Algebra Lineare ed Elementi di Geometria
– Corso di Laurea in Matematica Applicata –
MODULO 1

Prof. Lidia Angeleri

Anno accademico 2015-2016[1]

[1]appunti aggiornati in data 14 gennaio 2016

Indice

Parte I

GRUPPI

1 Il concetto di gruppo

1.1 Gruppo

Un[1] *gruppo* $(G, +)$ è costituito da un insieme non vuoto G e un'operazione $+ : G \times G \to G$, $(a, b) \mapsto a + b$ su G che gode delle seguenti proprietà:
(G1) associatività: $a + (b + c) = (a + b) + c$ per $a, b, c \in G$;
(G2) elemento neutro: $a + 0_G = 0_G + a = a$ per ogni $a \in G$;
(G3) elemento inverso: per ogni $a \in G$ esiste $b \in G$ tale che $a + b = b + a = 0_G$;
Il gruppo $(G, +)$ si dice *abeliano*[2] se vale anche la proprietá:
(G4) commutativa: $a + b = b + a$ per $a, b \in G$.

OSSERVAZIONI
(1) 0_G è univocamente determinato e per ogni $a \in G$ l'elemento inverso è univocamente determinato e si indica con $-a$.
(2) In un gruppo si ha la proprietà cancellativa:
se $a + x = a + y$ allora $x = y$ per $a, x, y \in G$.
(3) Si usa spesso la notazione moltiplicativa $(G, \cdot)$. In tal caso l'elemento neutro si indica con e oppure con 1_G e l'elemento inverso di a si indica con a^{-1}.

1.2 Esempi

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ sono gruppi abeliani.

1.3 Esempio: Classi di resto modulo n

(1) $n = 2$: $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ dove $\overline{0}$ è l'insieme dei numeri pari e $\overline{1}$ è l'insieme dei numeri dispari.

Tavola dell'addizione: $\begin{array}{c|cc} + & \overline{0} & \overline{1} \\ \hline \overline{0} & \overline{0} & \overline{1} \\ \overline{1} & \overline{1} & \overline{0} \end{array}$ Con questa operazione $\mathbb{Z}/2\mathbb{Z}$ diventa un gruppo abeliano.

(2) Più in generale, per un numero naturale $n \geq 2$ e $a, b \in \mathbb{Z}$ di forma

$$a = q_1 n + r_1$$

$$b = q_2 n + r_2$$

si ha

$$a + b = (q_1 + q_2)n + (r_1 + r_2).$$

[1] Questo primo capitolo è più dettagliato visto che alcune lezioni sono concomitanti con il test dei saperi minimi. Tuttavia queste note **non** sono le dispense del corso, ma vogliono soltanto fornire un "filo rosso" attraverso le prime lezioni. Sicuramente il materiale qui raccolto non è sufficiente per preparare l'esame.

[2] Niels Abel, matematico norvegese (1802-1829)

In altre parole, in $\mathbb{Z}/n\mathbb{Z}$, se le classi di resto

$$\overline{a} = \overline{r_1} \text{ e } \overline{b} = \overline{r_2}$$

allora

$$\overline{a+b} = \overline{r_1 + r_2}.$$

Possiamo quindi definire un'addizione sulle classi di resto come segue

$$\overline{a} + \overline{b} + \overline{a+b}.$$

$(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo abeliano rispetto a questa operazione con elemento neutro

$$\overline{0} = \{nz \mid z \in \mathbb{Z}\} = n\mathbb{Z}.$$

(3) $n = 12$ ...

(4) $n = 7$ ...

(5) $n = 5$ ...

1.4 Esempio: il gruppo simmetrico

Sia A un insieme non vuoto e sia $S(A)$ l'insieme di tutte le funzioni biiettive $f : A \to A$. La composizione di applicazioni definisce un'operazione $\circ : S(A) \times S(A) \to S(A)$, $(f, g) \mapsto g \circ f$. Con questa operazione $(S(A), \circ)$ diventa un gruppo con elemento neutro

$$\mathrm{id}_A : A \to A,\ a \mapsto a.$$

Infatti una funzione $f : A \to A$ è biiettiva se e solo se è invertibile, ovvero esiste una funzione $f^{-1} : A \to A$ tale che

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_A.$$

Vedremo in 3.3 che in generale $(S(A), \circ)$ non è abeliano.

2 Gruppi ciclici

2.1 Sottogruppo

Sia $(G, +)$ un gruppo. Un sottoinsieme non vuoto $H \subset G$ si dice *sottogruppo* di G se H è un gruppo rispetto all'operazione $+$ di G. In tal caso si scrive $H \leq G$.

