Campi e sistemi lineari - Sommario

Sommario temporaneo da ristrutturare; sommario creato ad-hoc per inserire gli appunti presi dal 17.10.2023 al 18.10.2023 (IDEA: Mantenere questo sommario però di partizionare la parte sui sistemi lineari, una sulle definizioni e sugli esempi e l'altra sui teoremi vari.)

Campi

Definizione di un campo; le proprietà caratterizzanti dei campi; esempi di campi e non-campi.

---

0. Preambolo

Questo capitolo ci serve per riflettere sui *fondamenti* che abbiamo usato finora, in particolare quando abbiamo parlato di equazioni, sistemi lineari, matrici, spazi vettoriali, come quando parliamo delle matrici a *coefficienti reali*; oppure dei $\mathbb{R}$-*spazi vettoriali*. Tutte le proprietà di cui abbiamo visto valgono in quanto $\mathbb{R}$ è un *campo* con le sue operazioni $+, \cdot$.
Infatti avevamo implicitamente fatto una *meta-operazione* in cui usavamo le proprietà di questo campo. Ora definiamo rigorosamente un *campo*.

1. Definizione

DEF 1. Sia K un *insieme* (Teoria degli Insiemi) si cui sono definite delle operazioni (o funzioni) (Funzioni) di *somma* e *moltiplicazione*, ovvero:

$$\begin{aligned} + :\ & K \times K \longrightarrow K \\ & (a,b) \mapsto a+b \\ \cdot :\ & K \times K \longrightarrow K \\ & (a,b) \mapsto a \cdot b \end{aligned}$$

tali per cui vengono soddisfatte le seguenti proprietà K:

$$\begin{aligned}
&\mathrm{K}_1 : \forall a, b \in K; a+b=b+a \mid a \cdot b = b \cdot a \\
&\mathrm{K}_2 : \forall a, b, c \in K; a+(b+c)=(a+b)+c \mid a \cdot (b \cdot c) = (a \cdot b) \cdot c \\
&\mathrm{K}_3 : \exists 0 \in K : \forall a \in K, a+0=0+a=a \\
&\mathrm{K}_{3.1} : \exists 1 \in K : \forall a \in K, a \cdot 1 = 1 \cdot a = a \\
&\mathrm{K}_4 : \forall a \in K, \exists (-a) \in K : a+(-a)=-a+a=0 \\
&\mathrm{K}_{4.1} : \forall a \in K \diagdown, \{0\} \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1 \\
&\mathrm{K}_5 : \forall a, b, c \in K, (a+b) \cdot c = a \cdot c + b \cdot c
\end{aligned}$$

Queste regole si chiamo rispettivamente nei seguenti modi:
K1: Commutatività rispetto alla somma e prodotto
K2: Associatività rispetto alla somma prodotto
K3: Esistenza degli elementi neutri $0, 1$ dove $0 \neq 1$
K4: Esistenza degli opposti (somma) e inversi (prodotto)
K5: Distributività
Allora un tale insieme si dice **campo**.

1.1. Esempi

ESEMPIO 1.1.a. Gli insiemi $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono dei *campi infiniti*, invece $\mathbb{N}, \mathbb{Z}$ *non* sono *campi*.
OSS 1.1.a. Osserviamo che possono esistere anche dei *campi finiti*, che hanno una rilevanza fondamentale nella *crittografia*. L'esempio **1.1.c.** sarà l'esempio di un *campo finito*.

ESEMPIO 1.1.b. L'insieme delle *funzioni razionali* ovvero

$$\{\frac{p}{q} : p, q \text{ sono polinomi in una variabile}\}$$

può essere dotata di *somma* e *prodotto* in modo tale da rendere questa un *campo*.

ESEMPIO 1.1.c. Sia

$$\mathbb{Z}_2 := \{0, 1\}$$

su cui definiamo una operazione di *somma* e *prodotto* $(+, \cdot)$.
Definiamo queste mediante delle *tabelle di somma* e di *moltiplicazione*.

