Lezione del 14 marzo; Registro dettagliato

Polinomi.

1. Ricordiamo che consideriamo solo anelli con unita' e omomomorfismi di anelli che preservino l'unita'.

   Siano B un anello commutativo, $A \subseteq B$ un sottoanello di B, e $c \in B$. Il piu' piccolo sottoanello di B contenente A e c, che viene detto sottoanello di B generato da A e c, si descrive esplicitamente come l'insieme degli elementi di B che si possono scrivere in almeno un modo come somma di prodotti di elementi di A per potenze di c cioe' come

   $$(*) \qquad a_0 + a_1 c + a_2 c^2 + \cdots , \qquad \text{(numero finito di addendi)}$$

   con gli a_i in A. Infatti: da una parte, ogni sottoanello di B che contiene A e c deve contenere anche gli elementi di questo tipo; dall'altra, l'insieme degli elementi di questo tipo e' un sottoanello di B che contiene A e c. In particolare: se due elementi a, b di B si possono scrivere come somma di prodotti di elementi di A per potenze di c

   $$a = a_0 + a_1 c + a_2 c^2 + \cdots + a_m c^m, \qquad b = b_0 + b_1 c + b_2 c^2 + \cdots + b_n c^n,$$

   allora anche la loro somma $a + b$ e il loro prodotto ab si possono scrivere come somma di prodotti di elementi di A per potenze di c

   $$a + b = (a_0 + b_0) + (a_1 + b_1)c + (a_2 + b_2)c^2 + \cdots + (a_p + b_p)c^p$$
   $$ab = a_0 b_0 + (a_1 b_0 + a_0 b_1)c + (a_0 b_2 + a_1 b_1 + a_2 b_0)c^2 + \cdots + a_m b_n c^{m+n}$$

   (nella scrittura di $a + b$, si e' indicato con p un intero maggiore-uguale ad m ed n, e si intende $a_i = 0$ per $m < i \leq p$ e $b_i = 0$ per $n < i \leq p$).

2. La descrizione data del sottoanello generato da A e c nell'anello B e' data solo in funzione di A e c ed e' sempre la stessa, mentre il sottoanello generato da A e c in B varia in funzione dalla relazione fra A e c in B. Informalmente, l'anello dei polinomi a coefficienti in A in una indeterminata x e' la struttura che hanno in comune tutti i sottoanelli generati da A e da un elemento in un anello. Piu' precisamente, si ha il seguente

   Theorem 1. *Dato un anello commutativo A, esiste un anello commutativo $A[x]$ che contiene una copia isomorfa di A e un elemento $x \in A[x]$ e che possiede la proprieta' universale*

   > *per ogni anello commutativo B che contiene una copia isomorfa di A e per ogni elemento $c \in B$ esiste uno ed un solo omomorfismo di anelli $A[x] \to B$ che fissa A e manda x in c.*

   L'anello $A[x]$ e' unico a meno di isomorfismi, e' l'anello dei polinomi a coefficienti in A nella indeterminata x; l'omomorfismo $A[x] \to B$ che fissa A e manda x in c e' la "sostituzione di x nell'elemento $c \in B$".

Nei prossimi punti daremo una costruzione dell'anello dei polinomi $A[x]$, quella come sottoanello dell'anello delle serie formali $A[[x]]$, e verificheremo che possiede la proprieta' universale.

3. **Anelli di serie formali in una indeterminata**. Sia A un anello commutativo. In modo leggermente naive, si puo' dire che una serie formale a coefficienti in A nell'indeterminata x e' una scrittura formale

$$a = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{i=0}^{\infty} a_i x^i$$

dove $(a_0, a_1, a_2, \ldots) = (a_n)_0^\infty$ e' una successione di elementi di A, i coefficienti di a; la successione dei cofficienti e' l'unico dato di cui consiste una serie formale, tutto il resto, in particolare il segno $+$, e' formale. Di regola, indicheremo le serie formali con lettere minuscole e se indicheremo una serie con una lettera, indicheremo i suoi coefficienti con la stessa lettera con indici. L'insieme delle serie formali a coefficienti in A nell'indeterminata x si indica con $A[[x]]$.

