WEB

2 Strutture algebriche

1 Leggi di composizione

L'operazione di addizione nell'insieme $\mathbb{N}$ dei naturali associa a ogni coppia $(m; n)$ di numeri naturali ancora un numero naturale s, risultato dell'operazione. L'addizione costituisce una *legge di composizione interna*, in quanto, operando su elementi di $\mathbb{N}$, dà come risultato ancora un elemento di $\mathbb{N}$.

DEFINIZIONE Indicato con $E \times E$ l'insieme delle coppie ordinate di elementi di E, una legge di composizione interna è un'applicazione (funzione) dell'insieme $E \times E$ (o di un suo sottoinsieme) in E:

$$E \times E \to E$$

Indicheremo la legge con uno dei seguenti simboli:

$$+ \qquad \cdot \qquad \times \qquad \square \qquad *$$

Quindi, se la legge associa alla coppia $(a; b)$ il numero c scriveremo, per esempio:

$$a \cdot b = c$$

oppure:

$$a + b = c$$

o semplicemente:

$$ab = c$$

L'insieme E, munito della legge di composizione interna indicata con il simbolo $\cdot$, verrà indicato con

$$(E; \cdot)$$

Esempi

1. La legge di addizione tra numeri naturali è una legge di composizione interna definita per ogni coppia $(m; n)$ di numeri naturali; non lo è invece la legge di sottrazione tra naturali, essendo definita solo per coppie $(m; n)$ con $m \geq n$.

2. L'addizione, la sottrazione e la moltiplicazione tra numeri reali sono leggi di composizione interna definite per ogni coppia di numeri reali.
La divisione tra reali è una legge di composizione interna definita solo per le coppie $(a; b)$ con $b \neq 0$.

3 L'elevamento a potenza nell'insieme dei numeri reali, cioè la legge che associa alla coppia ordinata $(a; b)$ il numero reale a^b, è definita solo se la base a è > 0.

Una legge di composizione interna definita sull'insieme E può godere di alcune proprietà.

1. Proprietà commutativa

La legge $+$ si dice **commutativa** se $\forall\, a, b \in \mathrm{E}$ risulta:

$$a + b = b + a$$

Esempi

4 Sono leggi commutative le seguenti:

a) l'addizione e la moltiplicazione tra numeri naturali (o interi o reali o complessi);
b) le operazioni di unione $\cup$ e intersezione $\cap$ definite nell'insieme $\mathcal{P}(\mathrm{E})$ dei sottoinsiemi di E;
c) la somma tra vettori dello spazio (vedi vol. 2, § 4.3);
d) la somma tra matrici $m \times n$ (vedi vol. 2, § 5.2).

5 Non sono commutative, invece, le seguenti leggi:

a) l'elevamento a potenza tra naturali (o reali o complessi), poiché in generale risulta:

$$a^b \neq b^a$$

b) il prodotto tra matrici quadrate d'ordine n (vedi vol. 2, § 5.2);
c) il prodotto vettoriale tra vettori (vedi vol. 2, § 4.6), poiché:

$$\vec{u} \wedge \vec{v} = -\vec{v} \wedge \vec{u}$$

2. Proprietà associativa

La legge $+$ si dice **associativa** se $\forall\, a, b, c \in \mathrm{E}$ risulta:

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

Esempi

6 Le leggi degli esempi 4*a*, 4*b*, 4*c*, 4*d* sono associative.

7 Il prodotto vettoriale tra vettori dello spazio è una legge associativa.

Un esempio di legge non associativa è l'elevamento a potenza tra numeri reali; infatti se a, b, c sono tre numeri reali, risulta:

$$(a^b)^c = a^{bc}$$

mentre:

$$a^{(b^c)} = a^{b^c} \qquad \text{e} \qquad a^{bc} \neq a^{b^c}$$

Esempi

8 Siano:

$$a = 2 \qquad b = -3 \qquad c = 4$$

Si ha:

$$(a^b)^c = (2^{-3})^4 = \left(\frac{1}{8}\right)^4 = \frac{1}{4096}$$

$$a^{b^c} = 2^{(-3)^4} = 2^{81}$$

3. Esistenza dell'elemento neutro

Se nell'insieme E in cui è definita la legge $+$ esiste un elemento, che indichiamo con e, tale che:

$$a + e = e + a = a \qquad \forall\, a \in \mathrm{E}$$

tale elemento si chiama **elemento neutro** per la legge +.

Esempi

9 Nell'insieme dei naturali $\mathbb{N}$, in quello degli interi $\mathbb{Z}$, dei reali $\mathbb{R}$, dei complessi $\mathbb{C}$ lo zero è l'elemento neutro rispetto all'addizione.

10 Negli insiemi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ l'elemento neutro rispetto alla moltiplicazione è 1.

11 Nell'insieme delle matrici $m \times n$ l'elemento neutro rispetto alla somma tra matrici è la matrice $m \times n$ avente tutti i termini uguali a zero.

12 Nell'insieme dei sottoinsiemi di E l'elemento neutro rispetto all'operazione di unione è l'insieme vuoto.

13 Nell'insieme V dei vettori dello spazio l'elemento neutro rispetto alla somma tra vettori è il vettore nullo.

Osservazione 1

Non è detto è che per ogni legge di composizione interna debba esistere l'elemento neutro; pensiamo, per esempio, alla legge di elevamento a potenza nell'insieme dei reali positivi: non esiste alcun numero reale e tale che $\forall\, a \in \mathbb{R}_0^+$ risulti:

$$e^a = a^e = a$$

Così, per l'operazione di prodotto vettoriale tra vettori dello spazio non esiste l'elemento neutro.

Si può dimostrare che:

TEOREMA 1 **L'elemento neutro, se esiste, è unico.**

DIMOSTRAZIONE

Supponiamo, per assurdo, che esistano due elementi neutri e_1 ed e_2, allora:

- considerando e_1 come elemento neutro, risulta:

$$e_2 \cdot e_1 = e_1 \cdot e_2 = e_2$$

- considerando e_2 come elemento neutro, risulta:

$$e_1 \cdot e_2 = e_2 \cdot e_1 = e_1$$

e quindi:

$$e_1 = e_2$$

4. Esistenza dell'elemento simmetrico (o inverso)

Se nell'insieme E, in cui è definita la legge di composizione interna $\cdot$, **esiste** l'elemento neutro e e per ogni $a \in$ E esiste un elemento $a^{-1} \in$ E tale che:

$$a \cdot a^{-1} = a^{-1} \cdot a = e$$

allora a^{-1} prende il nome di **simmetrico** o **inverso** di a.
Il simmetrico di a viene indicato con $-a$ se la legge viene indicata con il simbolo +.

