Capitolo 1

Prima lezione: polinomi, operazioni elementari, ed algebra astratta

Ricordiamo brevemente alcune nozioni di base sui polinomi.

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

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

1. *Il* grado *di* $f(x)$ *è* n*, e si scrive* $\deg f(x)$*.*
2. *I reali* $a_n, \ldots, a_0$ *sono i* coefficenti *del polinomio.*
3. *I* termini *del polinomio sono gli* x^i *per cui il corrispondente coefficente* a_i *sia non nullo.*
4. *Il* termine di testa *di* $f(x)$ *è* x^n*.*
5. *Il* coefficente 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).*

Osservazione 1.2. [AAA04] *Il grado del polinomio* 0 *non è definito.*

Esempio 1.3. [AAA03] *Dato* $f(x) = x^5 + 2x - 1$

1. $\deg(f(x)) = 5$*.*
2. *Il coefficente di testa di* $f(x)$ *è* 1*. Il termine noto è* -1*.*
3. *I coefficenti 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* $x^5, x^1, 1 = x^0$*.*
4. *Il termine di testa è* x^5*.*

Definizione 1.4. [AAA01] *Siano* $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i \in \mathbb{R}[x]$*. Allora*

- *Principio di identità dei polinomi:*

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

- *Somma e prodotto*

$$f(x)+g(x)=\sum_{i=0}^{\max n,m}(a_i+b_i)x^i$$

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

Esempio 1.5. [AAX03]

- *I polinomi* $f(x)=x^5+2x-1$ *e* $g(x)=x^3+2x-1$ *sono diversi dato che hanno grado diverso* $f(x)\underset{\mathbb{R}[x]}{\not\equiv}g(x)$.
- $x^2-2x+1\underset{\mathbb{R}[x]}{\not\equiv}x^3-2x^2+x=x(x^2-2x+1)$ *dato che hanno il termine noto diverso, anche se hanno le stesse radici.*

Esercizio 1.6. [AAX04] *Dire per quali* $a\in\mathbb{R}$, *i polinomi* $x^2+4x-1, ax^2+(3a-1)x+5a\mathbb{R}[x]$ *sono uguali.*

I polinomi hanno lo stesso grado. Per avere $x^2+4x-1\equiv ax^2+(3a-1)x+5a$ *dobbiamo avere che i coefficienti sono uguali uno a uno, ovvero*

$$\begin{cases}1=a & \textit{grado 2}\\ 4=3a-1 & \textit{grado 1}\\ -1=5a & \textit{grado 0}\end{cases}$$

Dato che dalla prima equazione si ottiene $a=1$ *e dalla seconda* $a=-\frac{1}{5}$, *il sistema è impossibile e i polinomi sono diversi per ogni* $a\in\mathbb{R}$ *(*$\forall\ a\in\mathbb{R}$*).*

Osservazione 1.7. *Ricordiamo che l'espressione*

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

è una uguaglianza tra polinomi, il cui risultato è FALSO, mentre l'espressione

$$x^2=1$$

è una equazione sui reali, le cui soluzioni sono $x=\pm1$. *In questo secondo caso, l'insieme delle soluzioni dell'equazione si può scrivere, più formalmente, come*

$$\{x\in\mathbb{R}\ \mid\ x^2=1\}=\{x\in\mathbb{R}\ \mid\ x^2-1=0\}=\{\pm1\}$$

Osservazione 1.8. [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 1.9. [AAZ05] *Siano dati* $f(x)=x^2+2x-1$, $g(x)=x^3-x^2+x+2$ *polinomi in* $\mathbb{R}[x]$. *Allora*

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

Osservazione 1.10. [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*

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

Analogamente per i pari.