L'addizione e la moltiplicazione di due serie formali

$$a = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{i=0}^{\infty} a_i x^i, \qquad b = b_0 + b_1 x + b_2 x^2 + \cdots = \sum_{i=0}^{\infty} b_i x^i$$

sono definite da

$$a + b = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

$$ab = (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots = \sum_{i=0}^{\infty} \left[\sum_{j+h=i} a_j b_h \right] x^i;$$

in breve, sulle successioni si ha

$$\begin{aligned} (a+b)_i &= a_i + b_i, \qquad i \in \mathbb{N} \\ (ab)_i &= \sum_{j+h=i} a_j b_h \qquad i \in \mathbb{N}. \end{aligned}$$

Con queste operazioni, l'insieme $A[[x]]$ e' un anello commutativo. La serie nulla 0, l'opposta $-a$ di una serie a, e la serie unita' 1 sono date nei termini delle successioni dei coefficienti rispettivamente da $(0)_i = 0$, e $(-a)_i = -a_i$ e $(1)_i = \delta_{i0}$, per ogni $i \in \mathbb{N}$. I coefficienti della serie prodotto di tre fattori sono dati da

$$(abc)_i = \sum_{j+h+k=i} a_i b_j c_k, \qquad \forall i \in \mathbb{N}.$$

4. **Digressione**. Sia A un campo. Consideriamo in $A[[x]]$ l'equazione $ab = c$ dove a e c sono date serie e b e' una serie incognita. Esplicitamente, l'equazione si

traduce nei termini dei coefficienti nel sistema di infinite equazioni nelle infinite incognite $b_0, b_1, b_2, \ldots$

$$\begin{aligned} &a_0 b_0 = c_0 \\ &a_0 b_1 + a_1 b_0 = c_1 \\ &a_0 b_2 + a_1 b_1 + a_2 b_0 = c_2 \\ &\vdots \end{aligned}$$

Si noti che se $a_0 \neq 0$, allora il sistema ha una ed una sola soluzione, data ricorsivamente da

$$b_0 = a_0^{-1} c_0; \quad b_{i+1} = a_0^{-1}(c_{i+1} - a_1 b_i - \cdots - a_{i+1} b_0)$$

D'altro canto, se $a_0 = 0$ e $c_0 \neq 0$ allora il sistema non ha alcuna soluzione. Possiamo riassumere quete considerazioni con la

Proposition 1. *Se A e' un campo, allora gli elementi invertibili dell'anello $A[[x]]$ sono tutte e sole le serie formali con coefficiente zeresimo non nullo.*

In particolare, nell'anello $\mathbb{Q}[[x]]$ si ha

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots$$

5. **Anelli di polinomi in una indeterminata**. Sia A un anello commutativo. L'insieme delle serie formali a coefficienti in A in una indeterminata x aventi un numero finito di coefficienti non nulli e' un sottoanello dell'anello $A[[x]]$. Queste serie formali si dicono polinomi a coefficienti in A nell'indeterminata x e l'anello da esse formato si indica con $A[x]$. Si ha:

- La funzione $A \to A[x]$ che manda $a \in A$ nel polinomio $\bar{a} = a + 0x + 0x^2 + \cdots$ avente zeresimo coefficiente a e tutti gli altri nulli e' un monomorfismo di anelli, che trasforma A in una sua copia isomorfa $\bar{A}$ sottoanello di $A[x]$.

- $A[x]$ contiene il particolare polinomio $\xi = 0 + 1x + 0x^2 + \cdots$ avente primo coefficiente 1 e tutti gli altri nulli; per ogni $n \in \mathbb{N}$, la potenza $n-$ma di ξ e' il polinomio $\xi^n = 0 + \cdots + 0x^{n-1} + 1x^n + 0x^{n+1} + \cdots$.

- Per ogni polinomio $f_0 + f_1 x + f_2 x^2 + \cdots$, indicato con p un indice tale che $f_i = 0$ per ogni $i > p$, si ha

$$f_0 + f_1 x + f_2 x^2 + \cdots = \bar{f}_0 + \bar{f}_1 \xi + \bar{f}_2 \xi^2 + \cdots \bar{f}_p \xi^p$$

(si noti che al primo membro si ha una scrittura formale e al secondo membro si ha una espressione in $A[x]$). Dunque l'anello $A[x]$ e' generato dal sottoanello $\bar{A}$ e dall'elemento ξ.