Esempi

14 Rispetto all'operazione di addizione nell'insieme $\mathbb{N}$ dei naturali non esiste il simmetrico, mentre nell'insieme $\mathbb{Z}$ degli interi il simmetrico di a è il suo opposto $-a$.

15 Rispetto all'operazione di moltiplicazione negli insiemi $\mathbb{N}$ e $\mathbb{Z}$ non esiste il simmetrico, mentre nel l'insieme $\mathbb{R}$ dei numeri reali privato dello zero il simmetrico di a è il suo reciproco $a^{-1} = \frac{1}{a}$.

16 Nell'insieme $\mathbb{R}_0$, strutturato con l'operazione di divisione, non esiste l'unità né il simmetrico.

Sull'insieme E siano definite due leggi di composizione interna, che indicheremo con + e $\cdot$. Può valere la

5. Proprietà distributiva

Si dice che la legge $\cdot$ gode della proprietà **distributiva** rispetto alle legge + se $\forall\, a, b, c \in \mathrm{E}$ risulta:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Esempi

17 Negli insiemi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ il prodotto gode della proprietà distributiva rispetto alla somma.

18 Nell'insieme dei sottoinsiemi di E l'intersezione gode della proprietà distributiva rispetto all'unione.

Legge di composizione esterna

Siano, ora, dati due insiemi E e K.

DEFINIZIONE Si dice che in E è definita una legge di **composizione esterna** se a ogni coppia ordinata $(a; k)$, con $a \in \mathrm{E}$ e $k \in \mathrm{K}$, è associato uno ed un solo elemento di E.

Una legge di composizione esterna è, quindi, un'applicazione di $\mathrm{E} \times \mathrm{K}$ in E:

$$\mathrm{E} \times \mathrm{K} \to \mathrm{E} \mid (a; k) \to b \quad \text{con} \quad b \in \mathrm{E}$$

il risultato di tale operazione si indica con

$$b = k\, a$$

Gli elementi di K prendono il nome di **operatori** su E.

Esempi

19 Sia V l'insieme dei vettori del piano (vedi vol. 2, cap. 4); il prodotto di un vettore per un numero reale k è ancora un vettore $\vec{w} \in \mathrm{V}$; tale prodotto è pertanto una legge di composizione esterna in V con operatori in $\mathbb{R}$:

$$(\vec{v}; k) \to k\,\vec{v} = \vec{w}$$

20 Il prodotto di un polinomio per un numero reale è una legge di composizione esterna che dà come risultato ancora un polinomio.

21 Il prodotto di una matrice $m \times n$ per un numero reale è una legge di composizione esterna che dà come risultato ancora una matrice $m \times n$ (vedi vol. 2, § 5.2).

DEFINIZIONE Un insieme E su cui siano definite una o più leggi di composizione interne o esterne si dice dotato di una **struttura algebrica**.
Due insiemi E ed F sui quali siano definite leggi di composizione che godano di proprietà analoghe si dicono dotati della stessa struttura.

Nei paragrafi successivi presenteremo alcune strutture algebriche, quali quelle di *gruppo*, *anello*, *corpo*, *campo*, *spazio vettoriale*.

2 Gruppi

DEFINIZIONE Si dice **gruppo** un insieme non vuoto G in cui sia definita una legge di composizione interna +

$$(a; b) \to (a + b) \in G \qquad a \in G,\ b \in G$$

che goda delle seguenti proprietà:

1a. **associativa**:

$$(a + b) + c = a + (b + c) \qquad \forall\ a, b, c \in G$$

1b. esistenza dell'**elemento neutro** $e \in G$, tale che si abbia:

$$e + a = a + e = a \qquad \forall\ a \in G$$

1c. esistenza dell'**elemento inverso** o **simmetrico** di a, che indicheremo con $-a \in G$, tale che:

$$a + (-a) = (-a) + a = e \qquad \forall\ a \in G$$

Se a queste proprietà si aggiunge la

1d. **proprietà commutativa**:

$$a + b = b + a \qquad \forall\ a, b \in G$$

il gruppo si dice **commutativo** o **abeliano**.

Se G ha un numero finito di elementi, il loro numero si dice **ordine** del gruppo.

Esempi

22 L'insieme $\mathbb{Z}$ è un gruppo abeliano rispetto all'operazione di addizione. L'elemento neutro è lo zero e il simmetrico di a è il suo opposto $-a$.
Sono gruppi abeliani anche gli insiemi:

$$(\mathbb{Q}; +), \quad (\mathbb{R}; +), \quad (\mathbb{C}; +)$$

23 L'insieme $\mathbb{Z}$ strutturato con l'operazione di prodotto non è un gruppo, poiché non esistono i simmetrici degli elementi di $\mathbb{Z}$: il reciproco di un intero non è in generale un intero. La moltiplicazione tra interi gode, però, delle proprietà 1a e 1b.
Un insieme di questo tipo, strutturato con una legge di composizione interna per la quale valgano gli assiomi 1a e 1b, prende il nome di **monoide**.

24 L'insieme V dei vettori dello spazio è un gruppo abeliano rispetto alla somma tra vettori.
L'elemento neutro è il vettore nullo, il simmetrico di $\vec{v}$ è il vettore $-\vec{v}$.

25 Sia $\mathcal{P}[x]$ l'insieme dei polinomi di grado $\leq n$:

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

a coefficienti reali. Si definisce somma di due polinomi:

$$P_1(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \qquad P_2(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_0$$

il polinomio:

$$P_1(x) + P_2(x) = (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + \ldots + (a_0 + b_0)$$

L'operazione di somma così definita è una legge di composizione interna, poiché il polinomio $P_1(x) + P_2(x)$ è ancora di grado $\leq n$.
L'insieme $\mathcal{P}[x]$ è un **gruppo abeliano** rispetto all'operazione di somma. L'elemento neutro è il polinomio i cui coefficienti sono tutti nulli, l'opposto del polinomio $P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ è il polinomio $-P(x) = -a_n x^n - a_{n-1} x^{n-1} - \ldots - a_0$.
N.B. L'insieme dei polinomi di grado n non costituisce gruppo, poiché la somma di due polinomi di grado n può essere un polinomio di grado minore di n.

