Capitolo 2

Campi

2.1 Introduzione

Studiamo ora i campi. Essi sono una generalizzazione dell'insieme $\mathbb{R}$ dei numeri reali con le operazioni di addizione e di moltiplicazione.
Nel secondo paragrafo ricordiamo le proprietà delle operazioni di addizione e di moltiplicazione tra numeri reali. Ricordiamo solamente quelle proprietà che sono state utilizzate nel corso di geometria per studiare i sistemi di equazioni lineari a coefficienti reali.
Nel terzo paragrafo diamo la definizione di campo e ne studiamo alcune proprietà.

Nel quarto paragrafo vediamo come tutta la teoria dei sistemi lineari si estenda ai sistemi di equazioni lineari i cui coefficienti, anziché appartenere a $\mathbb{R}$, appartengano a un campo qualsiasi.

2.2 Addizione e moltiplicazione sui reali

Riassumiamo le proprietà dei numeri reali da noi utilizzate nel corso di Geometria.
Dati due numeri reali a e b, noi sappiamo cosa sia la loro somma $a + b$ e il loro prodotto $a \cdot b$. Sono quindi definite in $\mathbb{R}$ due operazioni, l'addizione e la moltiplicazione, che associano ad ogni coppia di numeri reali a e b i numeri reali $a + b$ e $a \cdot b$ rispettivamente.
Le operazioni di addizione e moltiplicazione verificano le seguenti proprietà:

1. **Proprietà associativa dell'addizione:**

$$(a + b) + c = a + (b + c) \text{ per ogni } a, b \text{ e } c \text{ in } \mathbb{R}.$$

2. **Proprietà commutativa dell'addizione:**

$$a + b = b + a \text{ per ogni } a \text{ e } b \text{ in } \mathbb{R}.$$

3. **Esistenza dell'elemento neutro rispetto all'addizione:** esiste un elemento e tale che

$$a + e = a \text{ per ogni } a \text{ in } \mathbb{R}.$$

Ovviamente esiste un unico elemento che soddisfa questa proprietà: il numero 0.

4. **Esistenza dell'opposto:** per ogni elemento a di $\mathbb{R}$ esiste un elemento b in $\mathbb{R}$ tale che

$$a + b = 0.$$

Ovviamente per ogni numero a esiste un unico elemento b che soddisfa questa proprietà: il numero $-a$ detto **opposto** di a.

5. **Proprietà associativa della moltiplicazione:**

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ per ogni } a, b \text{ e } c \text{ in } \mathbb{R}.$$

6. **Proprietà commutativa della moltiplicazione**:

$$a \cdot b = b \cdot a \text{ per ogni } a \text{ e } b \text{ in } \mathbb{R}.$$

7. **Esistenza dell'elemento neutro rispetto alla moltiplicazione:** esiste un elemento e' tale che

$$a \cdot e' = a \text{ per ogni } a \text{ in } \mathbb{R}.$$

Ovviamente esiste un unico elemento che soddisfa questa proprietà: il numero 1.

8. **Esistenza dell'inverso:** per ogni elemento a di $\mathbb{R}^* := \mathbb{R} - \{0\}$ esiste un elemento b in $\mathbb{R}$ tale che

$$a \cdot b = 1.$$

Ovviamente per ogni numero non nullo a esiste un unico elemento b che soddisfa questa proprietà: il numero a^{-1} detto **inverso** di a.

9. **Proprietà distributiva:**

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ per ogni } a, b \text{ e } c \text{ in } \mathbb{R}.$$

Notiamo che nella proprietà 8 abbiamo posto la condizione $a \neq 0$ per l'esistenza dell'inverso di a: qualunque sia b si ha infatti $0 \cdot b = 0 \neq 1$, e, dunque, il numero 0 non ha inverso.

2.3 Definizione di campo

Vogliamo ora studiare insiemi dotati di due operazioni che verifichino le nove proprietà elencate nel paragrafo precedente.

