Corso:Algebra Anelli (Unimib)/Anelli/Polinomi

1 Polinomi come successioni

Sia $(A, +, \cdot)$ un anello commutativo.

Definizione (270 Polinomio)

Si dice *polinomio sull'anello* A una successione $(a_0, a_1, \dots, a_i, \dots,)$ di elementi di A che sia definitivamente nulla, cioè tale che a partire da un certo posto in poi, $a_i = 0_A$.

Gli elementi a_0, a_1, a_i sono i *coefficienti* del polinomio.

Definizione (271 Somma e prodotto di polinomi)

Data la successione $(a_0, a_1, a_i, \dots)$ e $(b_0, b_1, b_i, \dots)$ definiamo la *somma* di polinomi come la successione $(a_0 + b_0, a_1 + b_1, \dots, a_i + b_i, \dots)$.

Prese due successioni definitivamente nulle come sopra, si definisce *prodotto* di polinomi la successione

$$(a_0, a_1, a_i) \cdot (b_0, b_1, b_i) = (a_0 * b_0, a_0 * b_1 + a_1 * b_0, \sum_{h=0}^{i} a_h * b_{i-h}, \dots$$

Senza imporre che la successione sia definitivamente nulla si ha una serie formale su A .

2 Anello dei polinomi

Proposizione (272)

L'insieme di tutti i polinomi su A con le operazioni di somma e prodotto sopra definite è un anello commutativo.

Dimostrazione

Basta verificare che si ha un gruppo abeliano rispetto alla somma, che il prodotto è commutativo e che il prodotto è associativo, che valgono le proprietà distributive e che lo zero e l'unità sono presenti. Lo zero è la successione identicamente nulla, cioè $0_A, 0_A, \dots, 0_A, \dots$; l'unità è la successione $(1_A, 0_A, \dots, 0_A)$.

3 Polinomi come espressioni formali

Due polinomi coincidono quando sono uguali termine a termine.

Per ottenere la rappresentazione usuale dei polinomi scegliamo un simbolo x (indeterminata). Se $A_i = 0_A \forall i > m$ e $a_m \neq 0$. La successione $(a_0, a_1, a_m, 0, 0, 0, \dots)$ viene scritta come

$$a_m * x^m + a_{m-1} * x^{m-1} + a_1 * x^1 + a_0 * x^0 = A(x)$$

Questa è una scrittura puramente formale.

Se qualche coefficiente a_j per $0 < j < n - 1$ è nullo, allora si omette il termine $a_j * x^j$.

Le operazioni di somma e prodotto di polinomi coincidono con quelle usuali nella usuale rappresentazione.

4 Interpretazione della scrittura formale

Considerando la scrittura:

$$A(x) = a_m * x^m + \cdots + a_1 * x + a_0$$

il polinomio $A(x)$ si può vedere come somma di particolari polinomi che chiamiamo *monomi* $a_i * x^i$, dove il simbolo $a_i * x^i$ è la successione $(0, 0, 0, a_i, 0, 0, \dots)$ con $0 \leq i \leq m$. La somma di queste successioni secondo la regola definita prima si ottiene proprio $A(x) = (a_0, a_1, \dots, a_i, \dots, a_m)$.

Il monomio $a_i * x^i$ è a sua volta prodotto del monomio $a_i = a_i * x^0 = (a_i, 0, 0, \dots)$ e il monomio $x_i = 1_A * x^i = (0, 0, 1_A, 0, 0, \dots)$.

x^i è sua volta si può intrerpretare come la potenza i -esima del polinomio $1_A * x$.

A questa scrittura formale si possono applicare le regole usate per i polinomi a coefficienti numerici.

L'anello dei polinomi su A nell'indeterminata x si denota con il simbolo $A[x]$.

5 Anticipazione: morfismi tra anelli

Definizione (273 Morfismo di anelli)

Siano A e B due anelli. Un'applicazione $f\colon A \to B$ si dice *morfismo di anelli* se

1. $\forall x, y \in A$, $f(x + y) = f(x) + f(y)$
2. $\forall x, y$, $f(xy) = f(x) * f(y)$
3. $f(1_A) = 1_B$

Un morfismo di anelli è un morfismo di gruppi abeliani e un morfismo di monoidi moltiplicativi.

Come nel caso dei gruppi, un morfismo può essere iniettivo (monomorfismo), suriettivo (epimorfismo) e biettivo (isomorfismo).

