Capitolo 1

Prima lezione: Polinomi ed algebra astratta

1.1 Polinomi, nozioni di base

Definizione 1.1. [AAX00] Definiamo come $\mathbb{R}[x]$ l'insieme dei polinomi a coefficienti in $\mathbb{R}$, l'insieme dei numeri reali. Dato un polinomio

$$f(x) \in \mathbb{R}[x], f(x) = \sum_{i=0}^n a_i x^i = a_n x^n + \cdots + a_1 x + a_0 \quad \text{con } a_0, \dots, a_n \in \mathbb{R} \text{ e } a_n \neq 0$$

1. Il grado di $f(x)$ è n , e si scrive $\deg f(x)$. Il grado del polinomio 0 non è definito.
2. I reali $a_n, \dots, a_0$ sono i coefficienti del polinomio.
3. I termini del polinomio sono gli x^i per cui il corrispondente coefficiente a_i sia non nullo.
4. Il termine di testa di $f(x)$ è x^n .
5. Il coefficiente di testa di $f(x)$ è a_n .
6. Il termine noto di $f(x)$ è a_0 (abuso di notazione - termine è ambiguo ma di uso corrente).

Esempio 1.2. [AAA03] Dato $f(x) = x^5 + 2x - 1$

1. $\deg(f(x)) = 5$.
2. Il termine di testa è x^5 . Il coefficiente di testa è 1.
3. Il termine noto è -1 .
4. I coefficienti di $f(x)$ sono $a_5 = 1, a_4 = 0, a_3 = 0, a_2 = 0, a_1 = 2, a_0 = -1$. I termini di $f(x)$ sono $x^5, x^1, 1 = x^0$.

Definizione 1.3. [AAA01] Siano $f(x) = \sum_{i=0}^n a_i x^i, g(x) = \sum_{i=0}^m b_i x^i \in \mathbb{R}[x]$, con ovviamente $\deg(f) = n, \deg(g) = m$ e $n \geq m$. Allora

- Principio di identità dei polinomi (Ovvero i due polinomi sono uguali come polinomi):

$$f(x) \stackrel{\mathbb{R}[x]}{=} g(x) \Leftrightarrow n = m \text{ e } \forall i : 0, \dots, n \ a_i = b_i$$

- *Somma e prodotto*

$$f(x) + g(x) = \sum_{i=0}^n (a_i + b_i)x^i \quad \text{ponendo } b_i = 0 \text{ per } i > m$$

$$f(x) \cdot g(x) = \sum_{d=0}^{m+n} \left(\sum_{i=0}^d a_i \cdot b_{d-i} \right) x^d$$

Esempio 1.4. [AA03]

- I polinomi $f(x) = x^5 + 2x - 1$ e $g(x) = x^3 + 2x - 1$ sono diversi dato che hanno grado diverso. Scriviamo $f(x) \not\equiv_{\mathbb{R}[x]} g(x)$.
- $x^2 - 2x + 1 \not\equiv_{\mathbb{R}[x]} x^2 - 2x + 3$ dato che hanno il termine noto diverso.

Osservazione 1.5. [AA05] Ricordiamo che l'espressione

$$x^2 \equiv_{\mathbb{R}[x]} 1$$

è una uguaglianza tra due polinomi dati, x^2 e 1 il cui risultato è FALSO, mentre l'espressione

$$x^2 = 1$$

è una equazione sui reali, ad incognita x , le cui soluzioni sono $x = \pm 1$. In questo secondo caso, l'insieme delle soluzioni dell'equazione si può scrivere, più formalmente, come

$$\{x \in \mathbb{R} \mid x^2 = 1\} = \{x \in \mathbb{R} \mid x^2 - 1 = 0\} = \{\pm 1\} \subset \mathbb{R}$$

Osservazione 1.6. [AAA05] Il polinomio somma di due polinomi ha grado minore od uguale al massimo dei gradi dei due. Il polinomio prodotto di due polinomi non nulli ha grado la somma dei gradi dei due polinomi.