Definizione 2.1 Un campo è un insieme (non vuoto) $\mathbb{K}$ dotato di due **operazioni** che indichiamo con $+$ e $\cdot$ e chiamiamo rispettivamente **addizione** e **moltiplicazione**. Sono cioè date due leggi che associano ad ogni coppia di elementi a e b di $\mathbb{K}$ due elementi di $\mathbb{K}$ che denotiamo con $a+b$ e $a \cdot b$. Non basta però che siano definite due operazioni per poter dire che K è un campo. Tali operazioni devono verificare le seguenti proprietà:

1. **Proprietà associativa dell'addizione:**

$$(a+b)+c = a+(b+c) \text{ per ogni } a, b \text{ e } c \text{ in } \mathbb{K}.$$

2. **Proprietà commutativa dell'addizione:**

$$a+b = b+a \text{ per ogni } a \text{ e } b \text{ in } \mathbb{K}.$$

3. **Esistenza dell'elemento neutro rispetto all'addizione:** esiste un elemento e tale che

$$a+e = a \text{ per ogni } a \text{ in } \mathbb{K}.$$

   Dimostreremo (vedi proposizione 2.2) che di tali elementi ne esiste uno solo. Chiamiamo questo elemento **zero** e lo indichiamo con il simbolo 0. Per questo motivo questà proprietà viene spesso chiamata **esistenza dello zero**.

4. **Esistenza dell'opposto:** per ogni elemento a di $\mathbb{K}$ esiste un elemento b in $\mathbb{K}$ tale che

$$a+b = 0.$$

   Dimostreremo (vedi proposizione 2.3) che per ogni elemento a di $\mathbb{K}$ esiste un unico elemento b che soddisfa questa proprietà: chiamiamo tale elemento **opposto** di a e lo indichiamo con il simbolo $-a$.

5. **Proprietà associativa della moltiplicazione:**

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ per ogni } a, b \text{ e } c \text{ in } \mathbb{K}.$$

6. **Proprietà commutativa della moltiplicazione**:

$$a \cdot b = b \cdot a \text{ per ogni } a \text{ e } b \text{ in } \mathbb{K}.$$

7. **Esistenza dell'elemento neutro rispetto alla moltiplicazione:** esiste un elemento e' tale che

$$a \cdot e' = a \text{ per ogni } a \text{ in } \mathbb{K}.$$

Dimostreremo (vedi proposizione 2.2) che di tali elementi ne esiste uno solo. Chiamiamo questo elemento **uno** o **unità** e lo indichiamo con il simbolo 1. Per questo motivo questà proprietà viene spesso chiamata **esistenza dell'unità**.

8. **Esistenza dell'inverso:** per ogni elemento a di $\mathbb{K}^* := \mathbb{K} - \{0\}$ esiste un elemento b in $\mathbb{K}$ tale che
$$a \cdot b = 1.$$
Dimostreremo (vedi proposizione 2.3) che per ogni elemento a di $\mathbb{K}^*$ esiste un unico elemento b che soddisfa questa proprietà: chiamiamo tale elemento **inverso** di a e lo indichiamo con il simbolo a^{-1}.

9. **Proprietà distributiva:**
$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ per ogni } a, b \text{ e } c \text{ in } \mathbb{K}. \qquad \triangle$$

Proposizione 2.2 *In un campo esiste un solo elemento neutro rispetto all'addizione e un solo elemento neutro rispetto alla moltiplicazione.*

DIMOSTRAZIONE Siano e e $\overline{e}$ due elementi neutri rispetto all'addizione. Pertanto, per ogni elemento A del campo $\mathbb{K}$ si ha:
i) $a + e = e + a = a$
ii) $a + \overline{e} = \overline{e} + a = a$.
Consideriamo ora $e + \overline{e}$.
Sfruttando la i) abbiamo $e + \overline{e} = \overline{e}$
Sfruttando la ii) abbiamo $e + \overline{e} = e$
Dalle due uguaglianze otteniamo $e = \overline{e}$.
In modo analogo si dimostra l'unicità dell'elemento neutro rispetto alla moltiplicazione. ■

Proposizione 2.3 *In un campo $\mathbb{K}$:*

1. *ogni elemento è dotato di uno ed un solo opposto*
2. *ogni elemento non nullo è dotato di uno e un solo inverso.*

DIMOSTRAZIONE 1. Fissato un elemento a del campo $\mathbb{K}$ siano b e b' due suoi elementi opposti. Si ha pertanto:
i) $a + b = b + a = 0$
ii) $a + b' = b' + a = 0$.
Consideriamo ora $b + a + b'$.
Abbiamo, applicando i):
$b + a + b' = (b + a) + b' = 0 + b' = b'$.
Abbiamo, applicando ii):
$b + a + b' = b + (a + b') = b + 0 = b$.
Dalle due uguaglianze segue $b = b'$.