Osservazione 1.11. [AAA02] *Dati $a, b \in \mathbb{R}$, $n \in \mathbb{N}$. Ricordiamo le formule*

1. $a^2 - b^2 = (a+b)(a-b)$.
2. $a^2 + b^2$ *non si può fattorizzare su* $\mathbb{R}$.
3. $a^3 - b^3 = (a-b)(a^2+ab+b^2)$.
4. $a^3 + b^3 = (a+b)(a^2-ab+b^2)$.
5. *Teorema del Binomio [Dimostrazione per induzione. Cfr. corso di Analisi.]*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

dove $\binom{n}{i}$ *è l'elemento della n-esima riga, i-esima colonna del triangolo di Tartaglia. Ricordiamo che*

$$\binom{n}{i} = \frac{n!}{k!(n-i)!} \qquad \text{dove } n! = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 \text{ e } 0! = 1$$

Esempio 1.12. [AAA08] *Abbiamo che*

$$(2x-3)^4 = \binom{4}{0}\cdot(2x)^4\cdot(-3)^0 + \binom{4}{1}\cdot(2x)^3\cdot(-3)^1 + \binom{4}{2}\cdot(2x)^2\cdot(-3)^2 + \\ + \binom{4}{3}\cdot(2x)^1\cdot(-3)^3 + \binom{4}{4}\cdot(2x)^0\cdot(-3)^4$$

dato che

$$\begin{aligned}
\binom{4}{0} &= \frac{4!}{0!4!} = \frac{4\cdot 3\cdot 2\cdot 1}{1\cdot(4\cdot 3\cdot 2\cdot 1)} = 1 \\
\binom{4}{1} &= \frac{4!}{1!3!} = \frac{4\cdot 3\cdot 2\cdot 1}{1\cdot(3\cdot 2\cdot 1)} = 4 \\
\binom{4}{2} &= \frac{4!}{2!2!} = \frac{4\cdot 3\cdot 2\cdot 1}{(2\cdot 1)(2\cdot 1)} = 6 \\
\binom{4}{3} &= \frac{4!}{3!1!} = \frac{4\cdot 3\cdot 2\cdot 1}{(3\cdot 2\cdot 1)\cdot 1} = 4 \\
\binom{4}{4} &= \frac{4!}{4!0!} = \frac{4\cdot 3\cdot 2\cdot 1}{(4\cdot 3\cdot 2\cdot 1)\cdot 1} = 1
\end{aligned}$$

$$\begin{aligned}
&= 16x^4 + 4\cdot(8x^3)\cdot(-3) + 6\cdot(4x^2)\cdot 9 + 4\cdot(2x)\cdot(-27) + 81 \\
&= 16x^4 - 96x^3 + 216x^2 - 216x + 81
\end{aligned}$$

Esempio 1.13. [AAA10] *Abbiamo che*

$$x^6 - 1 = (x^3-1)(x^3+1) = (x-1)(x^2+x+1)(x+1)(x^2-x+1)$$

Alternativamente,

$$x^6 - 1 = \left(\left(x^2\right)^3 - 1^3\right) = (x^2-1)(x^4+x^2+1)$$

da cui vedremo che, per il teorema della fattorizzazione unica, $(x^4+x^2+1) = (x^2+x+1)(x^2-x+1)$

Esempio 1.14. [AAA07] $x^5 - 32 = x^5 - 2^5 = (x-2)(x^4+2x^3+4x^2+8x+16)$

1.1 Divisione con resto

Come per gli interi, nei polinomi su un campo si può definire una divisione con resto.

Proposizione 1.15 (Divisione con resto)**.** `[AAC02]` *Dati i due polinomi in* $\mathbb{K}[x]$

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad e \quad g(x) = \sum_{i=0}^{m} b_i x^i$$

esistono unici $q(x), r(x) \in \mathbb{K}[x]$ *tali che*

$$f(x) = q(x)g(x) + r(x) \text{ con } r(x) = 0 \text{ o } \deg(r(x)) < \deg(g(x))$$

Esempio 1.16. `[AAA80]` *Esempio di divisione. Dividiamo* $x^4 + x^3 - 2x^2 - 3x + 1$*, per* $x^3 + x$

```
DivPoly(x^4+x^3-2x^2-3x+1,x^3+x);
Passo 1 ho        x^4 + x^3 - 2x^2 - 3x + 1 moltiplico per x
Passo 1 sottraggo x^4 + x^2
Passo 1 ottengo       x^3 - 3x^2 - 3x + 1

Passo 2 ho        x^3 - 3x^2 - 3x + 1 moltiplico per 1
Passo 2 sottraggo x^3 + x
Passo 2 ottengo       -3x^2 - 4x + 1

Resto=-3x^2 - 4x + 1
Quoto=x + 1
```