OSSERVAZIONE

Un sottoinsieme $H \subset G$ è un sottogruppo se e solo se $H \neq \emptyset$ e per tutti gli $a, b \in H$ si ha $a - b \in H$.

2.2 Esempi

(1) Ogni gruppo $(G, \cdot)$ possiede i sottogruppi banali $\{e\}$ e G.

(2) L'insieme dei numeri pari forma un sottogruppo di $(\mathbb{Z}, +)$. L'insieme dei numeri dispari *non* forma un sottogruppo di $(\mathbb{Z}, +)$ perché non è chiuso rispetto all'operazione $+$.

(3) I sottogruppi di $(\mathbb{Z}, +)$ sono precisamente i sottoinsiemi di forma $n\mathbb{Z}$ con $n \in \mathbb{N}_0$.
Infatti se $H \leq (\mathbb{Z}, +)$, allora si hanno due casi:

caso 1: $H = \{0\}$ allora $H = 0\mathbb{Z}$
caso 2: esiste un elemento $0 \neq a \in H$. Se $a < 0$ consideriamo $-a \in H$. Quindi H contiene un elemento $n > 0$. Sia n il minimo intero positivo contenuto in H. Sicuramente $n\mathbb{Z} \subset H$. Sia adesso $a \in H$. Allora esistono $q, r \in \mathbb{Z}$ tali che $a = qn + r$ con $0 \leq r \leq n-1$. Per la scelta di n segue che il resto della divisione $r = \underbrace{a}_{\in H} - \underbrace{qn}_{\in H} \in H$ dev'essere nullo, quindi $a = qn \in n\mathbb{Z}$.

2.3 Il sottogruppo generato da un elemento.

Sia $(G, \cdot)$ un gruppo con elemento neutro e. Per $a \in G$ e un intero $n \in \mathbb{Z}$ si pone

$$a^n = \begin{cases} \underbrace{a \cdot a \cdot \ldots \cdot a}_{n} & \text{se } n > 0 \\ e & \text{se } n = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{n} & \text{se } n < 0 \end{cases}$$

L'insieme $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ è un sottogruppo di G, detto il *sottogruppo generato da a*.

2.4 Esempio

I sottogruppi generati da un elemento in $(\mathbb{Z}/6\mathbb{Z}, +)$....

2.5 L'ordine di un elemento

Sia $(G, \cdot)$ un gruppo e sia $a \in G$. L'*ordine dell'elemento* a è definito come $ord(a) = \mid \langle a \rangle \mid$.
(1) Se $a^l \neq a^k$ per $l \neq k$ allora $ord(a) = \infty$.
(2) Se esistono $l \neq k$ tali che $a^l = a^k$ allora $ord(a) = m < \infty$, dove m è il minimo intero positivo tale che $a^m = e$.

Infatti ....

2.6 Gruppo ciclico

Un gruppo $(G, \cdot)$ è detto *ciclico* se esiste un elemento $a \in G$ tale che $G = \langle a \rangle$.
In particolare, un gruppo ciclico è sempre abeliano.

2.7 Omomorfismo, isomorfismo

Siano $(G, \cdot)$ e $(G', *)$ due gruppi. Un'applicazione $f : G \to G'$ si dice:
- *omomorfismo* se $f(a \cdot b) = f(a) * f(b)$ per $a, b \in G$;
- *isomorfismo* se f è un omomorfismo biiettivo.
Se esiste un isomorfismo $f : G \to G'$ si dice che G e G' sono *isomorfi* e si scrive $G \cong G'$.

2.8 Classificazione dei gruppi ciclici

Sia $(G, \cdot)$ un gruppo ciclico.
(1) Se $\mid G \mid = \infty$, allora $(G, \cdot) \cong (\mathbb{Z}, +)$.
(2) Se $\mid G \mid = m$ allora $(G, \cdot) \cong (\mathbb{Z}/m\mathbb{Z}, +)$.

<u>*DIMOSTRAZIONE*</u> :

Sia $G = \langle a \rangle$ con $a \in G$.
Allora nel caso (1) $f : \mathbb{Z} \to G$, $n \mapsto a^n$ è isomorfismo. Infatti $f(n+m) = a^{n+m} = a^n a^m = f(n)f(m)$.
Nel caso (2) analogamente $f : \mathbb{Z}/m\mathbb{Z} \to G$, $\overline{n} \mapsto a^n$ è un isomorfismo. $\square$

Vedremo in 3.3 che già per ordine 4 esistono gruppi non ciclici, e per ordine 6 esistono gruppi non abeliani.