$+$	**0**	**1**
0	0	1
1	1	0

$\cdot$	**0**	**1**
0	0	0
1	0	1

Allora concludo che

$$(\mathbb{Z}_2, +, \cdot)$$

è un *campo finito*.

2. Conclusione

Pertanto la precedente nozione di $\mathbb{R}$-*spazio vettoriale* sarà da ora in poi sostituita da quella di K-spazio vettoriale, con K un campo. Analogo il discorso per le *matrici a coefficienti in* K, ovvero $M_{m,n}(K)$.

Sistemi Lineari

Definizione rigorosa di sistema lineare. Nesso tra sistemi lineari, matrici e campi. Teoremi sui sistemi lineari.

---

0. Preambolo

Avevamo accennato che cosa sono i *sistemi lineari* nel capitolo sulle Equazioni e Proprietà Lineari; però avendo definito i Campi, ora è opportuno definirli in una maniera rigorosa e formale.

1. Definizione formale

DEF 1. Sia K un *campo* (Campi, **DEF 1.**); definiamo un **sistema di m equazioni in n incognite a coefficienti in K** come un *sistema di equazioni* nella forma seguente:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases}$$

dove $a_{ij} \in K$, $\forall i \in \{1, \ldots, m\}$ e $\forall j \in \{1, \ldots, n\}$; inoltre $\forall b_i \in K, \forall i \in \{1, \ldots, m\}$.
SUBDEF 1.a. Gli elementi $x_1, x_2, \ldots, x_n$ sono dette **incognite**.
SUBDEF 1.b. Gli elementi $b_1, b_2, \ldots, b_m$ sono detti **termini noti**.
SUBDEF 1.c. Gli elementi a_{ij} sono detti **coefficienti** del *sistema lineare*.

DEF 1.1. La **soluzione** di un *sistema lineare* è una n*-upla ordinata* di elementi di K, che rappresentiamo come un *vettore-colonna*, $S \in K^n$, ovvero

$$S = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix}$$

ove $s_i \in K$, tali per cui se ad ogni s_i sostituiamo x_i (dove $i \in \{1, 2, \ldots, n\}$), allora tutte le *uguaglianze* del *sistema lineare* diventano *vere*.

DEF 1.2. Un *sistema lineare* si dice **omogeneo** se tutti i *termini noti* sono nulli: ovvero se $b_1, b_2, \ldots, b_m = 0, 0, \ldots, 0$.
Analogamente, un *sistema lineare* si dice **non omogeneo** se questo sistema non è omogeneo. (Lo so, informazione sorprendentemente non ovvia)

DEF 1.3. Un *sistema lineare* si dice **compatibile** se ammette almeno una *soluzione* S; altrimenti si dice **incompatibile**.

OSS 1.1. Se un *sistema lineare* è *omogenea*, allora essa dev'essere anche *compatibile*. Infatti la n-upla nulla è *sempre* soluzione di un sistema *omogeneo*.

DEF 1.4. Dato un *sistema lineare* come in **DEF 1.**, definiamo la la matrice A dei *coefficienti*

$$A = (a_{ij})_{\substack{i \in \{1, \ldots, m\} \\ j \in \{1, \ldots, n\}}}; A \in M_{m,n}(K)$$

e X la n-upla delle incognite, b la n-upla dei termini noti, ovvero $X, b \in M_{m,1}(K)$ dove

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}; b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

allora posso scrivere il *sistema lineare* in **forma compatta** come

$$A \cdot X = b$$

DEF 1.5. Dato due *sistemi lineari*, queste si dicono **equivalenti** se ammettono le *medesime soluzioni*; ovvero se i loro insiemi delle soluzioni sono uguali.
OSS 1.2. Questa nozione è molto utile per risolvere dei sistemi lineari, quindi uno degli obbiettivi principali di questo corso sarà di trovare le operazioni che trasformano dei sistemi lineari in un altro mantenendoli *equivalenti*.

