

Formalizziamo l'idea delle "espressioni algebriche":

$$a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m$$

Consideriamo il seguente insieme di successioni:

$\mathbb{N} \rightarrow R$, $n \mapsto a_n$ con R anello commutativo

Tali che $\exists m$ t.c. $a_n = 0_R \forall n > m$

Date (a_n) , (b_n) definiamo:

$$(a_n) + (b_n) = (c_n) \text{ con:}$$

$$c_n = a_n + b_n$$

si avrà che certamente c_n sarà ammissibile ($c_n = 0$ $\forall n > m^*$ per un certo $m^* \in \mathbb{N}$).

Definiamo inoltre:

$$(a_n)(b_n) = (c_n) \text{ con:}$$

$$c_n = \sum_{k=0}^n a_k \cdot b_{n-k} = \sum_{\substack{i,s \text{ t.c.} \\ i+s=n}} a_i b_s$$

es.:

$$\begin{aligned} & (a_0 + a_1 x + a_2 x^2)(b_0 + b_1 x) = \\ & = a_0 b_0 + a_0 b_1 x + a_1 b_0 x + a_1 b_1 x^2 + a_2 b_0 x^2 + a_2 b_1 x^3 \\ & = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_1 b_1 + a_2 b_0) x^2 + a_2 b_1 x^3 \\ & = a_0 b_0 \\ & \quad + (a_0 b_1 + a_1 b_0) x \\ & \quad + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 \\ & \quad + (a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0) x^3 \\ & \quad + \dots \end{aligned}$$

Verifichiamo che tale insieme di successioni ammissibili con le 2 operazioni $+$, \cdot appena definite costituisce un anello:

1) le proprietà di $+$ sono ovvie ✓

2) \cdot è ben definita:

date (a_n) , (b_n) successioni ammissibili si ha

$$a_n = 0 \quad \forall n > m_1, \quad b_n = 0 \quad \forall n > m_2$$

\Rightarrow secondo la formula di sopra si ha:

$$m = \max \{m_1, m_2\},$$

$$c_{2m+1} = \sum_{k=0}^{2m+1} a_k b_{2m+1-k}$$

\Rightarrow Almeno 1 tra k e $2m+1$ è $> m$:

$$c_{2m+1} = \sum_{\substack{i, s \text{ t.c.} \\ i+s=2m+1}} a_i \cdot b_s = 0$$

Analogamente se $n > 2m+1$:

$$c_{2m+1} = \sum_{\substack{i, s \text{ t.c.} \\ i+s=2m+1}} a_i \cdot b_s = 0$$

perché almeno tra i, s è sicuramente $> m$

3) Associazività di \cdot :

date $a = (a_n)$, $b = (b_n)$, $c = (c_n)$ successioni ammissibili, si ha:

$$\Rightarrow ((a \cdot b) \cdot c)_n = \sum_{i+s=n} d_i c_s = \sum_{i+s=n} \left(\sum_{k+l=i} a_k b_l \right) c_s$$

$$\begin{aligned}
 &= \sum_{i+s=n} \left(\sum_{k+l=i} a_k b_l c_s \right) \stackrel{\uparrow}{=} \sum_{k+l+s=n} a_k b_l c_s \\
 &\quad \nearrow (x+y)z = \\
 &\quad \quad xz + yz \\
 &\quad \quad \quad a+b = b+a
 \end{aligned}$$

$$= \sum_{k+i} \alpha_k \left(\sum_{\ell+s=i} b_\ell c_s \right) = (\alpha(bc))_n$$

4) $\exists!$ dell' elemento neutro di \cdot :

$\Rightarrow (1, 0, 0, \dots)$ è elemento neutro di \cdot .

N.B.

Sia $x = (0, 1, 0, \dots)$, allora:

$$x^0 = (1, 0, \dots)$$

$$x^1 = x = (0, 1, 0, \dots)$$

\vdots

$$x^m = (0, \dots, \underset{\substack{\uparrow \\ m}}{1}, 0, \dots) \quad ((x)_m = 1)$$

N.B.

Data $a \in R$ sia $\hat{a} = (a, 0, \dots)$, si ha:

$$(a_0, a_1, \dots, a_m, 0, \dots) = \hat{a}_0 + \hat{a}_1 x + \dots + \hat{a}_m x^m$$

\Rightarrow la struttura risultante è un ANELLO COMMUTATIVO denotato con $R[\hat{x}]$, dove \hat{x} è una INDETERMINATA.

