

# Campi e sistemi lineari - Sommario

*Sommario sui campi e sui sistemi lineari.*

---

## A. Campi

---

### 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  $K$ :

$$K_1 : \forall a, b \in K; a + b = b + a \mid a \cdot b = b \cdot a$$

$$K_2 : \forall a, b, c \in K; a + (b + c) = (a + b) + c \mid a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

$$K_3 : \exists 0 \in K : \forall a \in K, a + 0 = 0 + a = a$$

$$K_{3.1} : \exists 1 \in K : \forall a \in K, a \cdot 1 = 1 \cdot a = a$$

$$K_4 : \forall a \in K, \exists (-a) \in K : a + (-a) = -a + a = 0$$

$$K_{4.1} : \forall a \in K \setminus \{0\} \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1$$

$$K_5 : \forall a, b, c \in K, (a + b) \cdot c = a \cdot c + b \cdot c$$

Queste regole si chiamano 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

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

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 |

| · | 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. Analogamente il discorso per le *matrici a coefficienti in*  $K$ , ovvero  $M_{m,n}(K)$ .

## B. Sistemi lineari

### 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. Inoltre rendiamo nota la seguente notazione:

**NOTAZIONE 0.** Andiamo a identificare i due seguenti spazi vettoriali:

la matrice colonna  $M_{m,1}(K)$  di tipo

$$\begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_m \end{pmatrix}$$

e la  $m$ -tupla  $K^m$  di tipo

$$\begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_m \end{pmatrix}$$

e questi due spazi vettoriali sono *isomorfi* (ovvero che presentano gli stessi comportamenti).

## 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:

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

dove  $a_{ij} \in K$ ,  $\forall i \in \{1, \dots, m\}$  e  $\forall j \in \{1, \dots, n\}$ ; inoltre  $\forall b_i \in K, \forall i \in \{1, \dots, m\}$ .

### 1.a. Incognite

**SUBDEF 1.a.** Gli elementi  $x_1, x_2, \dots, x_n$  sono dette **incognite**.

### 1.b. Termini noti

**SUBDEF 1.b.** Gli elementi  $b_1, b_2, \dots, b_m$  sono detti **termini noti**.

## 1.c. Coefficienti

**SUBDEF 1.c.** Gli elementi  $a_{ij}$  sono detti **coefficienti** del *sistema lineare*.

### 1.1. Soluzione di un sistema

**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  $i \in \{1, 2, \dots, n\}$ ), allora tutte le *uguaglianze* del *sistema lineare* diventano *vere*.

### 1.2. Omogeneità di un sistema

**DEF 1.2.** Un *sistema lineare* si dice **omogeneo** se tutti i *termini noti* sono nulli: ovvero se  $b_1, b_2, \dots, b_m = 0, 0, \dots, 0$ .

Analogamente, un *sistema lineare* si dice **non omogeneo** se questo sistema non è omogeneo. (Lo so, informazione sorprendentemente non ovvia)

### 1.3. Compatibilità di un sistema

**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*.

### 1.4. Forma compatta di un sistema

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

$$A = (a_{ij}); \begin{matrix} i \in \{1, \dots, m\} \\ j \in \{1, \dots, n\} \end{matrix}; A \in M_{m,n}(K)$$

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

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

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;

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

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

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

da cui discende che abbiamo *infinite* soluzioni.

**OSS 2.2.** Possiamo riscrivere l'insieme delle soluzioni come

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

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

---

## Teoremi sui Sistemi Lineari

*Teoremi sui sistemi lineari; teorema di Cramer; teoremi di strutture per i sistemi lineari; da continuare*

---

### 1. Teoremi sui sistemi lineari

Presentiamo dei teoremi importanti sui [Sistemi Lineari](#).

#### 1.1. Teorema di Cramer

**TEOREMA 1.1.** (*di Cramer*) Considero un sistema lineare con  $n$  equazioni ed  $n$  incognite, di forma



$$A \cdot X = b$$

Ovvero  $A \in M_n(K)$ .