Quindi

$$x^4 + x^3 - 2x^2 - 3x + 1 = (x^3 + x)(x + 1) + (-3x^2 - 4x + 1)$$

Esempio 1.17. `[AAA81]` *Dividiamo* $x^7 + x^4 - 1$*, per* $x^3 + x + 2$

```
DivPoly(x^7+x^4-1,x^3+x+2);

Passo 1 ho        x^7 + x^4 - 1 moltiplico per x^4
Passo 1 sottraggo x^7 + x^5 + 2x^4
Passo 1 ottengo       -x^5 - x^4 - 1

Passo 2 ho        -x^5 - x^4 - 1 moltiplico per -x^2
Passo 2 sottraggo -x^5 - x^3 - 2x^2
Passo 2 ottengo        -x^4 + x^3 + 2x^2 - 1

Passo 3 ho        -x^4 + x^3 + 2x^2 - 1 moltiplico per -x
Passo 3 sottraggo -x^4 - x^2 - 2x
Passo 3 ottengo        x^3 + 3x^2 + 2x - 1

Passo 4 ho        x^3 + 3x^2 + 2x - 1 moltiplico per 1
Passo 4 sottraggo x^3 + x + 2
Passo 4 ottengo       3x^2 + x - 3

Resto=3x^2 + x - 3
Quoto=x^4 - x^2 - x + 1
```

Quindi

$$x^7 + x^4 - 1 = (x^3 + x + 2)(x^4 - x^2 - x + 1) + 3x^2 + x - 3$$

Esempio 1.18. [AAA06] *Vogliamo risolvere l'equazione.*

$$\frac{x^5 - 2x^3 + x^2 - 2}{x^3 + 1} = 0$$

Dividiamo $x^5 - 2x^3 + x^2 - 2$*, per* $x^3 + 1$

```
DivPoly(x^5 - 2x^3 + x^2 - 2,x^3+1);
Passo 1 ho        x^5 - 2x^3 + x^2 - 2 moltiplico per x^2
Passo 1 sottraggo x^5 + x^2
Passo 1 ottengo       -2x^3 - 2

Passo 2 ho        -2x^3 - 2 moltiplico per -2
Passo 2 sottraggo -2x^3 - 2
Passo 2 ottengo         0

Resto=0
Quoto=x^2 - 2
```

ottenendo

$$x^5 - 2x^3 + x^2 - 2 = (x^2 - 2)(x^3 + 1)$$

Quindi

$$\begin{aligned} \frac{x^5 - 2x^3 + x^2 - 2}{x^3 + 1} &= 0 \\ x^2 - 2 &= 0 \\ x &= \pm\sqrt{2} \end{aligned}$$

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 $\mathbb{Q}$.
- $x^2 - 4 = 0$. 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 1.19. [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 *spesso si indica come* a^{-1}.

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

Osservazione 1.20. [AAA11] *Nella definizione precedente, quando diciamo che* $\oplus$ *è un operazione intendiamo che gli insiemi siano chiusi rispetto all' operazioni, ovvero che l'operazione di due elementi dell'insieme sia un elemento dell'insieme stesso.*

Osservazione 1.21. [AAA18] *Sia* $A \subset B$ *insiemi e* $\cdot$ *un operazione su* A. *Allora* B *si dice* chiuso *rispetto all'operazione* $\odot$ *se per ogni* $x, y \in B$ $x \odot y \in B$

Esempio 1.22. [AAA19] $\mathbb{Q} \subset \mathbb{R}$ *è chiuso rispetto alla somma ed al prodotto, ma non all'estrazione di radice quadrata.*

Osservazione 1.23. [AAA40] *Ricordiamo che non tutte le operazioni sono commutative o associative. L'elevamente a potenza non è nè associativo nè commutativo, dato che*

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

Esempio 1.24. [AAA12] $(\mathbb{Z}, +)$, $(\mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{K}[x], +)$, $(\mathbb{K}[x, y, z], +)$ *(polinomi nelle tre variabili* x, y, z*) Sono gruppi commutativi*