- Identificando l'anello A col sottoanello $\bar{A}$ e l'indeterminata x con l'elemento $\xi \in A[x]$, ogni polinomio a coefficienti A nell'indeterminata x puo' essere scritto nella forma familiare

$$f = f_0 + f_1 x + f_2 x^2 + \cdots \qquad \text{(numero finito di addendi)}$$

con gli a_i in A.

- Per ogni anello commutativo B contenente un sottoanello identificato con A e per ogni $c \in B$, esiste al piu' un omomorfismo di anelli $E_c : A[x] \to B$ tale che $E_c(x) = c$ ed $E_c(a) = a$ per ogni $a \in A$, dato da

$$E_c(a_0 + a_1x + a_2x^2 + \cdots + a_mx^m) = a_0 + a_1c + a_2c^2 + \cdots + a_mc^m.$$

Questa posizione definsce effettivamente una funzione, un omomorfismo di anelli, detta sostituzione di x in c.

Gli elementi $c \in B$ che sostituiti alla indeterminata x in $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$ danno lo zero di B, cioe' tali che $a_0 + a_1c + a_2c^2 + \cdots + a_mc^m = 0$ si dicono "radici" di p in B.

6. Per ogni polinomio non nullo $p = a_0 + a_1x + a_2x^2 + \cdots \in A[x]$ il massimo indice di un coefficiente non nullo si dice grado di p. Si ha che il grado del polinomio somma e' minore-uguale del massimo dei gradi dei polinomi addendi, e che il grado del polinomio prodotto e' minore-uguale della somma dei gradi dei polinomi fattori (se sono definiti). Se l'anello A e' un dominio di integrita' allora il polinomio prodotto di due polinomi non nulli e' non nullo e il suo grado e' la somma dei gradi dei due polinomi.

   Si ha il seguente fatto:

   > Sia A un anello commutativo. Siano $p = p(x)$ un polinomio non nullo in $A[x]$, e $c \in A$. Se $E_c(p) = 0$, allora $p(x)$ e' divisibile per $x - c$.

   Da questo fatto segue la

   Proposition 2. *Se A e' dominio di integrita', un polinomio non nullo di grado n in $A[x]$ puo' avere al piu' n radici distinte.*

7. **Polinomi e funzioni polinomiali**. Sia A un anello commutativo e sia S un insieme. L'insieme A^S delle funzioni $S \to A$, con le usuali operazioni di somma e prodotto definite punto a punto, e' una anello commutativo.

   Sia $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$ un polinomio in $A[x]$; associando a ciascun $c \in A$ la valutazione $p(c) = a_0 + a_1c + a_2c^2 + \cdots + a_mc^m$ di $p(x)$ in $x = c$, si ha una funzione $A \to A$. Le funzioni cosi' ottenute si dicono funzioni polinomiali su A; l'insieme $Pol[A]$ delle funzioni polinomiali su A e' un sottoanello dell'anello A^A delle funzioni da A in se', con le operazioni definite punto a punto. Per definizione si ha dunque un epimorfismo $E : A[x] \to Pol[A]$.

   Puo' succedere che a polinomi distinti corrispondano funzioni polinomiali coincidenti. Ad esempio cio' capita se A e' finito; infatti l'insieme dei polinomi su un qualsiasi anello A e' sempre infinito, mentre se A e' finito l'insieme delle funzioni polinomiali da A ad A e' finito. Si ha pero' la

   Proposition 3. *Se A e' un domnio d'integrita' infinito, allora $E : A[x] \to Pol[A]$ e' un isomorfismo.*

Infatti,se p e' un polinomio non nullo, allora p ha al piu' tante radici quanto e' il suo grado (essendo A dominio d'integrita') e la funzione polinomiale corrispondente non puo' essere la funzione identicamente nulla (essendo A infinito); dunque $\mathrm{Ker}(E) = \{0\}$, ed E e' un isomorfismo.

Appendice. Cenni alle funzioni generatrici

In questa parte si accenna, attraverso due esempi, alla relazione fra la combinatoria enumerativa e l'algebra delle serie formali (cfr. ad es. voce "funzione generatrice" su Wikipedia ed associata bibliografia).