26 L'insieme delle matrici $m \times n$, strutturato con l'operazione di somma tra matrici è un gruppo abeliano. L'elemento neutro è la matrice i cui elementi sono tutti uguali a zero e la simmetrica della matrice A è la matrice $-A$ i cui elementi sono gli opposti dei corrispondenti elementi di A.

27 Gli insiemi $\mathbb{Q}_0$, $\mathbb{R}_0$, $\mathbb{C}_0$, cioè dei razionali, dei reali e dei complessi privati dello zero, sono gruppi abeliani rispetto all'operazione di prodotto. In ciascuno di questi insiemi l'unità è il numero 1 e il simmetrico di a è il suo reciproco $\frac{1}{a} = a^{-1}$.

28 Consideriamo l'insieme $A = \{a; b; c\}$ e la legge di composizione interna definita secondo la tabella a fianco, cioè, per esempio:

$$a + a = a \qquad a + c = a \qquad c + b = b \qquad \text{ecc.}$$

È facile verificare che la legge così definita è associativa ma non commutativa e che, inoltre, non esiste l'elemento neutro.
Un insieme come questo, dotato di una legge di composizione interna per la quale valga solo la legge associativa, prende il nome di **semigruppo**.

+	a	b	c
a	a	b	a
b	c	b	a
c	a	b	c

29 L'insieme R delle rotazioni del piano intorno a un punto fisso, in senso antiorario, dotato, come operazione, dell'ordinaria composizione, forma un gruppo ancora commutativo. Se α e β sono due rotazioni, definiamo loro prodotto la rotazione ottenuta eseguendo prima la α e successivamente la β.
Tale composizione è ovviamente associativa e commutativa: l'elemento neutro è la rotazione α di… zero gradi, e l'inversa di α è la rotazione $2\pi - \alpha$.

Osservazione 2

In un gruppo l'equazione

$$a \cdot x = b$$

nell'incognita x ha una ed una sola soluzione qualunque siano a e b. Tale soluzione è:

$$x = a^{-1} \cdot b$$

come si verifica sostituendo tale valore nell'equazione.
L'equazione

$$y \cdot a = b$$

ha anch'essa una ed una sola soluzione:

$$y = b \cdot a^{-1}$$

In assenza di commutatività le due equazioni sono differenti…
Una conseguenza importante dell'unicità della soluzione per l'equazione $a \cdot x = b$ è la seguente:

$$\text{se} \quad c \neq d \quad \text{allora} \quad a \cdot c \neq a \cdot d$$

3 Alcuni gruppi finiti

Cerchiamo di individuare i gruppi "più piccoli": quelli di ordine uno, due, tre o quattro.

Gruppi di ordine uno

Un gruppo formato da un solo elemento è necessariamente formato dal solo elemento neutro "e":

$$e \cdot e = e \qquad e^{-1} = e$$

Gruppi di ordine due

Per l'ordine due è facile riconoscere che, chiamati "1" e "–1" i due elementi, l'unica operazione da porre su di essi che rispetti i quattro assiomi di gruppo è… l'ordinaria moltiplicazione. La tabella moltiplicativa è quella a fianco.

•	1	–1
1	1	–1
–1	–1	1

Gruppi di ordine tre

Elenchiamo alcuni casi significativi.

Gruppo I_3 delle classi resto modulo tre

Le classi resto modulo 3 composte con l'ordinaria addizione (vedi Algebra 1, § 2.12) costituiscono un gruppo di ordine tre: la tabella di composizione è la tabella 1.
Si verifica facilmente, osservando la tabella, che ogni elemento ha il simmetrico, che in questo caso si chiama, usualmente, opposto: per esempio, l'opposto di [2] è [1], infatti:

$$[2] + [1] = [0]$$

L'insieme I_3 delle classi resto modulo 3 è formato dalle tre classi [0], [1], [2]; tutti gli interi appartengono rispettivamente alle classi [0], [1], [2] a seconda che il resto della loro divisione per 3 sia 0, 1, 2.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Tabella 1

Gruppo R_3 delle rotazioni di un triangolo equilatero

Consideriamo le rotazioni di un triangolo equilatero attorno all'asse passante per il centro e perpendicolare al piano del triangolo che portano il triangolo a sovrapporsi a se stesso.
Chiamiamo "0" la posizione iniziale del triangolo con i vertici numerati come in figura 1.
Una rotazione di 120° in senso antiorario porta il triangolo nella posizione "1" (fig. 2). Il vertice 1 va nella posizione precedentemente occupata dal vertice 2, il vertice 2 in quella del vertice 3 e il vertice 3 in quella del vertice 1.
Una successiva rotazione, ancora di 120° in senso antiorario, porta il triangolo nella posizione "2": il vertice 1 va nella posizione occupata all'inizio dal vertice 3, il vertice 2 sulla posizione inizialmente occupata dal vertice 1 e infine il vertice 3 sulla posizione inizialmente occupata dal vertice 2 (fig. 3).

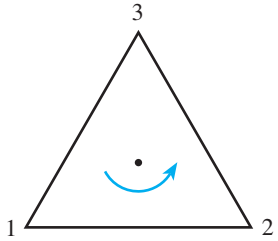

Figura 1

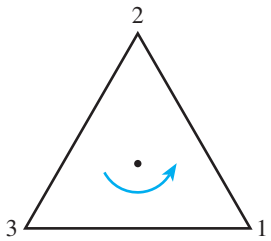

Figura 2

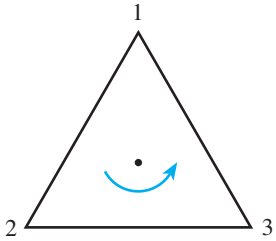

Figura 3

Una successiva rotazione, identica alle precedenti, riporta il triangolo nella posizione iniziale.
Indichiamo con [1] l'insieme delle rotazioni che portano dalla posizione "0" alla "1", cioè:

$$[1] = \{\text{rotazioni antiorarie di } 120° + k \cdot 360°,\ k \in \mathbb{N}\}$$

Indichiamo con [2] l'insieme delle rotazioni che portano dalla "0" alla "2", cioè:

$$[2] = \{\text{rotazioni antiorarie di } 240° + k \cdot 360°,\ k \in \mathbb{N}\}$$

Indichiamo con [0] l'insieme delle rotazioni che portano dalla "0" ancora alla "0", cioè:

$$[0] = \{\text{rotazioni antiorarie di } k \cdot 360°,\ k \in \mathbb{N}\}$$

L'insieme $R_3 = \{[0]; [1]; [2]\}$ delle rotazioni di un triangolo equilatero su se stesso forma gruppo qualora si definisca come prodotto tra due rotazioni la rotazione ottenuta applicandole successivamente.
L'elemento neutro è costituito dall'insieme [0].
La tabella di composizione è la tabella 2.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Tabella 2

Radici terze dell'unità

Le tre radici terze complesse dell'unità:

$$e = 1 \qquad a = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \qquad b = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

composte con l'ordinaria moltiplicazione tra numeri complessi, costituiscono un gruppo d'ordine tre.
Esse sono collocate sul piano complesso ai vertici del triangolo equilatero inscritto nella circonferenza di centro l'origine e raggio 1, con un vertice nel punto (1; 0).
Le tre radici forniscono un'immagine analitica del precedente gruppo R_3 delle rotazioni di un triangolo equilatero.