Esempio 1.7. [AAZ05] Siano dati $f(x) = x^2 + 2x - 1$, $g(x) = x^3 - x^2 + x + 2$ polinomi in $\mathbb{R}[x]$. Allora

$$(x^2 + 2x - 1) \cdot (x^3 - x^2 + x + 2) = \begin{array}{r} x^2 \cdot (x^3 - x^2 + x + 2) + \\ + 2x \cdot (x^3 - x^2 + x + 2) + \\ - 1 \cdot (x^3 - x^2 + x + 2) \end{array} = x^5 + x^4 - 2x^3 + 5x^2 + 3x - 2$$

Osservazione 1.8. [AAC07] Ricordiamo che ogni numero pari si può scrivere come $2n$ ed ogni numero dispari come $2n + 1$ per un opportuno n intero. Se preferite dirlo in altro modo, per ogni numero intero dispari a esiste n intero tale che $a = 2n + 1$. Oppure possiamo dire

$$\forall a \text{ intero dispari } \exists n \text{ intero tale che } a = 2n + 1$$

Analogamente per i pari.

1.2 Gruppi, anelli, campi

Alcune equazioni, e i gli ambiti dove hanno soluzioni.

- $x - 2 = 0$. Soluzioni nei numeri naturali $\mathbb{N}$.
- $x + 2 = 0$. Non ci sono soluzioni naturali. Soluzioni nei numeri interi $\mathbb{Z}$.

- $3x - 2 = 0$. Non ci sono soluzioni intere. Soluzioni nei numeri razionali $\mathbb{Q}$.
- $x^2 - 2 = 0$. Non ci sono soluzioni razionali. Soluzioni nei numeri reali $\mathbb{R}$.
- $x^2 + 2 = 0$. Non ci sono soluzioni reali. Soluzioni nei numeri complessi $\mathbb{C}$.

Definizione 1.9. [AAA87] Sia G un insieme, $e \in G$ e $\oplus$ un operazione tra elementi di G tale che

1. per ogni $a \in G$, $a \oplus e = a$. (e è l'elemento neutro per l'operazione $\oplus$).
2. Per ogni $a, b, c \in G$ $a \oplus (b \oplus c) = (a \oplus b) \oplus c$. Ha quindi senso scrivere $a \oplus b \oplus c$. Si possono quindi evitare queste parentesi. diciamo che $\oplus$ è un operazione associativa.
3. per ogni $a \in G$, $a \neq e$, esiste $b \in G$ tale che $a \oplus b = b \oplus a = e$. Questo b si dice inverso e spesso si indica come a^{-1} .

Allora $(G, e, \oplus)$ si dice gruppo. Se $a \oplus b = b \oplus a$ (l'operazione $\oplus$ è commutativa) per ogni $a, b \in G$, allora $(G, e, \oplus)$ si dice Gruppo commutativo.

Esempio 1.10. [AAA12] Gli insiemi con operazioni $(\mathbb{Z}, 0, +)$, $(\mathbb{Q} - \{0\}, 1, \cdot)$, $(\mathbb{K}[x], 0, +)$, $(\mathbb{K}[x, y, z], 0, +)$ (polinomi nelle tre variabili x, y, z) sono gruppi commutativi

Osservazione 1.11. [AAA18] Siano $A \subset B$ insiemi e $\odot$ un operazione su A . Allora B si dice chiuso rispetto all'operazione $\odot$ se per ogni $x, y \in B$ abbiamo che $x \odot y \in B$.

Esempio 1.12. [AAA19] L'insieme $\mathbb{Q} \subset \mathbb{R}$ è chiuso rispetto alla somma ed al prodotto, ma non all'estrazione di radice quadrata.

