unitario, che si chiama *l'anello dei polinomi nell'indeterminata x a coefficienti in A* . E' facile verificare che A é sottoanello unitario di $A[x]$ e che A e $A[x]$ hanno la stessa unitá. Gli elementi di A si chiamano *polinomi costanti*.

ESERCIZIO 14 *Provare che l'anello $A[x]$ é generato da A e da x .*

Osserviamo esplicitamente che la scelta del simbolo x usato per denotare l'indeterminata con cui abbiamo costruito $A[x]$ é del tutto arbitraria nel senso della seguente proposizione.

PROPOSIZIONE 15 *Siano $A[x]$ e $A[y]$ gli anelli dei polinomi a coefficienti in A nelle indeterminate x e y , rispettivamente. Allora l'applicazione*

$\varphi : a_0 + a_1x + \cdots + a_nx^n \in A[x] \rightarrow a_0 + a_1y + \cdots + a_ny^n \in A[y]$
é l'unico isomorfismo tra $A[x]$ e $A[y]$ tale che

$$\varphi(c) = c \text{ per ogni } c \in A \text{ e } \varphi(x) = y.$$

anelli di polinomi

Sia A un anello commutativo unitario. In $A[x]$ valgono le seguenti proprietà:

- $\deg(f) = \deg(-f)$.
- $f \neq -g \Rightarrow \deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.
- $fg \neq 0 \Rightarrow \deg(fg) \leq \deg(f) + \deg(g)$.
- Siano f, g polinomi non nulli i cui parametri direttori non siano entrambi divisori dello zero. Allora $fg \neq 0$ e

$$\deg(fg) = \deg(f) + \deg(g).$$

- Se A è un dominio di integrità, allora $A[x]$ è un dominio di integrità.

OSSERVAZIONE 16 L'anello dei polinomi su A , specialmente quando A è un campo, presenta molte analogie con l'anello Z degli interi; alcune di queste sono evidenti nelle definizioni e nei risultati che seguono.

DEFINIZIONE 17 Siano $f, g \in A[x]$ con $g \neq 0$. Si dice che per la coppia (f, g) vale l'algoritmo della divisione se esiste in $A[x]$ un'unica coppia di polinomi (q, r) tali che

$$f = gq + r, \quad \text{con } r = 0 \text{ oppure } \deg(r) < \deg(g).$$

In queste ipotesi, q si dice *quoziente* e r *resto* della divisione fra f e g .

divisione tra polinomi

PROPOSIZIONE 18 Siano $f, g \in A[x]$, $g \neq 0$ e il parametro direttore di g sia invertibile. Supponiamo che

$$f = gq + r, \quad \text{con } r = 0 \text{ oppure } \deg(r) < \deg(g),$$

$$f = gq' + r', \quad \text{con } r' = 0 \text{ oppure } \deg(r') < \deg(g).$$

Allora risulta $q = q'$ e $r = r'$.

DIM. • $gq + r = gq' + r' \Rightarrow g(q - q') = r' - r.$

• $r \neq r' \Rightarrow q \neq q' \Rightarrow \deg(r' - r) = \deg(g) + \deg(q - q') \geq \deg(g)$ e $\deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(g)$, assurdo.

• $r = r' \Rightarrow g(q - q') = 0 \Rightarrow q - q' = 0 \Rightarrow q = q'.$

TEOREMA 19 Siano $f, g \in A[x]$, $g \neq 0$ e il parametro direttore di g sia invertibile. Allora per (f, g) vale l'algoritmo della divisione.

DIM. Supponiamo $\deg(f) = n$, $\deg(g) = m$ e poniamo

$$f = a_0 + a_1x + \dots + a_nx^n, \quad g = b_0 + b_1x + \dots + b_mx^m.$$

• I casi $f = 0$; $f \neq 0$ e $n < m$; $n = m = 0$ sono banali.

• Se supponiamo $n \geq m$ e $n > 0$, possiamo procedere per induzione su n ; abbiamo così :

$\deg(a_nb_m^{-1}x^{n-m}g) = n$ e il parametro direttore di $(a_nb_m^{-1}x^{n-m}g)$ é a_n

$\Rightarrow f_1 = f - a_nb_m^{-1}x^{n-m}g$ ha grado minore di n o é nullo

\Rightarrow per (f_1, g) vale l'algoritmo della divisione

$\Rightarrow f_1 = gq_1 + r_1$ con $\deg(r_1) < \deg(g)$ o $r_1 = 0 \Rightarrow$

$$f = gq_1 + r_1 + a_nb_m^{-1}x^{n-m}g = g \underbrace{(q_1 + a_nb_m^{-1}x^{n-m})}_q + \underbrace{r_1}_r.$$

divisione tra polinomi

COROLLARIO 20 Se K é un campo, l'algoritmo della divisione vale per ogni coppia di polinomi (f, g) con $g \neq 0$.

OSSERVAZIONE 21 Notiamo che, nel corso della dimostrazione della proposizione precedente, il procedimento usato per trovare il quoziente e il resto della divisione tra f e g non é altro che l'usuale *algoritmo della divisione*, noto al Lettore dalle scuole medie. Per esempio, la procedura per il calcolo del quoziente $q(x)$ e del resto $r(x)$ della divisione in $Q[x]$ tra i polinomi $f(x) = 3x^4 + x^3 + 2x^2 + 1$ e $g(x) = 2x^2 + 2x + 1$ restituisce come risultato

$$q(x) = \frac{3}{2}x^2 - x + \frac{5}{4}, \quad r(x) = -\frac{3}{2}x - \frac{1}{4}.$$

OSSERVAZIONE 22 L'algoritmo e lo schema ricordati nell'esempio precedente valgono su un campo arbitrario. Per esempio, la procedura per il calcolo del quoziente $q(x)$ e del resto $r(x)$ della divisione in $Z_5[x]$ di $3x^4 + x^3 + 2x^2 + 1$ per $2x^2 + 2x + 1$ é formalmente la stessa che abbiamo usato in $Q[x]$; bisogna solo tener presente che questa volta le operazioni sono quelle di Z_5 . Abbiamo cosí

$$\begin{array}{r} 3x^4 + x^3 + 2x^2 + 1 \\ \underline{3x^4 + 3x^3 + 4x^2} \\ 3x^3 + 3x^2 + 1 \\ \underline{3x^3 + 3x^2 + 4x} \\ x + 1 \end{array} \quad \begin{array}{l} : 2x^2 + 2x + 1 \\ \hline 4x^2 + 4x \end{array}$$

e quindi

$$q(x) = 4x^2 + 4x, \quad r(x) = x + 1.$$