1. La successione dei numeri di Fibonacci e' definita per ricorsione dalle condizioni $F_0 = F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$ (per ogni $n \in \mathbb{N}$). A questa successione corrisponde la serie formale di Fibonacci

$$F = \sum_{n=0}^{+\infty} F_n x^n.$$

La ricorsione definitoria dei numeri di Fibonacci si riflette in una relazione sulla serie di Fibonacci. Infatti

$$\begin{aligned} F = \sum_{n=0}^{+\infty} F_n x^n &= 1 + x + \sum_{n=2}^{+\infty} F_n x^n \\ &= 1 + x + \sum_{n=2}^{+\infty} F_{n-1} x^n + \sum_{n=2}^{+\infty} F_{n-2} x^n \\ &= 1 + x + x \sum_{n=2}^{+\infty} F_{n-1} x^{n-1} + x^2 \sum_{n=2}^{+\infty} F_{n-2} x^{n-2} \\ &= 1 + xF + x^2 F \end{aligned}$$

Da questa relazione si ricava la formula esplicita

$$F = \frac{1}{1 - x - x^2}.$$

Da questa formula esplicita per la serie formale F si puo' ricavare una formula esplicita per i numeri di Fibonacci.

2. Il concetto di sottinsieme di un insieme ha una naturale generalizzazione al concetto di sottomultinsieme di un insieme, o come piu' spesso si dice, multinsieme su un insieme. Un multinsieme su un insieme e' dato assegnando a ciascun elemento dell'insieme un intero naturale, detto molteplicita' dell'elemento nel multinsieme. In altri termini, un multinsieme su un insieme A e' una funzione $M : A \to \mathbb{N}$. Per ciascun $a \in A$ l'intero $M(a)$ si dice molteplicita' di a in M; la somma $\sum_{a \in A} M(a)$ si dice cardinalita' del multinsieme M su A e si indica con $|M|$. Al posto di dire che M e' un multinsieme di cardinalita' k su A si dice che M e' un $k-$multinsieme su A.

Per ogni $n, k \in \mathbb{N}$ il numero dei $k-$multinsiemi su un $n-$insieme si dice coefficiente multinsiemistico n su k e si indica con $\left\langle {n \atop k} \right\rangle$.

I multinsiemi su un insieme A nei quali la molteplicita' di ciascun elemento e' al piu' uno possono essere identificati con i sottinsiemi di A, e la cardinalita' di tali multinsiemi coincide con la loro cardinalita' come sottinsiemi. Questa relazione fra sottomultinsiemi e sottinsiemi si riflette in una relazione fra coefficienti multinsiemistici e coefficienti binomiali.

Per ciascun $n \in \mathbb{N}$ fissato, si ha la successione di coefficienti multinsiemistici $\left\langle {n \atop 0} \right\rangle, \left\langle {n \atop 1} \right\rangle \left\langle {n \atop 2} \right\rangle, \ldots$ alla quale corrisponde una serie formale, che e' descritta esplicitamente dalla

Proposition 4. *Per ciascun $n \in \mathbb{N}$ fissato, si ha*

$$\sum_{k=0}^{\infty} \left\langle {n \atop k} \right\rangle x^k = \left[\sum_{k=0}^{\infty} x^k \right]^n = (1-x)^{-n}.$$

Idea della dimostrazione. Il prodotto di n serie formali e' dato da

$$\left[\sum_{k=0}^{\infty} f_k^{(1)} x^k \right] \cdots \left[\sum_{k=0}^{\infty} f_k^{(n)} x^k \right] = \sum_{k=0}^{\infty} \left[\sum_{k_1+\cdots+k_n=k} f_{k_1}^{(1)} \cdots f_{k_n}^{(n)} \right] x^k.$$

Specializzando questa uguaglianza al caso in cui $f_0^{(i)} = f_1^{(i)} = f_2^{(i)} = \cdots = 1$ per ogni $i = 1, \ldots, n$, e osservando che

$$\sum_{k_1+\cdots+k_n=k} 1 = \left\langle {n \atop k} \right\rangle$$

si ottiene la prima uguaglianza nell'enunciato. La seconda segue dal fatto che

$$\sum_{k=0}^{\infty} x^k = (1-x)^{-1}.$$