3 Il gruppo simmetrico

3.1 Permutazioni

Consideriamo il gruppo simmetrico di un insieme finito A. Possiamo assumere $A = \{1, 2, \ldots, n\}$. Il gruppo $S_n = S(A)$ è detto gruppo simmetrico su n oggetti e i suoi elementi si chiamano *permutazioni*. Abbiamo

$$| S_n |= n!$$

3.2 Notazione per le permutazioni

(1) Per indicare un elemento $\sigma \in S_n$ useremo la notazione

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

Ad esempio per $n = 3$ l'applicazione $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ con $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$ si indica con

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

mentre

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

indica l'applicazione $\tau : \{1, 2, 3\} \to \{1, 2, 3\}$ con $\tau(1) = 2, \tau(2) = 1, \tau(3) = 3$.

(2) Una permutazione $\pi \in S_n$ è detta *ciclo di lunghezza* k se permuta ciclicamente k elementi di $\{1, 2, \ldots, n\}$ e lascia fissi i restanti $n - k$ elementi, ovvero esistono $k \geq 2$ elementi distinti $m_1, \ldots, m_k \in \{1, \ldots, n\}$ tali che

$$\sigma(m_1) = m_2$$

$$\sigma(m_2) = m_3$$

$$\vdots$$

$$\sigma(m_{k-1} = m_k$$

$$\sigma(m_k) = m_1$$

e $\sigma(m) = m$ per tutti gli altri elementi $m \in \{1, \ldots, n\} \setminus \{m_1, \ldots, m_k\}$. In tal caso possiamo anche scrivere

$$\pi = (m_1, \ldots, m_k)$$

tralasciando dunque gli $n - k$ elementi fissati da π.

Ad esempio $\tau = (12) \in S_3$ è un ciclo di lunghezza 2, detto anche *trasposizione* o *scambio*, e $\sigma = (123)$ è un ciclo di lunghezza 3.
Ogni ciclo di lunghezza k è un elemento di S_n di ordine k.

(3) Due cicli σ_1, σ_2 si dicono *disgiunti* se operano su sottoinsiemi disgiunti di $\{1, \dots, n\}$. In tal caso

$$\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1.$$

Ad esempio in S_5 i cicli (12) e (345) sono disgiunti, mentre non lo sono (12) e (13).

3.3 Esempi

(1) S_3 è un gruppo di 6 elementi non abeliano, quindi in particolare non isomorfo a $\mathbb{Z}/6\mathbb{Z}$.
Si ha

$$S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}.$$

La tavola della moltiplicazione....

(2) L'insieme

$$\mathcal{V} = \{\mathrm{id},\ (12)(34),\ (13)(24),\ (14)(23)\} \subset S_4$$

è un sottogruppo di S_4, detto *gruppo di Klein*[3], che è abeliano ma non ciclico, quindi in particolare non isomorfo a $\mathbb{Z}/4\mathbb{Z}$. Si dimostra che, a meno di isomorfismo, esistono solo due gruppi di quattro elementi: $\mathbb{Z}/4\mathbb{Z}$ e $\mathcal{V}$.

3.4 Il segno di una permutazione

Data una permutazione $\sigma \in S_n$, una coppia di numeri (i, j) con $1 \leq i < j \leq n$ è detta *inversione per σ* se $\sigma(i) > \sigma(j)$. Se r è il numero delle inversioni per σ, chiamiamo *segno* di σ il numero

$$\varepsilon(\sigma) = (-1)^r = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Diremo che σ è *pari* se $\varepsilon(\sigma) = +1$, ovvero il numero delle inversioni è pari, altrimenti σ è detta *dispari*.
<u>DIMOSTRAZIONE:</u> ....

<u>ESEMPI</u>: La trasposizione $\tau = (13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$ ha le coppie $(1,2), (2,3), (1,3)$ come inversioni ed è pertanto dispari.
In generale una trasposizione $(i, j) \in S_n$ con $i < j$ ha la coppia (i, j) e tutte le coppie (i, k) e (k, j) con $i < k < j$ come inversioni ed è quindi sempre dispari.
Il ciclo $(123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$ ha le coppie $(2,3)$ e $(1,3)$ come inversioni ed è pari.