I punti che rappresentano le radici *n*-sime dell'unità sono i vertici di un poligono regolare di *n* lati, inscritto nella circonferenza di centro l'origine e raggio 1 con uno dei vertici in (1; 0) (vedi vol. 2, § 8.6).

Gruppo astratto di tre elementi

Indichiamo i tre elementi con:

"1", "*a*", "*b*"

dove abbiamo indicato con "1" naturalmente l'elemento neutro. La tabella di composizione è pertanto quella riportata a fianco.

•	1	*a*	*b*
1	1	*a*	*b*
a	*a*	?	?
b	*b*	?	?

In ogni riga e in ogni colonna devono comparire elementi diversi, quindi delle due possibilità:

$$a \cdot a = 1 \qquad \text{e} \qquad a \cdot a = b$$

solo la seconda è accettabile. Di conseguenza la tabella moltiplicativa è la tabella 3.
Facendo corrispondere nei gruppi osservati:

$$[0] \Leftrightarrow 1$$
$$[1] \Leftrightarrow a$$
$$[2] \Leftrightarrow b$$

•	1	*a*	*b*
1	1	*a*	*b*
a	*a*	*b*	1
b	*b*	1	*a*

Tabella 3

si riconosce che le tabelle di composizione 1, 2 e 3 diventano le stesse.

Gruppi in corrispondenza biunivoca tra loro e con tabelle di composizione corrispondenti, come nel caso osservato, si dicono **isomorfi**, cioè della stessa forma (vedi § 11).
Gruppi isomorfi sono di fatto "uno stesso gruppo": per studiare un gruppo non importa infatti il nome che si dà a ciascun elemento, ma il modo con cui gli elementi si compongono.
Il gruppo che abbiamo indicato con

$$\{1; a; b\}$$

sarebbe stato, forse, presentato agli studenti di Atene come il gruppo:

$$\{1; \alpha; \beta\}$$

senza tuttavia che il cambiamento alterasse in alcun modo la sostanza!
Concludiamo con il seguente teorema:

TEOREMA 2 **I gruppi di ordine tre sono tutti isomorfi, ovvero:**

"Esiste un solo gruppo di ordine tre"

Gruppi di ordine quattro

L'indagine sui gruppi di ordine 4 fornisce qualche sorpresa: scopriremo due gruppi diversi, in cui "diversi" significa avere tabelle moltiplicative differenti.

Gruppo R_4 delle rotazioni del quadrato

Le rotazioni di multipli di 90° intorno al centro offrono un insieme di 4 trasformazioni del quadrato in sé che, moltiplicate con l'ordinaria composizione, producono un gruppo appunto di ordine 4. Indicate con:

$$0°, \quad 90°, \quad 180° \quad \text{e} \quad 270°$$

esse si compongono secondo la tabella a fianco.
Il gruppo delle rotazioni di multipli di 90° è null'altro che un'immagine delle classi resto modulo 4 composte con l'ordinaria addizione.

•	0°	90°	180°	270°
0°	0°	90°	180°	270°
90°	90°	180°	270°	0°
180°	180°	270°	0°	90°
270°	270°	0°	90°	180°

Gruppo S_4 delle simmetrie

Esiste un altro insieme di quattro trasformazioni del quadrato in sé che offre ancora un gruppo d'ordine 4. Pensiamo al quadrato di vertici:

$$A = (-1; 1) \qquad B = (1; 1) \qquad C = (1; -1) \qquad D = (-1; -1)$$

Gli assi coordinati passano per il centro del quadrato.
Le simmetrie del piano rispetto agli assi cartesiani trasformano il quadrato in sé.
Indichiamo con X e Y le simmetrie rispetto all'asse x e rispetto all'asse y.
Indichiamo poi con XY la trasformazione ottenuta componendo le due simmetrie (l'ordine, come si può riconoscere, è irrilevante).
Detta U la trasformazione del quadrato in sé… lasciandolo fermo, è facile riconoscere che i quattro elementi

$$U \qquad X \qquad Y \qquad XY$$

moltiplicati mediante l'ordinaria composizione delle trasformazioni, formano un gruppo di ordine 4.
La tabella di S_4 fa riconoscere, tra l'altro, che ogni elemento coincide con il suo inverso, infatti:

$$X \cdot X = U \qquad Y \cdot Y = U \qquad XY \cdot XY = U$$

il che non accadeva nella tabella precedente di R_4.

•	U	X	Y	XY
U	U	X	Y	XY
X	X	U	XY	Y
Y	Y	XY	U	X
XY	XY	Y	X	U

Abbiamo quindi almeno due gruppi R_4 ed S_4 di ordine 4 diversi.
Chi volesse poi un gruppo con 123 elementi può pensare alle 123 radici 123-esime complesse dell'unità! O, anche, alle rotazioni del piano intorno all'origine di angoli multipli di $\left(\frac{360}{123}\right)^\circ$.

4 Il gruppo delle affinità

Verifichiamo ora che: **le affinità di $\mathbb{R}^2$ in $\mathbb{R}^2$** (vedi vol. 2, § 6.2)

$$T\colon (x; y) \to (ax + by + h;\ cx + dy + k) \qquad (ad - bc \neq 0)$$

formano gruppo rispetto all'operazione di composizione.
Infatti:

- componendo due affinità T e T' di matrici associate rispettive A e A', la trasformazione composta:

$$T * T'$$

è un'affinità che ha per matrice associata la matrice prodotto:

$$A * A'$$

Un'**affinità** è una corrispondenza biunivoca tra due piani o tra punti di uno stesso piano che trasforma rette in rette conservando il parallelismo.

