TEORIA DI ALGEBRA LINEARE

RACCOLTA DI TUTTE LE DEFINIZIONI E I TEOREMI SCRITTI NELLE DISPENSE DEL PROFESSORE MASSIMO CABOARA

INGEGNERIA CHIMICA

ANNO 2021/2022 – PROFESSORE M. CABOARA

A cura di Elena C.

master COPY COPISTERIA

master COPY COPISTERIA

master COPY

INDICE:

- CAPITOLO 1- POLINOMI
- CAPITOLO 2-NUMERI COMPLESSI
- CAPITOLO 3 –SISTEMI
- CAPITOLO 4 –MATRICI
- CAPITOLO 5 –SPAZI VETTORIALI
- CAPITOLO 6 – MORFISMI DI SPAZI VETTORIALI
- CAPITOLO 7 –AUTOVETTORI E AUTOVALORI
- PAGINE UTILI PER L'ORALE

master COPY COPISTERIA

master COPY

Polinomi

1.1 Operazioni elementari

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).*

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:*

$$f(x) \equiv_{\mathbb{R}[x]} g(x) \Leftrightarrow n = m \text{ e } \forall\ i = 1, \ldots, n\ a_i = b_i$$

- *Somma e prodotto*

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

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

Definizione 1.12. [AAA87] *Sia* G *un insieme,* $e \in G$ *e* $\oplus$ *un operazione 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 additivo *o* opposto *di* a *e spesso si indica come* $-a$.

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.

Definizione 1.17. [AAA14] *Sia* A *un insieme,* $0, 1 \in A$ *e* $\oplus, \odot$ *operazioni tali che*

1. $(A, \oplus)$ *sia un gruppo commutativo con neutro additivo* 0.
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....)*

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* $\frac{1}{a}$.

Definizione 1.24 (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.*

Definizione 1.29. [AAA26] *Siano* $f(x), g(x) \in \mathbb{K}[x]$. *Allora*

Diciamo che $g(x)$ *divide* $f(x)$ *se esiste* $q(x) \in \mathbb{K}[x]$ *tale che* $f(x) = q(x)g(x)$.

Definizione 1.30. [AAA27] *Un polinomio* $f(x) \in \mathbb{K}[x]$ *di grado* ≥ 1 *che non abbia divisori propri (diversi dal polinomio stesso* $f(x)$*) si dice* irriducibile. *Un polinomio che non sia irriducibile si dice* riducibile. *Gli elementi di* $\mathbb{K}$ *si indicano spesso come* scalari.

Teorema 1.31 (Teorema di Fattorizzazione Unica). [AAA28] *Sia* $f(x) \in \mathbb{K}[x]$. *Allora esistono unici* $f_1(x), \ldots, f_n(x) \in \mathbb{K}[x]$ *irriducibili distinti e* $\alpha_1, \ldots, \alpha_n \in \mathbb{N}^+$ *(gli interi positivi) tali che*

$$f(x) = \prod_{i=1}^{n} f_i(x)^{\alpha_i} = f_1(x)^{\alpha_1} \cdots f_n(x)^{\alpha_n}$$

I polinomi $f_i(x)$ *si dicono* fattori irriducibili *di* $f(x)$ *e i naturali* α_i *sono le loro* molteplicità.

Definizione 1.34. [AAA31] *Se due polinomi in* $\mathbb{K}[x]$ *non hanno fattori irriducibili comuni, allora* $f(x), g(x)$ *sono detti* coprimi.

1.4 Radici e Ruffini

Definizione 1.39. [AAA41] *Sia* $f(x) = \sum_{i=0}^{n} a_i x^i$ *e* $c \in \mathbb{K}$. *Allora il numero reale*

$$f(c) = \sum_{i=0}^{n} a_i c^i$$

è detto valutazione *di* $f(x)$ *in* c.

Definizione 1.40. [AAA42] *Sia* $f(x) \in \mathbb{K}[x]$ *e* $a \in \mathbb{K}$. *Se* $f(a) = 0$ *allora* a *è detta* radice *del polinomio* $f(x)$.

Teorema 1.42 (Teorema delle Radici). [AAA43] *Sia*

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_n x^n \in \mathbb{Z}[x]$$

un polinomio di grado n (e quindi con $a_n \neq 0$) con coefficenti in $\mathbb{Z}$. Allora abbiamo che tutte le radici razionali sono date da un divisore del termine noto diviso un divisore del termine di testa. Ovvero, se $b_1, \ldots, b_k$ sono i divisori del termine di testa $a_n \in \mathbb{Z}$ e $c_1, \ldots, c_p$ i divisori del termine noto a_0 abbiamo che, per $a \in \mathbb{Q}$

$$f(a) = 0 \Rightarrow a = \pm \frac{c_i}{b_j} \quad \text{per opportuni } i : 1 \ldots k, \quad j : 1 \ldots p$$