3.5 Esempio

In S_8 si ha $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 8 & 7 & 5 & 6 & 2 \end{pmatrix} = (13)(248)(576) = (13)(24)(48)(57)(76).$

[3]Felix Klein, matematico tedesco (1849-1925)

3.6 Scomposizione di permutazioni

(1) Ogni permutazione è prodotto di cicli disgiunti (e tale scomposizione è unica a meno dell'ordine).
(2) Ogni permutazione è prodotto di trasposizioni.

OSSERVAZIONI:
(1) Una permutazione è pari (rispettivamente, dispari) se e solo se può essere espressa come prodotto di un numero pari (rispettivamente, dispari) di trasposizioni.

(2) La scomposizione

$$\sigma = \tau_1 \circ \ldots \circ \tau_r$$

in prodotto di trasposizioni non è unica, peró il numero delle trasposizioni in qualsiasi scomposizione è unico a meno di congruenza modulo 2. Più precisamente: se abbiamo anche $\sigma = \rho_1 \circ \ldots \circ \rho_s$, allora $\overline{r} = \overline{s} \in \mathbb{Z}/2\mathbb{Z}$, ovvero r, s sono entrambi pari o entrambi dispari.

(3) L'insieme delle permutazioni pari si indica con A_n. Si ha

$$\mid A_n \mid = \frac{n!}{2}$$

Parte II

<u>CAMPI</u>

4 Il concetto di campo

4.1 Definizione

Un campo $(K, +, \cdot)$ è costituito da un insieme non vuoto K con due operazioni $+, \cdot : K \times K \to K$ che godono delle proprietà **(K1)** $(K, +)$ è un gruppo abeliano con elemento neutro 0_K;
(K2) $(R, \cdot)$ è un gruppo abeliano con elemento neutro 1_K;
(K3) Legge distributiva: $a(b + c) = ab + ac$ per $a, b, c \in K$.

4.2 Osservazioni

(1) $a \cdot 0_K = 0_K$ per $a \in K$.
Infatti $a \cdot 0_K + a \cdot a = a \cdot (0_K + a) = a \cdot a$ quindi $a \cdot 0_K = 0_K$.
(2) $(-a) \cdot b = a \cdot (-b) = -a \cdot b$ per $a, b \in R$.
(3) 0_K e 1_K sono univocamente determinati e $1_K \neq 0_K$.
(4) K non ha divisori di zero: se $a, b \in K \setminus \{0_K\}$, allora $ab \neq 0_K$.

4.3 Esempi

(1) $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ sono campi.
(2) $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$

con l'addizione di classi di resto e la moltiplicazione data dalla tavola $\begin{array}{c|cc} \cdot & \overline{0} & \overline{1} \\ \hline \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} \end{array}$ è un campo.

(3) Più in generale, per un numero naturale $n \geq 2$ e $a, b \in \mathbb{Z}$ di forma

$$a = q_1 n + r_1$$

$$b = q_2 n + r_2$$

si ha

$$ab = qn + (r_1 \cdot r_2)$$

per un $q \in \mathbb{Z}$. Possiamo quindi definire una moltiplicazione sulle classi di resto come segue

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Si dimostra che $\mathbb{Z}/n\mathbb{Z}$ diventa un campo rispetto a queste operazioni se e solo se n è un numero primo.

5 Diario delle lezioni successive

§5. Il campo dei numeri complessi

5.1 Il campo $\mathbb{C}$

5.2 Numeri immaginari

5.3 Forma algebrica di un numero complesso

5.4 Coniugato e modulo

5.5 Esempio

5.6 Coordinate polari

5.7 Forma trigonometrica di un numero complesso

5.8 Prodotto di numeri complessi in forma trigonometrica

5.9 La Formula di De Moivre

5.10 Definizione: radici n-esime

5.11 Teorema sulle radici n-esime

5.12 Esempio: Divisione del cerchio

5.13 Esempio

5.14 Teorema Fondamentale dell'Algebra

(*vedi anche* [GS, Appendice A] oppure [AF, Cap. 4.6 e 4.7])

III. Matrici

§6. Matrici e loro operazioni

6.1 Esempio

6.2 Definizioni

6.3 Esempi

6.4 Somma di due matrici

6.5 Moltiplicazione di una matrice per uno scalare

6.6 Prodotto di due matrici

6.7 Altri esempi

(*vedi* [GS, Capitolo I])