2. L'unicità dell'inverso si dimostra in modo analogo. ■

Osservazione 2.4 Nello scrivere la proprietà associativa e la proprietà distributiva abbiamo utilizzato regole per la precedenza tra operazioni del tutto analoghe a quelle che siamo abituati a utilizzare per le operazioni tra reali. Per esempio quando scriviamo $a + (b + c)$ intendiamo dire che prima calcoliamo la somma $b + c$ e poi calcoliamo la somma tra a e $b + c$. Quando invece scriviamo $a \cdot b + a \cdot c$ intendiamo dire che prima calcoliamo i prodotti $a \cdot b$ e $a \cdot c$ e poi sommiamo i risultati così ottenuti. △

Osservazione 2.5 La proprietà associativa dell'addizione ci permette di dire che sommando a alla somma $b + c$ o sommando $a + b$ a c otteniamo lo stesso risultato. D'ora in poi possiamo quindi usare il simbolo $a + b + c$ senza problemi: la proprietà associativa ci garantisce che comunque operiamo il risultato è sempre lo stesso. Per la stessa ragione possiamo scrivere la somma di più di tre elementi senza far uso di parentesi (possiamo ad esempio scrivere $a+b+c+d$). Analogamente la proprietà associativa della moltiplicazione ci permette di scrivere il prodotto di tre o più elementi senza far uso di parentesi (possiamo ad esempio scrivere $a \cdot b \cdot c$ o $a \cdot b \cdot c \cdot d$). △

Nota 2.6 Nella definizione di campo abbiamo utilizzato la nomenclatura (addizione, moltiplicazione, etc.) e la simbologia (1, 0 , $-a$, a^{-1}, etc.) dei numeri reali. Questo utilizzo è fatto unicamente per ragioni di comodo e non significa che gli elementi di un qualsiasi campo siano necessariamente numeri. △

Esempi

1. L'insieme $\mathbb{R}$ dei numeri reali con le usuali operazioni di addizione e moltiplicazione è un campo.

2. L'insieme $\mathbb{Q}$ dei numeri razionali con le usuali operazioni di addizione e moltiplicazione è un campo.

3. L'insieme $\mathbb{C}$ dei numeri complessi con le usuali operazioni di addizione e moltiplicazione è un campo.

4. L'insieme $\mathbb{Z}$ dei numeri interi con le usuali operazioni di addizione e moltiplicazione non è un campo: infatti esso soddisfa tutte le proprietà tranne quella dell'esistenza dell'inverso.

5. L'insieme $M(\mathbb{R}, n, n)$ delle matrici quadrate reali di ordine n (con $n \geq 2$) con le usuali operazioni di addizione e moltiplicazione riga per colonna non è un campo: infatti esso soddisfa tutte le proprietà con l'eccezione della proprietà commutativa della moltiplicazione e dell'esistenza dell'inverso (esistono matrici non invertibili).

Esercizio di base EB.2.1 Consideriamo l'insieme K formato da due elementi che chiamiamo P e D. Introduciamo in esso due operazioni che indichiamo con i simboli $+$ e $\cdot$, ponendo:

$$P + P = D + D = P \ , \ D + P = P + D = D$$

e

$$P \cdot P = P \ , \ P \cdot D = P \ , \ D \cdot P = P \ , \ D \cdot D = D$$

Facciamo osservare che le due operazioni non sono introdotte a caso. Con P si intendono infatti i numeri pari e con D si intendono i numeri dispari. La formula $P + D = D$ significa che sommando un numero pari con un numero dispari si ottiene un numero dispari. Analogamente per le altre somme. Invece la formula $P \cdot D = P$ significa che il prodotto di un numero pari per un numero dispari è un numero pari. Analogamente per gli altri prodotti.