◻

Osservazione:

Consideriamo $\mathbb{N} \times \mathbb{N}$ con \sim relazione di equivalenza t.c.:

$$(a, b) \sim (c, d) \iff a + d = c + b$$

\Rightarrow su $\mathbb{N} \times \mathbb{N}/\sim$ definiamo le seguenti operazioni:

$$1) \quad [(a, b)] + [(c, d)] = [(a+c, b+d)]$$

$$2) \quad -[(a, b)] = [(b, a)]$$

$$3) \quad [(a, b)] \cdot [(c, d)] = [(ac + bd), (bc + ad)]$$

\Rightarrow la funzione $\begin{array}{c} \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}/\sim \\ a \longmapsto [(a, 0)] \end{array}$ è iniettiva.

Inoltre $\forall x \in \mathbb{Z}$ si ha che $x = [(a, 0)] \vee x = [(0, a)]$ per un certo $a \in \mathbb{N}$.

Studiamo ora l'anello dei polinomi $R[x]$:

Il polinomio nullo $\hat{0} = (0, \dots) = 0$ ha $\deg(\hat{0}) = -\infty$ dove $\deg(a_0 + a_1 x + \dots + a_m x^m) = m$ ($a_m \neq 0$).

Notazione:

se $f(x) = a_0 + a_1 x + \dots + a_m x^m$, $a_m \neq 0$

si ha $\deg(f(x)) = m$

Valgono le seguenti FORMULE PER IL GRADO IN UN ANELLO QUALESIASI:

$$1) \deg(f(x) + g(x)) \leq \max \{ \deg(f(x)), \deg(g(x)) \}$$

$$2) \deg(f(x) \cdot g(x)) \leq \deg(f(x)) + \deg(g(x))$$

(se $a, b \in R$ con $a \neq 0 \neq b \wedge ab = 0$ si ha che:

$$(ax)(bx) = abx^2 = 0 !!!$$

Esempio:

in un anello booleano si ha $a \neq 0 \neq (1+a)$

$$\text{con } a(1+a) = a + a^2 = a + a = 0$$

$$\Rightarrow ax(1+a)x = a(1+a)x^2 = 0 !!!)$$

In un dominio di integrità tale fenomeno non può avvenire, quindi possiamo riformulare la formula per il grado nel seguente modo:

Proposizione:

Se R è un dominio, allora:

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$$

In particolare, $R[x]$ è un dominio.

Dim.:

se $f = g = 0$ si ha $\deg(f \cdot g) = -\infty$

se $f \neq 0 \neq g$ si ha:

$$f(x) = f_0(x) + \alpha x^m \text{ con } \alpha \neq 0 \Rightarrow \deg f_0(x) < m$$

$$g(x) = g_0(x) + \beta x^n \text{ con } \beta \neq 0 \Rightarrow \deg g_0(x) < n$$

$$\begin{aligned} \Rightarrow f(x)g(x) &= b x^m f_0(x) + \alpha x^m g_0(x) + f_0(x) g_0(x) \\ &\quad + \alpha \beta x^{m+n} \end{aligned}$$

$$\Rightarrow \deg(b x^m f_0(x) + \alpha x^m g_0(x) + f_0(x) g_0(x)) < m + n$$

$$\Rightarrow \deg(f(x)g(x)) = m + n$$

q.e.d.

Tale dimostrazione funziona se uno dei 2 polinomi è, per esempio, monico: $a_m = 1$

Divisione con resto:

Dati $f(x), g(x) \in R[x]$ con g monico, si ha che
 $\exists! q(x), r(x) \in R[x]$ t.c.:

$$1) f(x) = q(x)g(x) + r(x)$$

$$2) \deg(r(x)) < \deg(g(x))$$

Dim.

1) Unicità:

Sia $f = q_1 g + r_1 = q_2 g + r_2$
 $\Rightarrow \deg r_1 < \deg g \wedge \deg r_2 < \deg g$
 $\Rightarrow r_2 - r_1 = (q_1 - q_2)g$
 $\Rightarrow \deg(r_2 - r_1) < \deg g$, se $q_1 - q_2 \neq 0$, $\deg((q_1 - q_2)g) \geq \deg g$
 \Rightarrow deve essere $q_1 - q_2 = 0$ e quindi $r_2 - r_1 = 0$

2) Esistenza:

Se $f = 0$, è ovvio: $q = r = 0$ ✓

se $f \neq 0$, procediamo per induzione su $\deg f$:

caso base: $\deg f = 0 \Rightarrow$ se $\deg g = 0$ allora
 $g = 1$ e quindi $f = f \cdot g + 0$
se $\deg g > 0$ allora $f = 0 \cdot g + f$

passo induttivo:

supponiamo che la divisione valga per polinomi
con $\deg() < \deg f > 0$.