1a. la composizione di affinità è *associativa*;

1b. l'*elemento neutro* è la trasformazione identica $I\colon (x; y) \to (x; y)$;

1c. ogni affinità T ammette l'inversa, cioè esiste un'affinità T^{-1} tale che risulta:

$$T * T^{-1} = T^{-1} * T = I$$

Il gruppo delle affinità così definito **non è commutativo**; infatti, in generale:

$$T * T' \neq T' * T$$

Esempio 30

Siano:

$$T\colon (x; y) \to (2x + y;\ x - 3y)$$
$$T'\colon (x; y) \to (3x; y)$$

Risulta:

$$T * T'\colon (x; y) \to (6x + y;\ 3x - 3y)$$
$$T' * T\colon (x; y) \to (6x + 3y;\ x - 3y)$$

quindi $T * T' \neq T' * T$.

Verifichiamo che le similitudini dirette formano un sottogruppo del gruppo delle affinità. Basta dimostrare che sono verificate la proprietà di gruppo.

- Se T e T' sono due similitudini dirette di matrici associate:

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \qquad A' = \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix}$$

la trasformazione composta $T * T'$ ha associata la matrice prodotto:

$$A * A' = \begin{pmatrix} aa' - bb' & -ab' - ba' \\ ab' + ba' & aa' - bb' \end{pmatrix}$$

Una **similitudine** è un'affinità che mantiene costante il rapporto tra segmenti corrispondenti.

Si verifica quindi che componendo due similitudini dirette si ottiene una similitudine diretta.

- Considerata la similitudine T di matrice associata A, la trasformazione inversa ha matrice associata A^{-1} inversa di A:

$$A^{-1}=\begin{pmatrix} \dfrac{a}{a^2+b^2} & \dfrac{b}{a^2+b^2} \\ \dfrac{-b}{a^2+b^2} & \dfrac{a}{a^2+b^2} \end{pmatrix}$$

La trasformazione inversa è ancora una similitudine diretta.

Verifichiamo ora che le similitudini indirette non formano gruppo e quindi non costituiscono un sottogruppo del gruppo delle affinità. Infatti la trasformazione identica non è una similitudine indiretta e inoltre la composizione di due similitudini indirette T e T' di matrici associate rispettive A e A':

$$A=\begin{pmatrix} a & b \\ b & -a \end{pmatrix} \qquad A'=\begin{pmatrix} a' & b' \\ b' & -a' \end{pmatrix}$$

ha la matrice associata:

$$A*A'=\begin{pmatrix} aa'+bb' & ab'-a'b \\ a'b-ab' & aa'+bb' \end{pmatrix}$$

che determina una similitudine diretta.
Quindi: *la composizione di due similitudini indirette è una similitudine diretta.*

Inoltre, si può verificare che: *la composizione di due similitudini, l'una diretta e l'altra indiretta, è una similitudine indiretta.*

Concludendo:

a) *l'insieme delle similitudini dirette forma gruppo*;
b) *l'insieme delle similitudini indirette non forma gruppo*;
c) *l'insieme delle similitudini forma gruppo.*

Inoltre è facile convincersi che, essendo le isometrie delle particolari similitudini di rapporto 1, componendo due isometrie si ottiene ancora un'isometria, la legge di composizione è associativa, l'elemento neutro è l'identità, l'inversa di un'isometria è una isometria.

Concludendo: *l'insieme delle isometrie forma un sottogruppo del gruppo della affinità.*

5 Sottogruppi

Consideriamo il gruppo d'ordine 4:

$$\{U;\ X;\ Y;\ XY\}$$

introdotto nel § 3. Nella sua tabella moltiplicativa si può osservare che anche i due soli elementi:

$$\{U;\ X\}$$

composti con la stessa legge continuano a costituire un gruppo, di ordine 2, che merita evidentemente il nome di **sottogruppo** del gruppo originale.
Se G è un gruppo ed H è un suo sottoinsieme, non sarà vero, in generale, che H continui ad avere la proprietà di gruppo. Per esempio, riferendosi al gruppo:

$$G = \{0°;\ 90°;\ 180°;\ 270°\}$$

delle rotazioni di multipli di 90°, il sottoinsieme:

$$H = \{0°;\ 90°\}$$

non forma gruppo: componendo infatti due volte la rotazione di 90° se ne genera una di 180° che non figura in H.

Le condizioni che un sottoinsieme $H \subseteq G$ deve soddisfare per risultare un "sottogruppo" sono le seguenti:

1. se $a, b \in H$, allora anche $a \cdot b$ deve appartenere ad H;
2. se $a \in H$ anche a^{-1} deve appartenere ad H.

Segue, in particolare, che ogni sottogruppo $H \subseteq G$ deve contenere l'elemento neutro di G.

Osservazione 3

Se G è un gruppo è facile indicare due sottoinsiemi particolari che costituiscono un sottogruppo:

$$H = \{1\} \qquad K = G$$

Tali due sottogruppi meritano, ovviamente, il nome di **sottogruppi banali**.

Esempi

31 L'insieme $(\mathbb{Z}; +)$ è un sottogruppo del gruppo $(\mathbb{R}; +)$.

32 L'insieme dei numeri pari è un sottogruppo dell'insieme degli interi rispetto all'addizione.

33 Sia (V; +) il gruppo dei vettori del piano rispetto alla somma tra vettori. Se $\vec{v}$ è un determinato vettore, l'insieme S costituito dai vettori $k\vec{v}$, essendo k un numero reale, cioè l'insieme dei vettori paralleli a un vettore dato, è un sottogruppo di (V; +).

34 Consideriamo il gruppo moltiplicativo formato dalle quattro radici quarte complesse dell'unità:

$$G = \{1; i; -1; -i\}$$

Il sottoinsieme $H = \{1; -1\}$ è un sottogruppo di G; il sottoinsieme $K = \{i; -i\}$ invece non costituisce un sottogruppo: infatti, per esempio, $i \cdot (-i) = 1 \notin K$.