Dimostrare che l'insieme K con le operazioni di addizione e moltiplicazione appena introdotte è un campo. △

2.4 Proprietà dei campi

Definizione 2.7 In un campo $\mathbb{K}$ possiamo introdurre l'operazione di **sottrazione** nel modo seguente: dati a e b in $\mathbb{K}$ poniamo

$$a - b := a + (-b) \, .$$ △

Osservazione 2.8 Per definire questa operazione abbiamo dovuto utilizzare la proprietà dell'esistenza dell'opposto. Abbiamo inoltre utilizzato l'operazione di addizione. Notiamo che l'operazione di sottrazione non è, salvo che per alcuni campi molto particolari, né commutativa né associativa. △

Esercizio di base EB.2.2 Mostrare con opportuni esempi che l'operazione di sottrazione in $\mathbb{R}$ non è commutativa né associativa. △

Diamo ora altre proprietà di un campo $\mathbb{K}$ analoghe a proprietà dei numeri reali. Per ognuna di esse diamo la dimostrazione lasciando come esercizio al lettore il compito di individuare quali proprietà di un campo siano state utilizzate a ogni passaggio.

Proposizione 2.9 ***Proprietà di semplificazione rispetto all'addizione.*** *Siano a, b e c elementi di un campo $\mathbb{K}$. Allora*

$$a = b \text{ se e solo se } a + c = b + c.$$

DIMOSTRAZIONE Se $a = b$ ovviamente risulta $a + c = b + c$. Dimostriamo il viceversa: supponiamo che $a + c = b + c$. Allora $(a + c) + (-c) = (b + c) + (-c)$. Da questa segue che $a + (c + (-c)) = b + (c + (-c))$. Dunque $a + 0 = b + 0$ e pertanto $a = b$. ■

Osservazione 2.10 La proprietà di semplificazione rispetto all'addizione, applicata al caso particolare in cui $b = 0$ ci permette di affermare che, dati due elementi a e c di un campo $\mathbb{K}$, allora si ha $a + c = c$ se e solo se $a = 0$. △

Proposizione 2.11 *Per ogni elemento a in $\mathbb{K}$ si ha $a \cdot 0 = 0$.*

DIMOSTRAZIONE Poiché $0 = 0 + 0$, si ha $a \cdot 0 = a \cdot (0 + 0)$, da cui otteniamo $a \cdot 0 = a \cdot 0 + a \cdot 0$. La proprietà di semplificazione dell'addizione dà quindi $0 = a \cdot 0$. ■

Osservazione 2.12 Come conseguenza di questa proprietà si ha che, se $\mathbb{K}$ ha almeno due elementi, l'elemento neutro rispetto all'addizione e alla moltiplicazione non possono coincidere vale a dire $1 \neq 0$ (questo può sembrare banale ma si ricordi che 0 e 1 non sono, in generale, il numero 0 e il numero 1). Infatti, scegliamo un elemento a di $\mathbb{K}$ diverso da 0 (per assicurare l'esistenza di un tale elemento utilizziamo il fatto che in $\mathbb{K}$ ci siano almeno due elementi). Ora $a \cdot 1 = a$ e $a \cdot 0 = 0$: poiché $a \neq 0$ abbiamo quindi $a \cdot 1 \neq a \cdot 0$, mentre se fosse $1 = 0$ dovremmo allora avere $a \cdot 1 = a \cdot 0$.

Per evitarci complicazioni d'ora in poi supporremo sempre che un campo $\mathbb{K}$ abbia almeno due elementi (d'altra parte un campo con un solo elemento non è particolarmente interessante!) △

Osservazione 2.13 Nella proprietà 8 abbiamo richiesto l'esistenza dell'inverso solo per elementi diversi da 0: infatti non è possibile che lo 0 abbia inverso dal momento che $0 \cdot a = 0$ per ogni $a \in \mathbb{K}$. △

Per il prodotti che coinvolgono opposti di elementi del campo $\mathbb{K}$ valgono analoghe proprietà a quelle note per le operazioni tra reali. Più precisamente:

Proposizione 2.14 *Se a e b sono elementi di un campo $\mathbb{K}$ allora si ha*

$$(-a) \cdot b = a \cdot (-b) = -(a \cdot b), \qquad (-a) \cdot (-b) = a \cdot b.$$

La prima proprietà ci permette allora di scrivere senza ambiguità $-a \cdot b$, per indicare l'elemento $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

DIMOSTRAZIONE Lasciata per esercizio. ■

Esercizio di base EB.2.3 Dimostrare queste due proprietà. Suggerimento: sommare $(-a) \cdot b$ a $a \cdot b$ e utilizzare la proprietà distributiva. △