2. Esempi

Tentiamo di applicare queste nozioni mediante degli esempi.

ESEMPIO 2.1. Consideriamo il seguente sistema.

$$\begin{cases} x_1 + 2x_2 = 3 \\ x_1 + 2x_2 = 5 \end{cases}$$

che in *forma compatta* si scrive

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

1. Questo è un sistema *non omogeneo*, in quanto *almeno uno* termine noto è *non-nullo*.
2. Si può immediatamente stabilire che questo sistema è *incompatibile*; infatti se si suppone che esiste una soluzione $S = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$ allora varrebbe che $s_1 + 2s_2 = 3 = 5$, il che è un assurdo.

ESEMPIO 2.2. Consideriamo il seguente sistema.

$$\begin{cases} x_1 + 2x_2 = 3 \\ x_1 - x_2 = 1 \end{cases}$$

1. Chiaramente questo sistema è *non-omogeneo*
2. Qui non è possibile stabilire a priori se questo sistema sia *compatibile* o meno. Allora mediante delle trasformazioni tentiamo di trovare una soluzione. Quindi

$$\begin{cases} x_1 + 2x_2 = 3 \sim x_1 = 3 - 2x_2 \\ x_1 - x_2 = 1 \end{cases} \implies \begin{cases} x_1 = 3 - 2x_2 \\ 3 - 2x_2 - x_2 = 1 \sim x_2 = \frac{2}{3} \end{cases}$$

allora

$$x_1 = 3 - 2x_2 \implies x_1 = 3 - 2\frac{2}{3} = \frac{5}{3}$$

quindi il *sistema* ha un'unica *soluzione*

$$S = \begin{pmatrix} \frac{5}{3} \\ \frac{2}{3} \end{pmatrix}$$

Perciò abbiamo stabilito che il sistema è anche *compatibile*.
OSS 2.1. Qui diciamo che la *soluzione* non solo esiste, ma è addirittura *unica*

in quanto per ottenere il *sistema finale* abbiamo trasformato il *sistema iniziale* tramite delle operazioni che mantengono i due sistemi *equivalenti*.

ESEMPIO 2.3. Consideriamo il sistema lineare

$$\begin{cases} x_1 + 2x_2 = 3 \\ 2x_1 + 4x_2 = 6 \end{cases}$$

e tentiamo di trovare una soluzione. Iniziamo dunque effettuando delle manipolazioni;

$$\begin{cases} x_1 + 2x_2 = 3 \text{ (a)} \\ 2x_1 + 4x_2 = 6 \implies 2(x_1 + 2x_2) = 2(3) \overset{(a)}{\implies} 2(3) = 2(3) \end{cases}$$

vediamo che la seconda equazione è *sempre vera*; allora ciò significa che anche l'equazione

$$x_1 + 2x_2 = 3 \iff x_1 = 3 - 2x_2$$

è sempre vera.
Perciò posso trovare una soluzione fissando un valore di x_2 preciso per poter determinare x_1; quindi generalizzando fisso $x_2 = t \in \mathbb{R}$ ed esprimo le soluzioni così:

$$x_1 = 3 - 2t$$

Ovvero le soluzioni sono della forma

$$S = \{t \in \mathbb{R} : \begin{pmatrix} 3 - 2t \\ t \end{pmatrix}\}$$

da cui discende che abbiamo *infinite* soluzioni.
OSS 2.2. Possiamo riscrivere l'insieme delle soluzioni come

$$S = \{t \in \mathbb{R} : \begin{pmatrix} 3 \\ 0 \end{pmatrix} + t \begin{pmatrix} -2 \\ 1 \end{pmatrix}\}$$

che *geometricamente* corrisponde ai *punti* di una *retta* passante per $(3, 0)$ e $(1, 1)$.

3. Teoremi sui sistemi lineari