6 Il teorema di Lagrange

Tra l'ordine di un gruppo finito e quello dei suoi eventuali sottogruppi intercorre una relazione importante che costituisce il seguente teorema:

TEOREMA 3 (DI LAGRANGE) **L'ordine di un gruppo finito è divisibile per l'ordine di qualsiasi suo sottogruppo.**

DIMOSTRAZIONE
Sia $H \subseteq G$; per ogni elemento $a \in G$ consideriamo la totalità di elementi ottenibili come prodotto di a per ciascun elemento di H. Chiamiamo questo insieme "classe laterale a di H" e indichiamolo con H_a.
È facile riconoscere che, al variare di a, si ottengono classi laterali diverse ma certamente formate dallo stesso numero di elementi.
Tenuto conto che se prendiamo un elemento $a \in H$, la classe laterale H_a coincide con H stesso, si riconosce quindi che tutte le classi laterali hanno lo stesso numero p di elementi di H.
È altrettanto facile riconoscere che due classi laterali o sono disgiunte o coincidono.
Gli N elementi di G vengono pertanto a essere suddivisi su un certo numero n di classi laterali, ciascuna formata dallo stesso numero p di elementi.
Quindi, se N è l'ordine di G e p l'ordine del sottogruppo H, si ha:

$$N = n \cdot p$$

Cioè p, ordine del sottogruppo H, è un divisore dell'ordine N del gruppo G.

Osservazione 4

Il teorema di Lagrange serve, per esempio, a escludere che i gruppi di ordine 23 abbiano sottogruppi (oltre i due banali).
Infatti 23 è un numero primo, cioè non ha divisori diversi da 1 e da se stesso. Quindi, poiché l'ordine degli eventuali sottogruppi dovrebbe dividere 23, se ne deduce che non esistono sottogruppi (non banali).
Dal teorema di Lagrange segue che ogni gruppo di ordine p, con p primo, non ammette sottogruppi non banali.
Può inoltre dedursi che ogni gruppo di ordine p primo è isomorfo al gruppo delle rotazioni di angoli multipli di $\frac{2\pi}{p}$.

7 Anelli

Sia A un insieme in cui siano definite due leggi di composizione interna (due operazioni) che indichiamo con $+$ e con $\cdot$.

DEFINIZIONE Si dice che A è un anello se:

1. A è un *gruppo abeliano* rispetto all'operazione +;

2a. la legge $\cdot$ è *associativa*;

2b. la legge $\cdot$ è *distributiva* rispetto alla legge +.

In definitiva, A è un anello se valgono i seguenti assiomi:

▶ *per la legge +*

1a. proprietà associativa:

$$a + (b + c) = (a + b) + c \qquad \forall\, a, b, c \in \mathrm{A}$$

1b. esiste l'elemento neutro che indichiamo con 0:

$$a + 0 = 0 + a = a \qquad \forall\, a \in \mathrm{A}$$

1c. esiste, $\forall\, a \in \mathrm{A}$, **il simmetrico**, che chiamiamo **opposto** e indichiamo con $-a$:

$$a + (-a) = (-a) + a = 0$$

1d. proprietà commutativa:

$$a + b = b + a \qquad \forall\, a, b \in \mathrm{A}$$

▶ *per la legge $\cdot$*

2a. proprietà associativa:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \forall\, a, b, c \in \mathrm{A}$$

2b. proprietà distributiva della legge $\cdot$ rispetto alla legge +:

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \forall\, a, b, c \in \mathrm{A}$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Se la legge $\cdot$ è **commutativa** l'anello si dice **commutativo.**

Se esiste l'**elemento neutro** rispetto alla legge $\cdot$ l'anello si dice **unitario**.

Esempi

35 L'insieme dei numeri interi dotato delle ordinarie operazioni di somma e di prodotto è il modello fondamentale di anello.
In realtà il prodotto sugli interi gode anche di proprietà più ricche di quelle minime richieste in un anello:

- è commutativo;
- vale la legge di annullamento del prodotto.

Si tratta di un anello particolare: un anello "commutativo" e "privo di divisori dello zero", intendendo con questo nome elementi diversi dallo zero il cui prodotto dia zero.

36 L'insieme P degli interi pari, dotato delle ordinarie operazioni di somma e prodotto, è un anello: infatti la somma o il prodotto di numeri pari dà risultati pari e l'equazione:

$$a + x = b$$

con a e b pari ha ovviamente soluzione $x = b - a$ pari.
Esso è un anello "non unitario".
Attenzione: l'insieme D dei dispari non è un anello…!

37 L'insieme $\mathbb{R}$ dei numeri reali, come quello $\mathbb{C}$ dei complessi, al solito dotati degli ordinari somma e prodotto, costituiscono anelli commutativi unitari privi di divisori dello zero.

38 Consideriamo l'anello delle **classi resto modulo un intero** m (vedi Algebra 1, § 2.12).
La relazione sull'insieme $\mathbb{Z}$ degli interi:

$$a \equiv b \quad \Leftrightarrow \quad a - b = k \cdot m$$

è una relazione d'equivalenza: l'insieme delle classi d'equivalenza rispetto a tale relazione si dice "insieme $\mathbb{Z}_m$ delle classi resto modulo m".
Se, per esempio, $m = 6$, $\mathbb{Z}_6$ è costituito dalle 6 classi:

$$[0], \quad [1], \quad [2], \quad [3], \quad [4], \quad [5]$$

ove con il simbolo [0] si intende l'insieme {…; –6; 0; 6; 12; …} con il simbolo [1] si intende l'insieme {…; –11; –5; 1; 7; 13; …} ecc.
Sugli elementi di $\mathbb{Z}_m$ si eseguono somme e prodotti al modo seguente:

$$[a] + [b] = [a + b]$$
$$[c] \cdot [d] = [c \cdot d]$$

procedimento corretto e che rispetta i tre gruppi di proprietà che spettano a una struttura di anello.
Tornando all'esempio di $m = 6$, si ha:

$$[4] + [2] = [4 + 2] = [0]$$
$$[2] \cdot [4] = [2 \cdot 4] = [8] = [2]$$

Attenzione:

$$[3] \cdot [2] = [6] = \ldots [0]$$

Nell'anello $\mathbb{Z}_6$ si incontrano divisori dello zero, cioè elementi diversi dallo zero il cui prodotto dà zero.
Evidentemente la presenza o meno di divisori dello zero in $\mathbb{Z}_m$ dipende dall'essere m prodotto di due o più fattori o primo.
Nell'anello $\mathbb{Z}_6$ abbiamo trovato due divisori dello zero nelle due classi [3] e [2], infatti 3 e 2 sono fattori di 6.
Nell'anello $\mathbb{Z}_7$ non si trovano divisori dello zero perché il numero 7 non ha fattori essendo un numero primo.

39 L'insieme $\mathcal{P}[x]$ dei polinomi in x a coefficienti reali, dotato dell'ordinaria somma e moltiplicazione tra polinomi, è un anello commutativo privo di divisori dello zero.