Teorema 1.44 (Teorema di Ruffini). [AAA45] *Sia $f(x)$ un polinomio in $\mathbb{K}[x]$ e $a \in \mathbb{K}$. Allora*

$$f(a) = 0 \Leftrightarrow (x - a) \mid f(x)$$

Ovvero a è una radice di $f(x)$ se e solo se $x - a$ è un fattore di $f(x)$,

Definizione 1.49. [AAA50] *Sia $f(x) \in \mathbb{K}[x]$ e $a \in \mathbb{K}$ una sua radice. Allora a è detta* radice di molteplicità *k del polinomio $f(x)$ se*

$$(x - a)^k \mid f(x) \text{ e } (x - a)^{k+1} \nmid f(x)$$

Teorema 1.51 (Criterio di Eisenstein). [AAA52] *Sia $f(x) = \sum_{i=0}^{n} \in \mathbb{Z}[x]$ di grado n. Allora se esiste $p \in \mathbb{N}$, primo tale che*

$$p \nmid a_n \quad p \mid a_{n-1}, \ldots, p \mid a_0 \quad \text{e} \quad p \nmid a_0^2$$

il polinomio $f(x)$ è irriducibile su $\mathbb{Q}[x]$. Si dice che $f(x)$ è irriducibile per Eisenstein, con primo p.

Proposizione 1.59 (Divisione con resto). [AAC02] *Dati i due polinomi in $\mathbb{K}[x]$*

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

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

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

Definizione 1.63. [AAA88] *Sia $f(x) \in \mathbb{K}[x]$ con $LC(f(x)) = 1$ (il coefficente del termine di testa è 1). Allora il polinomio $f(x)$ si dice* monico.

Definizione-Proposizione 1.65 (Massimo Comun Divisore, Minimo Comune Multiplo). [AAA57] *Dati $f(x), g(x) \in \mathbb{K}[x]$.*

- *Il* massimo comun divisore *di $f(x), g(x)$ e' il polinomio monico di grado minore tra quelli che dividono sia $f(x)$ che $g(x)$. Tale polinomio esiste sempre, al limite è 1.*
- *Il* minimo comune multiplo *di $f(x), g(x)$ e' il polinomio monico di grado maggiore tra quelli che sono divisi sia da $f(x)$ che da $g(x)$. Tale polinomio esiste sempre, al limite è $f(x)g(x)$.*
- $\gcd(f(x), g(x)) \operatorname{lcm}(f(x), g(x)) = f(x) \cdot g(x)$.

Proposizione 1.67. [AAA59] *Siano*

$$f(x) = \prod_{i=1}^{n} f_i(x)^{\alpha_i} \quad \text{e} \quad g(x) = \prod_{i=1}^{m} g_i(x)^{\beta_i}$$

due polinomi in $\mathbb{K}[x]$. Allora

1. *Il massimo comun divisore di $f(x), g(x)$ è dato dal prodotto di tutti i fattori comuni ai due polinomi presi una sola volta con minimo esponente.*
2. *Il minimo comune multiplo di $f(x), g(x)$ è dato dal prodotto di tutti i fattori non comuni ai due polinomi e di quelli comuni presi una sola volta con massimo esponente.*

Proposizione 1.71 (Algoritmo Euclideo). [AAA63] *Dati $f_0(x), f_1(x) \in \mathbb{K}[x]$, con $\deg f_0(x) \geq \deg f_1(x)$. Sia*

$$f_i(x) = q_i(x) f_{i+1}(x) + f_{i+2}(x)$$

la divisione con resto di $f_i(x)$ rispetto a $f_{i+1}(x)$, per opportuni $q_i(x)$. La sequenza di coppie

$$(f_i(x), f_{i+1}) \longrightarrow (f_{i+1}, f_{i+2}(x))$$

termina con una coppia $(g(x), 0)$, $\gcd(f_0(x), f_1(x)) = g(x)$.

Proposizione 1.73. [AAA82] *Conservando la notazione della proposizione precedente, notiamo alcuni fatti utili:*

1. $\gcd(f(x), g(x)) = \gcd(g(x), h(x))$
2. *Il* gcd *dei polinomi di ogni coppia è lo stesso.*
3. *Dati $f(x), g(x), h(x) \in \mathbb{K}[x]$ possiamo definire*

   $$\gcd(f(x), g(x), h(x)) = \gcd(\gcd(f(x), g(x)), h(x))$$

   Abbiamo altresì

   $$\gcd(\gcd(f(x), g(x)), h(x)) = \gcd(f(x), \gcd(g(x), h(x)))$$

4. *Ricordiamo che $\forall\ f(x) \in \mathbb{K}[x]$ $\gcd(f(x), 0) = 1$ e che $\gcd(0, 0) = 0$.*

Dimostrazione. Tutte queste proprietà discendono immediatamente dall'equivalenza delle tre definizioni del gcd. □

Un esempio di esecuzione dell'algoritmo euclideo sugli interi. È lo stesso meccanismo dei polinomi, ma la semplicità dei conti lo rende piu' comprensibile.