Osservazione 1.13. [AAA40] Ricordiamo che non tutte le operazioni sono commutative o associative. L'elevamento a potenza non è nè associativo nè commutativo, dato che

$$3^{27} = \boxed{3^{(3^3)} \neq (3^3)^3} = 3^9 \quad \text{e} \quad 3^2 \neq 2^3$$

Osservazione 1.14. [AAA13] Ricordiamo che il simbolo $\forall$ significa "per ogni", il simbolo $\exists$ significa "esiste", il simbolo $\exists!$ significa "esiste unico", il simbolo $\nexists$ significa "non esiste".

Definizione 1.15. [AAA14] Sia A un insieme, $0, 1 \in A$ e $\oplus, \odot$ operazioni tali che

1. $(A, 0, \oplus)$ sia un gruppo commutativo con neutro 0 (neutro additivo).
2. $\forall a \in A$, $0 \odot a = a \odot 0 = 0$.
3. $\forall a \in A$, $a \odot 1 = a$. (1 è neutro moltiplicativo).
4. $\forall a, b, c \in A$ $a \odot (b \oplus c) = (a \odot b) \oplus a \odot c$ (distributività del prodotto sulla somma)
5. $\forall a, b, c \in A$ $(b \oplus c) \odot a = (b \odot a) \oplus c \odot a$ (distributività del prodotto sulla somma ad destra, nel caso l'anello sia non commutativo)

Allora $(A, 0, 1, \oplus, \odot)$ si dice anello. Se $a \odot b = b \odot a$ per ogni $a, b \in A$, allora $(A, 0, 1, \oplus, \odot)$ si dice anello commutativo. (se l'operazione $\odot$ commuta....)

Esempio 1.16. [AAA15] $(\mathbb{Z}, 0, 1, +, \cdot)$, $(\mathbb{K}[x], 0, 1, +, \cdot)$, $(\mathbb{K}[x, y, z, t], 0, 1, +, \cdot)$ sono anelli commutativi.

Osservazione 1.17. [AAQ15] Per semplicità spesso indicheremo un gruppo od un anello omettendo i neutri, se questi sono ovvi.

Osservazione 1.18. [AAW13] *L'anello è una generalizzazione dei numeri interi $\mathbb{Z}$ con le loro operazioni standard. Il campo è una generalizzazione dei numeri razionali $\mathbb{Q}$ con le loro operazioni standard.*

Definizione 1.19. [AAA16] *Sia $(\mathbb{K}, \oplus, \odot)$ un anello commutativo tale che per ogni $a \in \mathbb{K}$, $a \neq 0$ esista $b \in \mathbb{K}$ tale che $a \odot b = b \odot a = 1$. Allora $(\mathbb{K}, \oplus, \odot)$ si dice campo e b l'inverso moltiplicativo di a o inverso e si indica come a^{-1} o in alcuni casi $\frac{1}{a}$.*

Esempio 1.20. [AAA17] $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sono campi. Se

$$\mathbb{K}(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{K}[x], g(x) \not\equiv_{\mathbb{K}[x]} 0 \right\}$$

allora $(\mathbb{K}(x), +, \cdot)$ è un campo, e si dice campo delle funzioni razionali o campo delle frazioni di $\mathbb{K}[x]$.

Osservazione 1.21. [AAT20] *L'elemento $\frac{x^2+2}{x-2} \in \mathbb{R}[x]$ è ben definito, dato che $x-2 \not\equiv_{\mathbb{K}[x]} 0$. Il fatto che l'equazione $x-1$ sia uguale a zero se $x=1$ è irrilevante.*

Esempio 1.22. [AAA20] $\mathbb{Z} \subset \mathbb{Q}$ non è un campo, visto che 2 non ha inverso.