Proposizione 2.15 ***Proprietà di semplificazione rispetto alla moltiplicazione.*** *Siano a, b e c elementi di un campo $\mathbb{K}$, con $c \neq 0$. Allora*

$$a = b \text{ se e solo se } a \cdot c = b \cdot c.$$

DIMOSTRAZIONE Se $a = b$ ovviamente risulta $a \cdot c = b \cdot c$. Dimostriamo il viceversa: supponiamo che $a \cdot c = b \cdot c$. Allora $(a \cdot c) \cdot c^{-1} = (b \cdot c) \cdot c^{-1}$. Da questa segue che $a \cdot \left(c \cdot c^{-1}\right) = b \cdot \left(c \cdot c^{-1}\right)$. Dunque $a \cdot 1 = b \cdot 1$ e pertanto $a = b$. ■

Osservazione 2.16 Chiaramente questa proprietà è falsa se $c = 0$. Scelti infatti a e b diversi tra loro si ha $a \cdot 0 = b \cdot 0 = 0$. △

Osservazione 2.17 La proprietà di semplificazione rispetto alla moltiplicazione, applicata al caso particolare in cui $b = 1$ ci permette di affermare che, dati due elementi a e c di un campo $\mathbb{K}$, con $c \neq 0$, allora si ha $a \cdot c = c$ se e solo se $a = 1$. △

Un'altra importante conseguenza della proprietà di semplificazione rispetto al prodotto è la seguente:

Proposizione 2.18 ***Principio dell'annullamento del prodotto.*** *Se a e b sono due elementi di un campo $\mathbb{K}$ tali che $a \cdot b = 0$ allora almeno uno tra a e b è uguale a 0.*

DIMOSTRAZIONE Abbiamo che $a \cdot b = a \cdot 0$. Allora o $a = 0$, oppure si può semplificare l'uguaglianza precedente e ottenere $b = 0$. ■

Si hanno poi le seguenti proprietà la cui dimostrazione è lasciata per esercizio:

Proposizione 2.19

- *Siano a, b e c elementi di un campo $\mathbb{K}$: si ha che $a + b = c$ se e solo se $a = c - b$.*
- *Siano a, b e c elementi di un campo $\mathbb{K}$ con $b \neq 0$: si ha che $a \cdot b = c$ se e solo se $a = c \cdot b^{-1}$.*

Esercizio di base EB.2.4 Dimostrare queste due proprietà. △

Applicando queste due proprietà si dimostra facilmente la seguente:

Proposizione 2.20 *Siano a, b e c elementi di un campo $\mathbb{K}$ con $a \neq 0$. L'equazione nell'incognita x:*

$$a \cdot x + b = c$$

ha un'unica soluzione data da:

$$x = (c - b) \cdot a^{-1}.$$

La dimostrazione è lasciata per esercizio.

2.5 Sistemi lineari a coefficienti in un campo

Nel corso di geometria abbiamo studiato i sistemi di equazioni lineari: in particolare abbiamo stabilito quando un sistema è risolubile e abbiamo poi determinato degli algoritmi per la determinazione delle soluzioni. Per far ciò abbiamo introdotto il concetto di matrice a coefficienti reali e l'insieme delle matrici $M(\mathbb{R}, p, q)$ a coefficienti reali con p righe e q colonne. Abbiamo poi definito in $M(\mathbb{R}, p, q)$ un'operazione di addizione. Abbiamo cioè definito la funzione:

$$\begin{aligned} + : M(\mathbb{R}, p, q) \times M(\mathbb{R}, p, q) &\to M(\mathbb{R}, p, q) \\ (A, B) &\to A + B \end{aligned}$$

Abbiamo poi definito l'operazione di moltiplicazione di un numero reale per una matrice. Abbiamo cioè definito la funzione:

$$\begin{aligned} \cdot : \mathbb{R}, \times M(\mathbb{R}, p, q) &\to M(\mathbb{R}, p, q) \\ (k, A) &\to k \cdot A \end{aligned}$$