§7. Sistemi lineari e matrici

7.1 Esempi

7.2 Sistemi lineari in forma matriciale

7.3 Operazioni elementari

7.4 Metodo di eliminazione di Gauss (EG)

7.5 Risoluzione di un sistema lineare

7.6 Esempio

7.7 Rango di una matrice

7.8 Matrici elementari

(*vedi* [GS, Capitolo I])

§8. Matrici invertibili

8.1 Lemma e Definizione

8.2 Esempi

8.3 Proposizione (sistemi lineari equivalenti)

8.4 Proposizione

8.5 Proposizione

8.6 Teorema (esistenza dell'inversa destra)

8.7 Definizione di H-trasposta

8.8 Teorema (esistenza dell'inversa sinistra)

8.9 Corollario (matrici invertibili)

8.10 Calcolo della matrice inversa. Esempio

(*vedi* [GS, Capitolo I])

IV. Spazi vettoriali

§9. Spazi vettoriali e basi

9.1 Spazio vettoriale

9.2 Esempi

9.3 Proposizione

9.4 Combinazioni lineari

9.5 Esempi

9.6 Insieme di generatori, base

9.7 Esempi

9.8 Spazi vettoriali finitamente generati

9.9 Esempi

§10. Dipendenza e indipendenza lineare

10.1 Definizione di indipendenza lineare

10.2 Osservazione: base = insieme di generatori linearmente indipendente

10.3 Esempi

10.4 Caratterizzazione di dipendenza lineare

10.5 Esempi

10.6 Proposizione

10.7 Caratterizzazioni di una base

(*vedi* [GS, Capitolo II])

§11. Dimensione di uno spazio vettoriale

11.1 Esistenza della base.

11.2 Teorema di Steinitz

11.3 Corollario

11.4 Dimensione.

11.5 Esempi

11.6 Teorema: completamento della base

11.7 Proprietá di uno spazio vettoriale di dimensione n

11.8 Esempi

(*vedi* [GS, Capitolo II])

§12. Sottospazi di uno spazio vettoriale

12.1 Definizione di sottospazio

12.2 Esempi

12.3 Un sottospazio di V coincide con V se e solo se ha la stessa dimensione.

12.4 L'intersezione di due sottospazi

12.5 Esempio (unione di sottospazi)

12.6 La somma di due sottospazi

12.7 Formula di Grassmann

12.8 Somma diretta di due sottospazi

12.9 Esempi e Osservazioni

(*vedi* [GS, Capitolo II])

§13. Applicazioni lineari

13.1 Definizione

13.2 Esempi

13.3 Alcune proprietà

13.4 Lemma

13.5 Teorema: Ogni spazio vettoriale su K di dimensione n è isomorfo a K^n.

13.6 Definizione: l'applicazione delle coordinate

13.7 Esempi

13.8 Corollario: due spazi vettoriali sono isomorfi se e solo se hanno la stessa dimensione.

13.9 nucleo e immagine

13.10 Esempi

13.11 Teorema (nullità + rango)

13.12 Corollario

13.13 L'applicazione $f_A : \mathbb{K}^n \to \mathbb{K}^m$, $x \mapsto Ax$ associata a $A \in M_{m\times n}(\mathbb{K})$

(*vedi* [GS, Capitolo II])

§14. Quattro spazi associati a una matrice

14.1 Lemma

14.2 Teorema sul rango

14.3 Corollario: nullità + rango

14.4 Osservazione su A^H

14.5 Teorema dei quattro sottospazi: $\mathbb{K}^m = C(A) \oplus N(A^H)$ e $\mathbb{K}^n = C(A^H) \oplus N(A)$

14.6 Esempio

14.7 Procedimento per determinare basi di $C(A)$ e $N(A)$

14.8 Teorema di Rouché - Capelli

14.9 Teorema: le soluzioni di Ax=b sono i vettori di forma $p + u$ con $u \in N(A)$

14.10 Esempio

14.11 Procedimento per la risoluzione di un sistema lineare

(*vedi* [GS, Capitolo II])

6 Bibliografia

[A] M. Abate, Algebra lineare, McGraw-Hill 2000.

[AF] M. Abate, de Fabritiis, Geometria analitica con elementi di algebra lineare, McGraw-Hill 2010.

[CB] M.Candilera, A.Bertapelle: Algebra lineare e primi elementi di Geometria, McGraw Hill, ISBN: 9788838661891.

[GS] E. Gregorio, L. Salce: Algebra lineare. Libreria Progetto, 2005.

Precorso on-line: sito web `http://precorso.dicom.uninsubria.it/`

Video - precorso di iversity sito web `https://iversity.org/en/courses/precorso-di-calcolo`