Ora supponiamo che  $A$  sia anche *invertibile* (*Matrice*, **DEF 2.6.**); allora da qui discende che esiste un'*unica soluzione*  $S$  del sistema lineare ed essa è data da

$$S = A^{-1} \cdot b$$

**OSS 1.1.1.** Questo teorema è molto importante in quanto ci dà due dati importanti:

1. Da un lato ci dice quando un *sistema lineare* è *compatibile*, quindi c'è questa componente "*esistenziale*" di questo teorema.
2. Dall'altro lato ci fornisce una formula per *calcolare* la soluzione. L'unico problema di questo teorema è che **per ora** non abbiamo gli strumenti per *invertire una matrice* o *determinare se una matrice sia invertibile o meno*.

**DIMOSTRAZIONE 1.1.** La dimostrazione si struttura in due parti:

1. Una parte in cui devo dimostrare che la soluzione effettivamente *esiste* ed equivale a  $A^{-1} \cdot b$
2. Un'altra parte in cui devo dimostrare che essa è effettivamente l'*unica* soluzione
3. Supponendo che  $A^{-1} \cdot b$  sia *soluzione*, allora per tale definizione devo essere in grado di sostituirla ad  $X$  per poter ottenere un'uguaglianza vera; quindi faccio

$$A \cdot X = b$$

$$A \cdot (A^{-1} \cdot b) = b$$

$$(A \cdot A^{-1}) \cdot b = b$$

$$\mathbb{1}_n \cdot b = b \iff b = b$$

e l'ultima uguaglianza è vera.

4. Ora supponiamo per assurdo che esiste un'altra soluzione  $S'$  sia un'altra soluzione; allora per definizione questa verifica

$$\begin{aligned}
A \cdot S' &= b \\
A^{-1} \cdot (A \cdot S') &= A^{-1} \cdot b (!) \\
(A^{-1} \cdot A) \cdot S' &= A^{-1} \cdot b \\
S' &= A^{-1} \cdot b
\end{aligned}$$

che è esattamente uguale alla soluzione proposta dal teorema di *Cramer*; quindi esiste solo la soluzione  $S = A^{-1} \cdot b$ .

**OSS 1.1.2.** Focalizziamoci sulla parte contrassegnata con (!); notiamo che abbiamo moltiplicato da ambo le parti per  $A^{-1}$  a *SINISTRA*, e non a *DESTRA*; infatti nel contesto delle *matrici* la moltiplicazione a *sinistra* può comportarsi diversamente da quella a *destra*; infatti se avessimo moltiplicato a *destra*, tutta l'espressione avrebbe perso senso in quanto avremmo ottenuto  $b \cdot A^{-1}$  in quanto moltiplichiamo una matrice  $n \times 1$  per  $n \times n$ , che non è definita.

## 1.2. Teorema di struttura per i sistemi lineari omogenei

**TEOREMA 1.2.** (*di struttura per le soluzioni dei sistemi lineari omogenei*)

Considero un *sistema lineare omogeneo* di  $m$  equazioni in  $n$  incognite. Ovvero

$$A \cdot X = 0$$

dove  $A = M_{m,n}(K)$  e  $X = K^n$ ,  $0$  è la *matrice nulla* (*Matrice*, **DEF. 2.2.**).

Poi siano  $s, s' \in K^n$  due soluzioni distinte e sia  $\lambda \in K$ , allora:

1.  $s + s'$  è soluzione
2.  $\lambda \cdot s$  è soluzione

Pertanto ricordandoci che il vettore (o la matrice) nullo/a è *sempre* soluzione di un sistema *omogeneo*, ottengo che l'*insieme delle soluzioni* di questo sistema è l'insieme

$$S = \{r \in K^n : A \cdot r = 0\}$$

allora si verifica che  $S$  è un *sottospazio vettoriale* (*Sottospazi Vettoriali*, **DEF 1.**) di  $K^n$ .

**OSS 1.2.1.** Notiamo che in questo teorema ci interessa *il sistema lineare* sé stesso, invece nel **TEOREMA 1.1.** (di Cramer) ci interessava solo la *matrice* dei coefficienti  $A$

## DIMOSTRAZIONE 1.2.

Dimostriamo la prima parte del teorema

1. Dato che  $s$  e  $s'$  sono soluzioni, allora devono valere che:

$$\begin{cases} A \cdot s = 0 \\ A \cdot s' = 0 \end{cases}$$

E supponendo che  $s + s'$  sia soluzione, deve valere anche che:

$$A \cdot (s + s') = 0$$

e sviluppandolo, otterremo

$$\begin{aligned} A \cdot (s + s') &= 0 \\ A \cdot s + A \cdot s' &= 0 \\ 0 + 0 &= 0 \iff 0 = 0 \end{aligned}$$

che è vera.