Ciò ci ha permesso di parlare di combinazioni lineari di matrici di $M(\mathbb{R}, p, q)$ con coefficienti reali, di matrici linearmente indipendenti e indipendenti in $\mathbb{R}$. Considerando poi le righe (o le colonne) di matrici come particolari matrici, abbiamo parlato di combinazioni lineari a coefficienti in $\mathbb{R}$ di righe o colonne di una matrice e di righe (o colonne) linearmente dipendenti e indipendenti in $\mathbb{R}$. Per ogni coppia di matrici $A \in M(\mathbb{R}, p, q)$ e $B \in M(\mathbb{R}, q, s)$ abbiamo definito la matrice prodotto righe per colonne $A \cdot B \in M(\mathbb{R}, p, s)$. Abbiamo cioè definito la funzione:

$$\begin{aligned} \cdot : M(\mathbb{R}, p, q) \times M(\mathbb{R}, q, s) &\to M(\mathbb{R}, p, s) \\ (A, B) &\to A \cdot B \end{aligned}$$

Ciò ci ha permesso di scrivere un sistema di equazioni lineari nella forma matriciale

$$AX = B.$$

A partire dalla definizione del prodotto abbiamo poi introdotto il concetto di matrice invertibile in $M(\mathbb{R}, n, n)$.

Per ogni matrice $A \in M(\mathbb{R}, n, n)$ abbiamo poi definito il suo determinante. Abbiamo cioè definito la funzione:

$$\begin{aligned} \det : M(\mathbb{R}, n, n) &\to \mathbb{R} \\ A &\to \det A \end{aligned}$$

Abbiamo visto che una matrice è invertibile se e solo se il suo determinante è non nullo.

Abbiamo poi introdotto il concetto di rango di una matrice $A \in M(\mathbb{R}, p, q)$. Abbiamo cioè definito la funzione:

$$\begin{aligned} \mathrm{rk} : M(\mathbb{R}, p, q) &\to \mathbb{N} \cup \{0\} \\ A &\to \mathrm{rk}\, A \end{aligned}$$

Tutto ciò ci ha permesso di dare alcuni algoritmi per la discussione e risoluzione di sistemi di equazioni lineari. Abbiamo introdotto l'algoritmo di Cramer per sistemi di n equazioni in n incognite aventi la matrice dei coefficienti invertibile. Abbiamo poi presentato gli algoritmi di Rouché-Capelli e di Gauss per sistemi in un numero di incognite ed equazioni qualunque (non necessariamente uguali fra loro). Sfruttando le operazioni elementari sulle righe abbiamo determinato un algoritmo per calcolare il rango di una matrice qualsiasi, il determinante di una matrice quadrata e l'inversa di una matrice quadrata invertibile.

In tutte le definizioni e dimostrazioni date (e anche in quelle non date in maniera esplicita) si sono utilizzate solo le proprietà di campo di $\mathbb{R}$.

Non abbiamo utilizzato altre proprietà tipiche dei numeri reali, quali, ad esempio, l'ordinamento dei numeri reali (dati a e b reali è verificata una e una sola delle relazioni $a = b$ o $a < b$ o $a > b$), né il fatto che dati a e b reali con $a < b$ allora esistono infiniti reali x tali che $a < x < b$, né tantomeno la possibilità di estrarre radici n-esime di numeri reali $x \geq 0$ (abbiamo considerato solo sistemi di primo grado). Pertanto, dato un qualsiasi campo $\mathbb{K}$ possiamo definire tutti concetti e dimostrare tutti i risultati dati in precedenza. Abbiamo pertanto:

Proposizione 2.21 *Tutte le definizioni e i teoremi visti nel corso del primo anno riguardanti le matrici a elementi reali, le loro operazioni e i sistemi di equazioni lineari a coefficienti reali rimangono valide quando al campo dei numeri reali si sostituisce un campo qualsiasi.*

2.6 Soluzioni degli esercizi di base

Soluzione dell'esercizio di base EB.2.1 Le proprietà associative e commutative dell'addizione e della moltiplicazione di K derivano dalle proprietà associative e commutative dell'addizione e della moltiplicazione tra numeri interi.
Si verifica facilmente che P è l'elemento neutro rispetto all'addizione e che l'elemento neutro rispetto alla moltiplicazione è l'elemento D.
L'opposto di P è P stesso. L'opposto di D è D stesso.
L'elemento neutro P rispetto all'addizione non ha inverso.
L'elemento D ha come inverso D stesso.
La proprietà distributiva di K deriva dalla proprietà distributiva tra numeri interi.
di Le proprietà commuti

Soluzione dell'esercizio di base EB.2.2 Per mostrare che la sottrazione in $\mathbb{R}$ non è commutativa dobbiamo trovare due numeri a e b tali che $a - b \neq b - a$. Si vede subito che $a - b = b - a$ se e solo se $a = b$. Se scegliamo allora a e b diversi tra loro, ad esempio $a = 0$ e $b = 1$ abbiamo che $a - b \neq b - a$.