40 Consideriamo l'anello delle matrici quadrate d'ordine n (vedi vol. 2, § 5.2).
L'insieme M delle matrici 2×2 dotato delle ordinarie operazioni di somma e di prodotto, righe per colonne, fra matrici costituisce un anello non commutativo, dotato di divisori dello zero.
Infatti, nel prodotto tra matrici non vale la legge di **annullamento del prodotto**, cioè, se il prodotto tra due matrici è la matrice nulla, non necessariamente una delle due matrici è nulla. Per esempio:

$$\begin{pmatrix} 1 & 0 \\ 6 & 0 \end{pmatrix} * \begin{pmatrix} 0 & 0 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Anche l'insieme delle matrici quadrate di ordine 3 o quello delle matrici quadrate di qualsivoglia ordine forniscono esempi di anelli non commutativi via via più complicati.

41 L'insieme X delle coppie di numeri reali $(a; b)$ dotato delle operazioni di

a) somma: $(a; b) + (c; d) = (a + b; c + d)$

b) prodotto: $(a; b) \cdot (c; d) = (a \cdot b; c \cdot d)$

è un anello commutativo dotato di divisori dello zero, infatti:

$$(1; 0) \cdot (0; 1) = (0; 0)$$

Domanda Che cosa si perde in presenza di divisori dello zero dell'ordinaria aritmetica?

Risposta Si perde la legge di semplificazione dei fattori comuni nelle uguaglianze. Da

$$a \cdot x = a \cdot y$$

siamo usi dedurre che se $a \neq 0$ segue $x = y$. Questo perché si scrive l'uguaglianza nella forma:

$$a \cdot (x - y) = 0$$

da cui, stante l'assenza di divisori dello zero, si ricava:

$$a \neq 0 \quad \Rightarrow \quad x - y = 0$$

Ovviamente le cose vanno diversamente nell'anello del corrente esempio.
Scelto $a = (1; 0)$, si ha:

$$(1; 0) \cdot (0; 2) = (1; 0) \cdot (0; 1)$$

pur essendo $(0; 2) \neq (0; 1)$.

8 Corpi - Campi

Sia K un anello rispetto alle operazioni + e $\cdot$ e sia 0 l'elemento neutro rispetto all'operazione +.
Se l'insieme $K - \{0\}$ è un gruppo rispetto all'operazione $\cdot$ allora si dice che K è un **corpo**.
Se poi la seconda operazione $\cdot$ è **commutativa** si dice che K è un **campo**. Pertanto, affinché l'insieme K sia un **corpo** rispetto alle operazioni + e $\cdot$, agli assiomi 1a, 1b, 1c, 1d, 2a, 2b del § 7, si devono aggiungere gli assiomi:

2c. esiste l'elemento neutro, che indichiamo con 1, rispetto alla legge $\cdot$

$$a \cdot 1 = 1 \cdot a = a \qquad \forall a \in K$$

2d. esiste, $\forall a \in K - \{0\}$, il simmetrico $a^{-1} \in K$, che chiamiamo inverso

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

Affinché K sia un **campo** si deve aggiungere l'assioma:

2e. proprietà commutativa

$$a \cdot b = b \cdot a \qquad \forall\, a, b \in \mathrm{K}$$

Pertanto possiamo dare la seguente:

DEFINIZIONE Un insieme X dotato di due operazioni, somma e prodotto, si dice **corpo** se:

1. è un anello;
2. per $a \neq 0$ le equazioni:
$$a \cdot x = b \quad \text{e} \quad y \cdot a = b$$
sono sempre risolubili.

Esempi

42 L'insieme $\mathbb{R}$ dei numeri reali è un campo rispetto alle operazioni di addizione e moltiplicazione.

43 Il campo più semplice è l'insieme $\mathbb{Z}_2$ delle classi resto modulo 2: i suoi elementi sono $\{[0]; [1]\}$; la somma e il prodotto sono ovvi.

44 L'insieme $\mathbb{C}$ dei numeri complessi è un campo rispetto alle operazioni di addizione e moltiplicazione.
Lo zero è l'unità rispetto alla somma e l'opposto di $z = a + i\,b$ è $-z = -a - i\,b$.
L'unità rispetto alla moltiplicazione è 1, mentre l'inverso di $z \neq 0$ è:

$$z^{-1} = \frac{1}{z} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$$

45 Consideriamo l'insieme delle coppie ordinate $(a; b)$ di numeri reali.
Definiamo la somma nel modo seguente:

$$(a; b) + (c; d) = (a + c; b + d)$$

Rispetto alla somma l'unità è la coppia $(0; 0)$ e l'opposta di $(a; b)$ è la coppia $(-a; -b)$.
Definiamo la moltiplicazione al modo seguente:

$$(a; b) \cdot (c; d) = (ac - db; ad + bc)$$

L'unità è la coppia $(1; 0)$ e l'inversa di $(a; b) \neq (0; 0)$ è la coppia:

$$\left(\frac{a}{a^2+b^2};\ -\frac{b}{a^2+b^2}\right)$$

È facile verificare che l'insieme delle coppie ordinate $(a; b)$ di numeri reali così strutturato è un **campo**; non è difficile riconoscere che questo insieme non è che il campo dei numeri complessi.

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

47 Sia $\mathrm{Q}[x]$ l'insieme delle funzioni razionali a coefficienti reali. Se

$$f(x) = \frac{P_1(x)}{P_2(x)} \qquad \text{e} \qquad g(x) = \frac{P_3(x)}{P_4(x)}$$

sono due funzioni razionali ($P_1(x)$, $P_2(x)$, $P_3(x)$, $P_4(x)$ sono polinomi in x), si definisce somma la funzione:

$$\varphi(x) = f(x) + g(x) = \frac{P_1(x)\cdot P_4(x) + P_2(x)\cdot P_3(x)}{P_2(x)\cdot P_4(x)}$$

L'elemento neutro è il polinomio a coefficienti tutti nulli, l'opposta di $f(x)$ è la funzione $-f(x)=-\dfrac{P_1(x)}{P_2(x)}$.

Definiamo il prodotto al modo seguente:

$$\tau(x)=f(x)\cdot g(x)=\frac{P_1(x)\cdot P_3(x)}{P_2(x)\cdot P_4(x)}$$

L'unità è il polinomio $I(x)=1$ e la reciproca di $f(x)$ (che non sia il polinomio a coefficienti tutti nulli) è:

$$\frac{1}{f(x)}=\frac{P_2(x)}{P_1(x)}.$$

L'insieme $Q[x]$ così strutturato è un campo.

