

Calcolo Numerico

Appunti

Giovanni Palma e Alex Bastianini

Contents

Chapter 1

Fondamenti della Teoria delle Rappresentazioni _____ Page _____

- 1.1 Robe per Informatici
Gruppi — • Campo — • Anelli —
- 1.2 Struttura algebrica

Chapter 1

Fondamenti della Teoria delle Rappresentazioni

1.1 Robe per Informatici

1.1.1 Gruppi

Definition 1.1.1: Gruppo

E' una coppia (G, \cdot) dove:

- G e' un insieme non vuoto
- \cdot e' un'operazione $G \times G \rightarrow G$ (chiusa su G)

Che soddsfa gli assiomi:

- Associativita'
- Esistenza dell'elemento *neutro*
- Esistenza dell'*inverso* per ogni $a \in G$

Definition 1.1.2: Sottogruppo

Dato un gruppo (G, \cdot) ,

Proprieta' fondamentali

- **Unicita'** dell'elemento inverso e neutro
- **Inverso del prodotto:** $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
- **Legge della cancellazione:** $a \cdot b = a \cdot c$ moltiplicando a sx per a^{-1} si ottiene $b = c$

Teoremi principali

Theorem 1.1.1 Lagrange

Se G e' un gruppo finito e H un suo sottogruppo, allora la cardinalita' degli elementi di G divide esattamente

1.1.2 Campo

Definition 1.1.3: Campo

Un **campo** K è una struttura algebrica dotata di due operazioni:

- **Somma:** t.c. $(K, +)$ è un *gruppo abeliano* (con elem neutro 0)
- **Prodotto:** t.c. $(K \setminus \{0\}, \cdot)$ è un *gruppo abeliano* (con elem neutro 1)
- Vale la proprietà distributiva del prodotto rispetto alla somma

Proprietà Fondamentali

Caratteristica del Campo ($\text{char}(K)$): È il più piccolo intero positivo p tale che sommando l'elemento identità 1 a se stesso p volte si ottiene 0 (cioè $1 + \dots + 1 = 0$).

Chiusura Algebrica: Un campo K si dice algebricamente chiuso se ogni polinomio non costante a coefficienti in K ha almeno una radice in K . Il campo \mathbb{C} è algebricamente chiuso, mentre \mathbb{R} non lo è (ad esempio, $x^2 + 1 = 0$).

1.1.3 Anelli

Definition 1.1.4: Anello

Un anello è una terna $(R, +, \cdot)$, dove R è un insieme dotato di due operazioni binarie interne (somma e prodotto), tale che:

- $(R, +)$ è un *gruppo abeliano*
- (R, \cdot) è un *monoide*:
 - Associatività: $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in R$
 - Unità: $\exists 1 \in R \mid a \cdot 1 = 1 \cdot a = a, \forall a \in R$
- Proprietà distributiva (sx e dx)

Note:

A differenza dei campi, in un anello generale non si richiede che il prodotto sia commutativo ($a \cdot b$ può essere diverso da $b \cdot a$), e non si richiede che ogni elemento non nullo abbia un inverso moltiplicativo (cioè non si può sempre "dividere").

Proprietà fondamentali

Per manipolare gli anelli, definiamo alcune categorie di elementi e strutture interne fondamentali:

- **Divisori dello zero:** Un elemento $a \neq 0$ si dice divisore dello zero se esiste un elemento $b \neq 0$ tale che $a \cdot b = 0$. Si osservi che nei campi questa eventualità non si verifica mai per definizione.
- **Elementi Invertibili (Unità):** Gli elementi di R che possiedono un inverso moltiplicativo formano un gruppo rispetto all'operazione di prodotto, indicato con il simbolo R^\times (o $U(R)$).
- **Ideali:** Un sottoinsieme $I \subseteq R$ è un **ideale sinistro** se è un sottogruppo additivo e "assorbe" il prodotto da sinistra: ovvero, per ogni $r \in R$ e ogni $x \in I$, si ha che $r \cdot x \in I$. Gli ideali rappresentano per gli anelli ciò che i sottogruppi normali rappresentano per i gruppi, permettendo la costruzione degli **anelli quoziente** R/I .

1.2 Struttura algebrica

Cosa vuol dire combinatoria algebrica?

Vuol dire studiare strutture algebriche (gruppi, anelli, campi, etc.) attraverso la combinatoria.

Definition 1.2.1: Struttura algebrica

Si definisce struttura algebrica una coppia $(G, *)$ dove G è un insieme e $*$ è una operazione binaria su G

Example 1.2.1 (Strutture algebriche)

- **Gruppo:** $(G, *)$ con $*$ binaria e associativa, G con elemento neutro e ogni elemento ha un inverso
- **Anello:** $(G, +, \cdot)$ con $+$ e \cdot binarie e associative, G con elemento neutro per $+$ e ogni elemento ha un inverso per $+$
- **Campo:** $(G, +, \cdot)$ con $+$ e \cdot binarie e associative, G con elemento neutro per $+$ e ogni elemento ha un inverso per $+$

Per "astratta", dal latino, "tirata fuori", si intende estrapolata dal suo contesto originale. La combinatoria quindi, vuole studiare le strutture algebriche e darne una rappresentazione più concreta.