Per mostrare invece che la sottrazione in $\mathbb{R}$ non è associativa dobbiamo trovare tre numeri a, b e c tali che $(a - b) - c \neq a - (b - c)$. Ora

$$(a - b) - c = a + (-b) + (-c)$$

e

$$a - (b - c) = a + (-b) + c.$$

Dunque $(a - b) - c = a - (b - c)$ se e solo se

$$a + (-b) + (-c) = a + (-b) + c.$$

Per la legge di cancellazione questo si verifica solo se $c = -c$, ovvero se $c = 0$. Basta allora scegliere a, b e c con $c \neq 0$, ad esempio $a = b = 0$ e $c = 1$ e vediamo che $(a - b) - c \neq a - (b - c)$.

Soluzione dell'esercizio di base EB.2.3 Osserviamo che

$$(-a) \cdot b + a \cdot b = ((-a) + a) \cdot b = 0 \cdot b = 0.$$

Dunque $(-a)\cdot b$ è l'opposto di $a\cdot b$, vale a dire $(-a)\cdot b = -(a\cdot b)$. Notiamo ora che $a\cdot(-b) = (-b)\cdot a$, e, dunque, per quanto abbiamo appena dimostrato si ha

$$(-b)\cdot a = -(b\cdot a) = -(a\cdot b)\,.$$

Infine

$$(-a)\cdot(-b) = -(a\cdot(-b)) = -(-(a\cdot b)) = a\cdot b.$$

Soluzione dell'esercizio di base EB.2.4 Se $a = c-b$ chiaramente risulta $a+b = c$. Se viceversa supponiamo che $a+b=c$ sommando $-b$ a entrambi i membri di questa uguaglianza otteniamo il risultato cercato.
Se $a = c\cdot b^{-1}$ chiaramente risulta $a\cdot b = c$. Se viceversa $a\cdot b = c$ moltiplicando per b^{-1} entrambi i membri di questa uguaglianza otteniamo il risultato cercato.

2.7 Sunto

2.7.1 Definizione di campo

Definizione Un campo è un insieme (non vuoto) $\mathbb{K}$ dotato di due **operazioni** che indichiamo con $+$ e $\cdot$ e chiamiamo rispettivamente **addizione** e **moltiplicazione**, e che soddisfano le proprietà date nel paragrafo 2.3.
L'elemento neutro rispetto alla somma viene indicato con il simbolo 0, l'elemento neutro rispetto al prodotto viene indicato con il simbolo 1. △

Nota Nella definizione di cambo abbiamo utilizzato la nomenclatura (addizione, moltiplicazione, etc.) e la simbologia (1, 0 , $-a$, a^{-1}, etc.) dei numeri reali. Questo utilizzo è fatto unicamente per ragioni di comodo e non significa che gli elementi di un qualsiasi campo siano necessariamente numeri. △

2.7.2 Proprietà dei campi

Proposizione *Se il campo $\mathbb{K}$ ha almeno due elementi allora l'elemento neutro rispetto alla somma e l'elemento neutro rispetto al prodotto sono diversi ($0\neq 1$).*

Definizione In un campo $\mathbb{K}$ possiamo introdurre l'operazione di **sottrazione** nel modo seguente: dati a e b in $\mathbb{K}$ poniamo

$$a-b := a+(-b)\,.$$ △

Proposizione ***Proprietà di semplificazione rispetto all'addizione.*** *Siano a, b e c elementi di un campo $\mathbb{K}$. Allora*

$$a = b \text{ se e solo se } a+c = b+c.$$

Proposizione *Per ogni elemento a in $\mathbb{K}$ si ha $a\cdot 0 = 0$.*
Proprietà. *Se a e b sono elementi di un campo $\mathbb{K}$ allora si ha*

$$(-a)\cdot b = a\cdot(-b) = -(a\cdot b)\,, \qquad (-a)\cdot(-b) = a\cdot b.$$

Proposizione ***Proprietà di semplificazione rispetto alla moltiplicazione.*** *Siano a, b e c elementi di un campo $\mathbb{K}$, con $c\neq 0$. Allora*

$$a = b \text{ se e solo se } a\cdot c = b\cdot c.$$

Proposizione ***Principio dell'annullamento del prodotto:*** *Se a e b sono due elementi di un campo $\mathbb{K}$ tali che $a \cdot b = 0$ allora almeno uno tra a e b è uguale a 0.*