Prima di dimostrare la seconda parte del teorema ci occorre fare un'osservazione:

**OSS 1.2.2.** Dati un  $A \in M_{m,n}(K)$  e un  $s \in K^n$  e un  $\lambda \in K$  allora abbiamo

$$A \cdot (\lambda \cdot s) = \lambda \cdot (A \cdot s)$$

Ora siamo pronti per concludere la dimostrazione.

2. Se  $s$  è soluzione, allora è vera che

$$A \cdot s = 0$$

allora supponendo che  $\lambda s$  sia soluzione abbiamo

$$A \cdot (\lambda \cdot s) = 0$$

e sviluppandola otterremo

$$\begin{aligned} A \cdot (\lambda \cdot s) &= 0 \\ \lambda \cdot (A \cdot s) &= 0 \\ \lambda \cdot 0 &= 0 \iff 0 = 0 \end{aligned}$$

il che è vera. ■

### 1.3. Osservazione

**OSS 1.3.** Osserviamo che possiamo "*combinare*" questi due teoremi e verificare un fenomeno:

Sia  $A \in M_n(K)$  e supponiamo che questa matrice sia anche *invertibile*; ora consideriamo il sistema lineare *omogeneo*

$$A \cdot X = 0$$

Allora da qui discende che 0 è *l'unica* soluzione di questo sistema (per il **TEOREMA 1.1.** (di Cramer)).

Infatti  $\lambda \cdot 0 = 0$  e  $0 + 0 = 0$  sono anche *soluzioni* in quanto sono uguali all'*unica soluzione* 0.

### 1.4. Teorema di struttura per i sistemi lineari

**TEOREMA 1.4.** (*di struttura per le soluzioni dei sistemi lineari*)

Considero un *sistema lineare*

$$A \cdot X = b$$

con  $A \in M_{m,n}(K)$  e  $b \in K^n$ . Sia  $\tilde{s}$  una soluzione; allora un elemento  $s \in K^n$  è soluzione di questo sistema lineare se e solo se possiamo scrivere

$$s = \tilde{s} + s_0$$

dove  $s_0$  è una soluzione del *sistema lineare omogeneo*

$$A \cdot X = 0$$

In altre parole l'insieme delle soluzioni di  $A \cdot X = b$  è

$$S = \{s \in K^n : s = \tilde{s} + s_0 \text{ per un qualche } s_0 \text{ sia soluzione}\}$$

**DEF 1.4.1.** Il *sistema lineare omogeneo*  $A \cdot X = 0$  si dice il **sistema lineare omogeneo associato** al sistema  $A \cdot X = b$ .

**DIMOSTRAZIONE 1.4.** Per pianificare la struttura di questo teorema, facciamo due considerazioni sulla *logica formale*, in particolare sulla *doppia implicazione* (*Connettivi*).

Questo teorema, da un punto di vista logico, vuole dire che

$$s \text{ è soluzione} \iff s = \tilde{s} + s_0$$

allora vogliamo dimostrare che entrambe le *implicazioni* sono vere; ovvero nel senso che valgono

$$\begin{cases} s \text{ è soluzione} \implies s = \tilde{s} + s_0 \\ s = \tilde{s} + s_0 \implies s \text{ è soluzione} \end{cases}$$

... [ DA FARE IN CLASSE ]

## C. Sistemi lineari a scala

---

### Sistemi lineari a scala

*Definizione dei sistemi lineari a scala; elementi di pivot; compatibilità dei sistemi lineari gradinizati.*

---

## D. Algoritmo di Gauß

---

### Algoritmo di Gauß

*Definizioni preliminari per la descrizione dell'algoritmo di Gauß (Matrice completa e le operazioni elementari OE). Descrizione dell'algoritmo di Gauß per rendere un sistema lineare in un sistema lineare equivalente a scala come un programma.*

---