6 Sottoanello delle costanti

Osservazione (274)

I monomi di tipo $a*x^0 = a$ con $a \in A$, cioè le successioni $(a, 0, 0, \dots)$ formano un sottoanello di $A[x]$. Infatti l'unità, le differenze e i prodotti appartengono ancora al sottoanello. Questo sottoanello è isomorfo all'anello A (infatti se al monomio $a * x^0$ si associa a , si verifica subito che c'è un omomorfismo di anelli).

In questo senso, si può identificare A come un sottoanello di $A[x]$ chiamato *anello delle costanti*. In particolare, lo zero e l'unità di A sono identificati con lo zero e l'unità di $A[x]$.

7 Grado

Definizione (275 Grado di un polinomio e coefficiente direttivo)

Sia $A[x] = a_n*x^n+a_{n-1}*x^{n-1}+\cdots+a_1*x+a_0$ con $a_n \neq 0$ un qualsiasi polinomio non nullo ($\neq 0_{A[x]}$) in $A[x]$. Allora per ogni $m > n$, $A_m = 0$. Diremo che n è il *grado di* $A[x]$ e si scrive $n = gr(A[x])$. a_n si dice *coefficiente direttivo* di $A[x]$ e se $a_n = 1_A$, $A(x)$ si dice *monico*. Al polinomio nullo si attribuisce convenzionalmente grado -1 .

NB: i polinomi di grado zero sono le costanti con $a \neq 0$.

Proposizione (276)

Siano $A(x), B(x) \in A[x]$. Allora

1. il grado della somma $A(x) + B(x) \leq \max\{gr(A(x)), gr(B(x))\}$.

(non vale sempre l'uguale, infatti, se ad esempio i due polinomi hanno lo stesso grado e i due termini di grado massimo sono opposti, il grado della somma è $n-1$)

1. Il grado del prodotto $gr(A(x) * B(x)) \leq gr(A(x)) + gr(B(x))$

Dimostrazione

2. Se $A(x) = a_n * x^n + a_1 * x + a_0$ e $B_x = b_m * x^m + \cdots + b_1 * x + b_0$, allora $A(x) * B(x) = (a_n * b_m) * x^{m+n} + (a_n * b_{n-1}) * x^{n-1} + \cdots + a_0 * b_0$ e quindi il grado del prodotto non può superare la somma dei gradi. Non è necessariamente

uguale, perché se A ha divisori dello zero, allora può avvenire che $a_n * b_n = 0$ anche se $a_n \neq 0, b_n \neq 0$.

Se A è un dominio, il grado del prodotto è esattamente uguale a $m + n$.

Ad esempio, se A è l'anello delle classi di resto modulo 6 , allora $A(x) = [2]x^3 + [1]$ e $B(x) = [3]x^2 + [2]$ allora la somma dei gradi è 5 ma il prodotto è $[4]x^3 + [3]x^2 + [2]$ (grado 3).

Proposizione (277 Proprietà di trasposto)

Se A è un dominio, anche il corrispondente anello $A[x]$ è un dominio, cioè è privo di divisori dello zero.

Dimostrazione

Dalla formula del prodotto: se prendo due polinomi non nulli con grado m e n , che sono diversi da zero, dalla formula si ha che il prodotto ha grado $n + m$ (il coefficiente di grado $n + m$ non può essere uguale a zero) e quindi il prodotto di due polinomi non nulli è sempre un polinomio non nullo se l'anello delle costanti è un dominio.

Sia A un dominio. Se il grado del prodotto di due polinomi non nulli è 0 , anche il grado dei fattori dev'essere 0 .

Se A è un dominio, un polinomio è invertibile se e solo se ha grado 0 . (se ha grado maggiore di 0 , anche il grado del prodotto dev'essere maggiore di 0 e quindi non esiste nessun polinomio che moltiplicato con quello di partenza è uguale all'unità). Gli elementi unitari sono tutte e sole le costanti invertibili nel dominio A . Ad esempio, se $A = \mathbb{Z}$, tutti gli elementi unitari di $A[x]$ sono ± 1 .

Preso l'anello dei polinomi delle classi di resto modulo 4 , ad esempio il polinomio $(2x + 1)^2 = [4]x^2 + [4]x + 1 = 1$. In questo anello $2x + 1$ è un polinomio di grado 1 che ha come inverso se stesso.

8 Fonti per testo e immagini; autori; licenze

8.1 Testo

- **Corso:Algebra Anelli (Unimib)/Anelli/Polinomi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Anelli_(Unimib)/Anelli/Polinomi?oldid=48111 *Contributori:* Toma.luca95 e Mmontrasio

8.2 Immagini

8.3 Licenza dell'opera