Proposizione 1.82. [AAA70] *Dati $f(x), g(x) \in \mathbb{K}[x]$, $a \in \mathbb{K}$, $a \neq 0$ e $h(x) \in \mathbb{K}[x]$ coprimo con $f(x), g(x)$*

1. $\gcd(f(x), ag(x)) = \gcd(f(x), g(x))$. *Posso quindi raccogliere e dividere per elementi non nulli del campo a piacere.*
2. $\gcd(f(x), h(x)g(x)) = \gcd(f(x), g(x))$. *Posso quindi eliminare un fattore che sia coprimo con entrambi i polinomi.*

Definizione 1.84. [AAA72] *Un polinomio $f(x) \in \mathbb{K}[x]$ che abbia fattorizzazione su $\mathbb{K}[x]$ in irriducibili distinti di molteplicità 1, ovvero*

$$\prod_{i=1}^{n} f_i(x)^{\alpha} \quad \text{con } \alpha_1 = \cdots = \alpha_n = 1$$

si dice squarefree.

Definizione 1.85. [AAA73] *Dato $f(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + + a_1 x + a_0 \in \mathbb{K}[x]$ definiamo come la* derivata FORMALE *di $f(x)$ il polinomio in $\mathbb{K}[x]$*

$$f'(x) = \sum^{n} i a_i x^{i-1} = n a_n x^{n-1} + n - 1 a_{n-1} x^{n-2} + \cdots + a_1$$

Proposizione 1.87. [AAA75] *Dati $f(x), g(x) \in \mathbb{K}[x]$ abbiamo che*

1. $(f(x) + g(x))' = f'(x) + g'(x)$.
2. $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.
3. $\deg f'(x) = \deg f(x) - 1$.
4. *La derivata di una costante è* 0.

Dimostrazione. In ogni caso, basta applicare la definizione di derivata formale e fare i conti □

Teorema 1.88. [AAA76] *[Criterio della molteplicità o del* gcd*] Sia $f(x) \in \mathbb{K}[x]$ e una sua fattorizzazione in irriducibili su $\mathbb{K}[x]$*

$$f(x) = \prod_{i=1}^{n} f_i(x)^{\alpha_i}$$

Allora

1. $\gcd(f(x), f'(x)) = \prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$.
2. $\gcd(f(x), f'(x)) | f(x)$
3. *$f(x)$ è squarefree se e solo se $\gcd(f(x), f'(x)) = 1$.*
4. *Il polinomio $\frac{f(x)}{\gcd(f(x), f'(x))}$ è squarefree.*



Dimostrazione.

1. Per le regole di derivazione del prodotto e della somma,

$$\begin{aligned} f'(x) &= (f_1(x)^{\alpha_1} \cdots f_n(x)^{\alpha_n})' \\ &= \alpha_1 f_1(x)^{\alpha_1 - 1} f_2(x)^{\alpha_2} \cdots f_n(x)^{\alpha_n} + \cdots \\ &\qquad + f_1(x)^{\alpha_1} \alpha_2 f_2(x)^{\alpha_2 - 1} f_3(x)^{\alpha_3} \cdots f_n(x)^{\alpha_n} + \cdots \\ &\qquad + f_1(x)^{\alpha_1} \cdots f_{n-1}(x)^{\alpha_{n-1}} \alpha_n f_n(x)^{\alpha_n - 1} \qquad (1.1) \\ &= \prod_{i=1}^{n} f_i(x)^{\alpha_i - 1} \cdot \sum_{i=1}^{n} \left(\prod_{j \neq i} f_j^{\alpha_j} \right) \end{aligned}$$

   raccogliendo il fattore $\prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$ comune a tutti gli addendi. Vediamo che

   - il polinomio $\prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$ divide sia $f(x)$, per costruzione, che $f'(x)$.
   - Si può dimostrare [Lasciato per esercizio] che un polinomio che divida sia $f(x)$ che $f'(x)$ deve necessariamente essere diviso da $\prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$ e che quindi $\prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$ è il divisore comune di grado minore possibile ed abbiamo

$$\gcd(f(x), f'(x)) = \prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}$$

2. Segue immediatamente dalla definizione di gcd.
3. Abbiamo che

$$\begin{aligned} \frac{f(x)}{\gcd(f(x), f'(x))} &= \frac{\prod_{i=1}^{n} f_i(x)^{\alpha_i}}{\prod_{i=1}^{n} f_i(x)^{\alpha_i - 1}} \\ &= f_1(x) \cdots f_n(x) \end{aligned}$$

   e quindi $f(x)$ è squarefree se e solo se $\gcd(f(x), f'(x)) = 1$.

4. Segue immediatamente da quanto sopra.