Proposizione *Siano a, b e c elementi di un campo $\mathbb{K}$ con $a \neq 0$. L'equazione nell'incognita x:*

$$a \cdot x + b = c$$

ha un'unica soluzione data da:

$$x = (c - b) \cdot a^{-1}.$$

Esempio

1. l'insieme $\mathbb{R}$ dei numeri reali, l'insieme $\mathbb{Q}$ dei numeri razionali, l'insieme $\mathbb{C}$ dei numeri complessi.
2. L'insieme $\mathbb{Z}$ dei numeri interi non è un campo.
3. L'insieme $M(\mathbb{R}, n, n)$ delle matrici quadrate reali di ordine n (con $n \geq 2$) con le usuali operazioni di addizione e moltiplicazione riga per colonna non è un campo. △

2.7.3 Sistemi lineari a coefficienti in un campo

Proposizione *Tutte le definizioni e i teoremi visti nel corso del primo anno riguardanti le matrici a elementi reali, le loro operazioni e i sistemi di equazioni lineari a coefficienti reali rimangono valide quando al campo dei numeri reali si sostituisce un campo qualsiasi.*

2.8 Esercizi

Esercizio E.2.1 Verificare la verità o falsità delle seguenti affermazioni:

1. Le eventuali soluzioni di un sistema di equazioni lineari in cui tutti i coefficienti e i termini noti sono numeri interi sono tutte formate da numeri interi.
2. Le eventuali soluzioni di un sistema di equazioni lineari in cui tutti i coefficienti e i termini noti sono numeri razionali sono tutte formate da numeri razionali.
3. Le eventuali soluzioni di un sistema di equazioni lineari in cui tutti i coefficienti e i termini noti sono numeri reali positivi sono tutte formate da numeri reali positivi.
4. Le eventuali soluzioni di un sistema di equazioni lineari aventi tutti i coefficienti complessi sono tutte formate da numeri complessi.
5. Le eventuali soluzioni di un sistema di equazioni lineari aventi tutti i coefficienti complessi e non reali sono tutte formate da numeri complessi non reali.

2.9 Soluzioni degli esercizi

Soluzione dell'esercizio E.2.1

1. Affermazione falsa. Osserviamo che l'insieme $\mathbb{Z}$ dei numeri interi non è un campo. Non possiamo quindi applicare quel che abbiamo detto sui sistemi di equazioni lineari a coefficienti in un campo.

Ciò però non implica a priori che l'affermazione sia falsa. Per dire che l'affermazione è falsa abbiamo bisogno di un controesempio. Dobbiamo cioè esibire un sistema di equazioni lineari avente tutti i coefficienti interi che ha soluzioni non intere. Diamo un controesempio molto semplice.
Consideriamo il sistema formato da una sola equazione in un'incognita

$$2x = 1$$

Tutti i coefficienti sono numeri interi, eppure la sola soluzione del sistema, $x = \frac{1}{2}$ non è intera.

2. Affermazione vera. L'insieme $\mathbb{Q}$ dei numeri razionali è un campo. Le eventuali soluzioni sono quindi tutte formate da numeri razionali.
3. Affermazione falsa. L'insieme dei numeri reali positivi non è un campo (manca lo zero, manca l'opposto). Non possiamo quindi applicare la teoria dei sistemi di equazioni lineari a coefficienti in un campo.
Viene lasciata come esercizio la ricerca di un controesempio.
4. Affermazione vera. L'insieme $\mathbb{C}$ dei numeri complessi è un campo. Le eventuali soluzioni sono quindi tutte formate da numeri complessi.
5. Affermazione falsa. L'insieme dei numeri complessi che non sono numeri reali non è un campo (perché?). Non possiamo quindi applicare la teoria dei sistemi di equazioni lineari a coefficienti in un campo.
Viene lasciata come esercizio la ricerca di un controesempio.