Se $\deg f < \deg g$: $f = 0g + f$

Se $\deg f \geq \deg g$:

$n = \deg f$, $m = \deg g \Rightarrow n \geq m$

$\Rightarrow f_1 = f - \alpha x^{n-m} g$ con α = coefficiente di
grado massimo di f . Si ha:

$\deg f_1 < \deg f$

$\Rightarrow f_1 = q_1 g + r$ con $\deg r < \deg g$

$\Rightarrow f = (\alpha x^{n-m} + q_1)g + r$

q.e.d.

Esempio:

$$\begin{array}{r}
 f(x) \quad 3x^4 - 2x^3 + 4x^2 - x + 2 \\
 g(x) \quad x^2 - 3x + 1
 \end{array}
 \begin{array}{r}
 f_1(x) \quad -3x^4 + 3x^3 - 3x^2 \\
 \hline
 // \quad 7x^3 + x^2 - x + 2
 \end{array}
 \begin{array}{r}
 g(x) \\
 3x^2 + 7x + 22
 \end{array}$$

$$\begin{array}{r}
 f_2(x) \quad // \quad 22x^2 - 8x + 2 \\
 \hline
 -22x^2 + 66x - 22
 \end{array}$$

$$\begin{array}{r}
 f_3(x) = r(x) \quad // \quad 58x - 20
 \end{array}$$

Sottoanelli:

Def. (Sottoanello):

Dati R anello, $S \subseteq R$, si dice che S è SOTTOANELLO

di R se:

- 1) $0, 1 \in S$
- 2) $a-b, ab \in S \quad \forall a, b \in S$

\Rightarrow se $S \subseteq R$ è sottoanello, allora è in particolare un sottogruppo di $(R, +)$

Esempio:

1) R anello, definiamo $R \times R$ con:

$$(a, b) + (c, d) = (a+c, b+d)$$

$$(a, b)(c, d) = (ac, bd)$$

$\Rightarrow R \times R$ è anello, $S = R \times \{0\} \subseteq R \times R$ non è sottoanello!!! Infatti $(1, 1) = 1_{R \times R} \notin S$

- 2) \mathbb{Z} è sottogruppo di \mathbb{Q}
- 3) \mathbb{Q} è sottogruppo di \mathbb{R}
- 4) \mathbb{R} è sottogruppo di $\mathbb{R}[X]$

Proposizione:

Ogni anello ha un sottogruppo minimo (rispetto all'inclusione insiemistica) P

Dim.

Indichiamo gli interi come \hat{n} , in particolare $\hat{0}, \hat{1}$.

Si ha che $\forall R$ anello :

$$P \subseteq R \text{ con } 1_R \in P \Rightarrow \langle 1 \rangle = \{ \hat{n} 1_R \mid \hat{n} \in \mathbb{Z} \} \subseteq P$$

\Rightarrow mostriamo che $\langle 1 \rangle$ è sottogruppo di R :

- 1) $\langle 1 \rangle$ è sottogruppo di $(R, +)$
- 2) $(\hat{n} 1)(\hat{m} 1) = (\hat{n} \hat{m}) 1$

Induzione su $\hat{n} \geq \hat{0}$:

caso base: $\hat{n} = \hat{0} \quad \checkmark$

passo induttivo:

$$\hat{n} \rightsquigarrow \hat{n} + \hat{1}$$

$$\Rightarrow ((\hat{n} + \hat{1}) 1)(\hat{n} 1) = (\hat{n} 1 + \hat{1} 1)(\hat{n} 1)$$

$$= (\hat{n} 1)(\hat{n} 1) + (\hat{1} 1)(\hat{n} 1)$$

$$= (\hat{n} 1)(\hat{n} 1) + \hat{n} 1$$

ipotesi induttiva $\rightarrow = (\hat{n} \hat{n} 1) + \hat{n} 1 = (\hat{n} \hat{n} + \hat{n}) 1 = ((\hat{n} + \hat{1}) \hat{n}) 1$

$\Rightarrow \langle 1 \rangle$ è sottogruppo minimo di R .

q.e.d.

esempi (sottramelli):

1) $\mathbb{Z}_p := \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}$ con p primo

($p = 3 \Rightarrow \frac{3}{6} \in \mathbb{Z}_3$ perché $\frac{3}{6} = \frac{1}{2}, 3 \nmid 2$)

è sottramello di \mathbb{Q} :

1) $0 = \frac{0}{1} \in \mathbb{Z}_p$

2) $1 = \frac{1}{1} \in \mathbb{Z}_p$

3) $\frac{a}{b}, \frac{c}{d} \in \mathbb{Z}_p \Rightarrow p \nmid b, p \nmid d \Rightarrow \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \in \mathbb{Z}_p$

$$\Rightarrow \frac{a}{b} \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Z}_p$$