Definition 1.2.2:

Sia G un gruppo, K un campo e V uno spazio vettoriale su K . si definisce una rappresentazione di G su V è un omomorfismo $\rho : G \rightarrow GL(V)$ tale che $\rho(g)\rho(h) = \rho(gh)$ per ogni $g, h \in G$.

Note:

In altre parole è un'azione (omomorfismo è un $G \rightarrow$) di G su V con immagine $GL(V)$ tramite isomorfismi

Definition 1.2.3

Diciamo che la rappresentazione è fedele se ρ è iniettivo, ovvero se $\rho(g) = \rho(h) \implies g = h$

Definition 1.2.4

Sia (V, ρ) una rappresentazione di G su V , diciamo che un sottospazio vettoriale $U \subseteq V$ è una sottorappresentazione di ρ se $\rho(g)U \subseteq U$ per ogni $g \in G$

Note:

In altre parole $(U, \rho|_U)$ è una rappresentazione di G su U , dove $\rho|_U : G \rightarrow GL(U)$ è l'omomorfismo che mappa $g \rightarrow \rho(g)|_U$

Example 1.2.2

$$G = \langle r | r^4 = i \rangle$$

Può essere rappresentato tramite rotazione di $V = \mathbb{R}^2$. Ovvero $\rho(r) = \begin{pmatrix} \cos(\frac{\pi}{2}) & -\sin(\frac{\pi}{2}) \\ \sin(\frac{\pi}{2}) & \cos(\frac{\pi}{2}) \end{pmatrix}$ ha sottorappresentazioni proprie?

Definition 1.2.5: R

Una rappresentazione è riducibile se ammette una sottorappresentazione propria (ovvero $U \neq \{0\}$ e $U \neq V$)

Example 1.2.3

Sia G il gruppo simmetrico $G = S_3$, $V = K^3$ rappresentazione matriciale. $\sigma \in S_3, (x_1, x_2, x_3) \in K^3$

$$\rho(\sigma)(x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$$

Ad esempio

$$\rho((123))(7, -4, 5/2) = (-4, 5/2, 7)$$

Example 1.2.4 (Esercizio)

Consideriamo i sottospazi $U = \{(t, t, t), t \in K\}$ e $W = \{(x_1, x_2, x_3), \in V | x_1 + x_2 + x_3 = 0\}$, mostrare che U e W sono sottorappresentazioni riducibili di ρ

Sol: $V = U \oplus W$



Definition 1.2.6

Una rappresentazione si dice indecomponibile se, ogni volta che $V = U \oplus W$ allora U e W sono sottorappresentazioni, abbiamo $U = V$ e $W = \{0\}$ o viceversa

Proposition 1.2.1

Chiaramente irriducibile \implies indecomponibile

Note:

vale il viceversa? in generale n perché potrebbe esserci un completamento

Example 1.2.5

$V = C^2 (Z, +)$

$$\rho(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

è un omomorfismo perché

$$\rho(n)\rho(m) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} = \rho(n+m)$$

Note:

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Lemma 1.2.1

Sia G un gruppo finito. E sia V una sottorappresentazione (su C) allora ogni sottorappresentazione $U \subseteq V$ ammette un complementare $W \subseteq V$ tale che $V = U \oplus W$ e W è una sottorappresentazione. Quindi indecomponibile \implies irriducibile

Dimostrazione: Data una sottorappresentazione $U \subseteq V$ consideriamo $U^\perp = \{v \in V | \langle v, u \rangle = 0 \forall u \in U\}$, dove $\langle \cdot, \cdot \rangle$ è un prodotto scalare hermitiano su V (quello G invariante), chiaramente $V = U \oplus U^\perp$ e U^\perp è una sottorappresentazione perché $\forall v \in U^\perp, \forall g \in G, \forall u \in U$ abbiamo $\langle \rho(g)v, u \rangle = \langle v, \rho(g^{-1})u \rangle = 0$ perché $u \in U$ e $\rho(g^{-1})u \in U$



Definition 1.2.7

A anello con 1_A , $(V, +)$ gruppo abeliano, è un A -modulo sinistro se $A \times V \rightarrow V$ tale che :

- $(a + b)v = av + bv$
- $a(v + w) = av + aw$
- $a(bv) = (ab)v$
- $1_A v = v$

Definition 1.2.8: $K[G]$

Combinazioni lineari formali di elementi di G con coefficienti in $K = \{\sum_{g \in G} a_g e_g \mid a_g \in K, \text{supp}(a_g) < \infty\}$
con prodotto a_g, e_g