Osservazione 1.25. [AAA13] *Ricordiamo che il simbolo* $\forall$ *significa "per ogni", il simbolo* $\exists$ *significa "esiste" ed il simbolo* $\exists!$ *significa "esiste unico".*

Definizione 1.26. [AAA14] *Sia* A *un insieme,* $0, 1 \in A$ *e* $\oplus, \odot$ *operazioni tali che*

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

Esempio 1.27. [AAA15] $(\mathbb{Z}, + \cdot)$, $(\mathbb{K}[x], +, \cdot)$, $(\mathbb{K}[x, y, z, t], +, \cdot)$ *sono anelli commutativi.*

Definizione 1.28. [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 1.29. [AAA17] $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ *sono campi. Se*

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

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

Esempio 1.30. [AAA20] $\mathbb{Z} \subset \mathbb{Q}$ *non è un campo, visto che* 2 *non ha inverso..*

Definizione 1.31 (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 1.32. [AAA22] $\mathbb{Q}$ *è sottocampo di* $\mathbb{R}$*. L'insieme*

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

è un sottoanello di $\mathbb{Q}[x]$*.*

Esercizio 1.33. [AAA24] *Sia* i *un oggetto tale che* $i^2 = -1$ *(quindi chiaramente non un numero reale). Allora dimostriamo che*

$$\mathbb{R}[i] = \{a + ib \mid a, b \in \mathbb{R}\}$$

è un campo con le operazioni ovvie derivate da quelle di $\mathbb{R}$ *e* $a + ib = 0 \Leftrightarrow a = 0$ *e* $b = 0$*.*

Svolgimento.
- Se $b \neq 0$, abbiamo $a + ib = 0 \Leftrightarrow i = -\frac{a}{b}$ e dato che $a, b \in \mathbb{R}$, $-\frac{a}{b} \in \mathbb{R}$ che implica $i \in \mathbb{R}$. Ma questo è impossibile, perchè nessun numero reale ha quadrato negativo. Quindi b deve essere nullo.
- Se $b = 0$, abbiamo $a + ib = 0 \Leftrightarrow a = 0$.

Quindi $a + ib = 0 \Leftrightarrow a = 0$ e $b = 0$

Bisogna dimostrare che ogni elemento non nullo di $\mathbb{R}[i]$ ha inverso in $\mathbb{R}[i]$, ovvero che per ogni $a + ib \in \mathbb{Q}[i]$, con a, b non ambedue nulli possiamo trovare un elemento $x + iy \in \mathbb{R}[i]$ tale che

$$(a + ib) \cdot (x + iy) = 1$$

Proviamo come candidato $x + iy = \frac{a-ib}{a^2+b^2}$, ovvero

$$x = \frac{a}{a^2 + b^2} \qquad y = -\frac{b}{a^2 + b^2}$$

che è ben definito in quanto nelle nostre ipotesi $a^2 + b^2 \neq 0$. Abbiamo che

$$(a + ib) \cdot \frac{a - ib}{a^2 + b^2} = \frac{a^2 - abi + abi + b^2}{a^2 + b^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1$$

Quindi ogni elemento non nullo $a + ib$ ha inverso moltiplicativo $\frac{a-ib}{a^2+b^2}$. □

Esercizio 1.34 (Proposto)**.** [AAT23] *Trovare, se esiste, un campo* B *tale che* $\mathbb{Q} \subsetneq B \subsetneq \mathbb{R}$*.*

Esercizio 1.35 (Proposto)**.** [AAA23] *L'insieme*

$$\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\} \subset \mathbb{R}$$

è un sottocampo di $(\mathbb{R}, +, \cdot)$ *che contiene* $\mathbb{Q}$*? Determinare se del caso la formula dell'inverso ed il principio di identità.*

Osservazione 1.36. [AAA25] *Indicheremo sempre con* $\mathbb{K}$ *un campo generico (per noi, sempre un campo infinito ed in genere,* $\mathbb{Q}, \mathbb{R}, \mathbb{C}$*). Le operazioni saranno in genere sottointese.*