Definizione 1.23 (Sottocampo). [AAA21] *Sia $(A, \oplus, \odot)$ un campo e $B \subset A$ tale che B sia chiuso rispetto alle operazioni $\oplus, \odot$. Allora B si dice sottocampo di A . Analogamente per anelli e gruppi.*

Osservazione 1.24. [AAA22] $\mathbb{Q}$ è sottocampo di $\mathbb{R}$. L'insieme

$$\mathbb{Z}[x] = \{f(x) \in \mathbb{Q}[x] \mid \text{i coefficienti di } f(x) \text{ sono tutti interi}\}$$

è un sottoanello di $\mathbb{Q}[x]$.

Osservazione 1.25. [AAA25] *Indicheremo sempre con $\mathbb{K}$ un campo generico (per noi, sempre un campo infinito ed in genere, $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Le operazioni saranno in genere sottointese.*

1.3 Prodotto cartesiano

Per descrivere le operazioni in modo piu' formale, ci servirà il concetto di prodotto cartesiano, che risulterà utile in molti altri contesti.

Definizione 1.26. [BBB02] *Siano A, B insiemi. Allora l'insieme delle coppie ordinate composte da un elemento di A ed uno di B si dice prodotto cartesiano di A e B e si scrive $A \times B$. Più formalmente*

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Due elementi di $A \times B$ sono uguali se sono uguali elemento per elemento, ovvero

$$(a, b) = (c, d) \Leftrightarrow a = c \text{ e } b = d$$

Esempio 1.27. [BBB03] *Alcuni esempi:*

1. $\{2, 4, 6\} \times \{0, 1\} = \{(2, 0), (2, 1), (4, 0), (4, 1), (6, 0), (6, 1)\}$
2. $\mathbb{Q} \times \mathbb{R} = \{(q, r) \mid q \in \mathbb{Q}, r \in \mathbb{R}\}$.
3. $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\} = \mathbb{R}^2$. *Il piano reale.*

Possiamo generalizzare il prodotto cartesiano a più di due fattori.

4. $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\} = \mathbb{R}^3$. Lo spazio reale.

5. $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} = \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in \mathbb{R}\}$.

Osservazione 1.28. [BBQ03] Possiamo generalizzare il prodotto cartesiano a più di due fattori. Per esempio

1. $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\} = \mathbb{R}^3$. Lo spazio reale.

2. $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} = \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in \mathbb{R}\}$.

Definizione 1.29. [BBF07] Dato A insieme, un operazione $\oplus$ su A è una funzione

$$\begin{aligned} \oplus: A \times A &\rightarrow A \\ (a, b) &\mapsto a \oplus b \end{aligned}$$

Osservazione 1.30. [BBB04] Notiamo che se $(A, +_A, \cdot_A), (B, +_B, \cdot_B)$ sono anelli, allora possiamo considerare $A \times B$ anello con le operazioni ovvie. Ovvero $(A \times B, \oplus, \odot)$ è un anello con le operazioni

$$\begin{aligned} \oplus: (A \times B) \times (A \times B) &\rightarrow (A \times B) \\ (a, b), (x, y) &\mapsto (a +_A x, b +_B y) \end{aligned}$$

e

$$\begin{aligned} \odot: (A \times B) \times (A \times B) &\rightarrow (A \times B) \\ (a, b), (x, y) &\mapsto (a \cdot_A x, b \cdot_B y) \end{aligned}$$

Dimostrazione. Il neutro additivo è $(0_A, 0_B)$, il neutro moltiplicativo è $(1_A, 1_B)$. Tutte le proprietà che richiediamo alle operazioni $\oplus, \odot$ discendono immediatamente dalle proprietà delle operazioni di anello $+_A, \cdot_A, +_B, \cdot_B$. $\square$

Esempio 1.31. [BBB05] In $\mathbb{R}^2$ abbiamo

$$(1, -3) + (1, 1) = (2, -2), \quad (1, -3) \cdot (1, 1) = (1, -3) \quad (2, 3) \cdot (0, 2) = (0, 6)$$

In $\mathbb{R} \times \mathbb{Q}[x]$ abbiamo

$$(1, x^2 - 1) + (1, 1) = (2, x^2) \quad (2, x^2 + 1) \cdot (3, x^2 - 1) = (6, (x^2 + 1)(x^2 - 1)) = (6, x^4 - 1)$$

In $\mathbb{R}^2$ abbiamo delle patologie:

$$(2, 0) \cdot (0, 3) = (0, 0)$$

Quindi esistono due elementi non nulli il cui prodotto è nullo.

Definizione 1.32. [BBB06] Dato un anello A , un suo elemento $a \neq 0$ è detto zero divisore se esiste $b \in A, b \neq 0$ tale che $a \cdot b = 0$. Chiaramente, secondo la definizione, anche b è uno zero divisore.

Esempio 1.33. [BBB07] $(\mathbb{R}^2, +, \cdot)$ non è un campo. Basta far vedere che l'elemento $(0, 1)$, non nullo, non è invertibile, dato che in un campo tutti gli elementi non nulli devono avere inverso. Se fosse invertibile, esisterebbe il suo inverso, un elemento $(x, y) \in \mathbb{R}^2$ tale che

$$(x, y) \cdot (0, 1) = (1, 1) \Leftrightarrow (0, y) = (1, 1) \Leftrightarrow \begin{cases} 0 = 1 \\ y = 1 \end{cases}$$

che è assurdo perchè $1 \neq 0$. Analogamente, $\mathbb{R}^n$ non è un campo con le operazioni ovvie.

Definizione 1.34. [CCW37] Ricordiamo che

1. due funzioni

$$\begin{array}{ccc} f: & A & \rightarrow & B \\ & a & \mapsto & f(a) \end{array} \quad \begin{array}{ccc} g: & A & \rightarrow & B \\ & a & \mapsto & g(a) \end{array}$$

sono uguali come funzioni ($f \equiv g$) se e solo se

$$\forall x \in A \quad f(x) = g(x)$$

2. L'operazione di composizione di funzioni è

$$\begin{array}{ccc} \circ: & \{F: \mathbb{R} \rightarrow \mathbb{R}\} \times \{F: \mathbb{R} \rightarrow \mathbb{R}\} & \rightarrow & \{F: \mathbb{R} \rightarrow \mathbb{R}\} \\ & (f, g) & \mapsto & f \circ g: \mathbb{R} \rightarrow \mathbb{R} \\ & & & x \mapsto f(g(x)) \end{array}$$

Esempio 1.35. [AAB99] Sia $\mathbb{F}$ l'insieme delle funzioni da $\mathbb{R}$ ad $\mathbb{R}$. Queste non formano un gruppo con la composizione perchè non sempre esiste l'inverso. Dimostriamo che l'insieme non è un gruppo con un controesempio: La funzione costante

$$\begin{array}{ccc} f: & \mathbb{R} & \rightarrow & \mathbb{R} \\ & x & \mapsto & 1 \end{array}$$

non è invertibile, quindi non ha inverso rispetto alla composizione.

Esempio 1.36. [AAB98] Sia $\mathbb{F}$ l'insieme delle funzioni bigettive da $\mathbb{R}$ ad $\mathbb{R}$ formano un gruppo non commutativo. Che siano un gruppo è immediato [cfr. corso di Analisi I per le proprietà delle funzioni]. Dimostriamo che il gruppo non è commutativo con un controesempio:

esistono due funzioni bigettive

$$\begin{array}{ccc} f: & \mathbb{R} & \rightarrow & \mathbb{R} \\ & x & \mapsto & x^3 \end{array} \quad \begin{array}{ccc} g: & \mathbb{R} & \rightarrow & \mathbb{R} \\ & x & \mapsto & x + 1 \end{array}$$

tali che

$$(f \circ g)(x) = f(g(x)) = f(x + 1) = (x + 1)^3 \neq x^3 + 1 = g(x^3) = g(f(x)) = (g \circ f)(x)$$