9 Il campo delle classi resto modulo *p* con *p* primo

Abbiamo osservato precedentemente che le classi resto modulo p formano un anello commutativo unitario. Dimostriamo ora che, se p è primo, esiste l'inversa rispetto alla moltiplicazione per ogni classe $[a]$ non nulla.
Consideriamo le classi non nulle:

$$[1],\quad [2],\quad \ldots,\quad [p-1]$$

e moltiplichiamo tali classi per $[a]$.
Si ottengono $p-1$ classi prodotto:

$$[a],\quad [2a],\quad \ldots,\quad [(p-1)a]$$

tutte non nulle non essendoci divisori dello zero.
Esse, a parte l'ordine, coincidono necessariamente con le precedenti; pertanto i prodotti:

$$([a]\cdot[2a]\cdot\ldots\cdot[(p-1)a]) \qquad \text{e} \qquad ([1]\cdot[2]\cdot\ldots\cdot[p-1])$$

coincidono. Si ha quindi, posto:

$$1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)=(p-1)!$$
$$[a^{p-1}]\cdot[(p-1)!]=[(p-1)!]$$

Semplificando si ottiene:

$$[a^{p-1}]=[1]$$

Poiché:

$$[a^{p-1}]=[a^{p-2}]\cdot[a]$$

possiamo scrivere:

$$[a^{p-2}]\cdot[a]=[1]$$

L'uguaglianza esprime che l'inversa della classe $[a]$ non nulla è la classe $[a^{p-2}]=[a]^{p-2}$.

Esempio

48 Consideriamo il caso $p=5$. Calcoliamo gli inversi dei quattro elementi non nulli:

$[1]^{-1}=[1^3]=[1]$ (… ovvio!)
$[2]^{-1}=[2^3]=[8]=[3]$ infatti $[2]\cdot[3]=[1]$
$[3]^{-1}=[3^3]=[27]=[2]$ infatti $[3]\cdot[2]=[1]$
$[4]^{-1}=[4^3]=[64]=[4]$ infatti $[4]\cdot[4]=[1]$

10 Spazi vettoriali

Sia V un insieme nel quale siano definite una **legge di composizione interna** + e una **legge di composizione esterna** $\cdot$ a operatori in un **campo** K.

DEFINIZIONE Se l'insieme V è un **gruppo abeliano** rispetto alla legge + e se la legge di composizione esterna $\cdot$ gode delle proprietà:

I **distributiva** rispetto all'operazione +;
II **distributiva** rispetto alla somma in K;
III **associativa**;
IV **neutralità** rispetto all'unità moltiplicativa in K,

allora V prende il nome di **spazio vettoriale** sul campo K e gli elementi di V si dicono **vettori**, mentre gli elementi di K si dicono **operatori**.

Gli elementi dello spazio vettoriale V vengono indifferentemente indicati con $\vec{u}, \vec{v}, \vec{w}, \ldots$ oppure con **u**, **v**, **w**, ...

Riassumiamo qui di seguito gli assiomi di spazio vettoriale.

▶ Per la legge +

1a. proprietà associativa

$$\vec{u} + (\vec{v} + \vec{w}) = (\vec{u} + \vec{v}) + \vec{w} \qquad \forall \vec{u}, \vec{v}, \vec{w} \in \mathrm{V}$$

1b. esiste l'elemento neutro

$$\vec{v} + \vec{0} = \vec{0} + \vec{v} = \vec{v} \qquad \forall \vec{v} \in \mathrm{V}$$

1c. esiste, $\forall \vec{v} \in \mathrm{V}$, il simmetrico $-\vec{v} \in \mathrm{V}$

$$\vec{v} + (-\vec{v}) = (-\vec{v}) + \vec{v} = \vec{0} \qquad \forall \vec{v} \in \mathrm{V}$$

1d. proprietà commutativa

$$\vec{u} + \vec{v} = \vec{v} + \vec{u} \qquad \forall \vec{u}, \vec{v} \in \mathrm{V}$$

▶ Per la legge $\cdot$

I. proprietà distributiva rispetto all'operazione +

$$k \cdot (\vec{u} + \vec{v}) = k \cdot \vec{u} + k \cdot \vec{v} \qquad \forall \vec{u}, \vec{v} \in \mathrm{V}, \forall k \in \mathrm{K}$$

II. proprietà distributiva rispetto alla somma in K

$$(k + h) \cdot \vec{v} = k \cdot \vec{v} + h \cdot \vec{v} \qquad \forall \vec{v} \in \mathrm{V}, \forall h, k \in \mathrm{K}$$

III. proprietà associativa

$$k \cdot (h\vec{v}) = (kh) \cdot \vec{v} \qquad \forall \vec{v} \in \mathrm{V}, \forall h, k \in \mathrm{K}$$

IV. neutralità rispetto all'unità moltiplicativa in K

$$1 \cdot \vec{v} = \vec{v} \qquad \forall \vec{v} \in \mathrm{V}$$

essendo 1 l'elemento neutro rispetto alla moltiplicazione in K.

Esempi

49 L'esempio più importante di spazio vettoriale è l'insieme di vettori del piano e dello spazio: spazio vettoriale sul campo $\mathbb{R}$ dei numeri reali. La legge di composizione interna è l'operazione di somma tra vettori; la legge di composizione esterna è il prodotto di un numero reale per un vettore (vedi vol. 2, § 4.3). L'insieme dei vettori del piano e dello spazio non è però l'unico esempio di spazio vettoriale.

50 L'insieme dei polinomi di grado $\leq n$, con n assegnato, dotato dell'ordinaria somma tra polinomi è uno spazio vettoriale. Se, per esempio, $n = 2$, si hanno di fatto tre polinomi speciali:

$$P_0 = 1 \qquad P_1 = x \qquad P_2 = x^2$$

Ogni altro polinomio $P(x)$ dello spazio dei polinomi di grado ≤ 2

$$P(x) = a + bx + cx^2$$

è null'altro che

$$P(x) = a \cdot P_0 + b \cdot P_1 + c \cdot P_2$$

ed è individuato di fatto dai tre coefficienti $(a; b; c)$.
Si potrebbe quasi dire che: "lo spazio dei polinomi di grado ≤ 2 è uguale allo spazio $\mathbb{R}^3$ delle terne di numeri reali".

51 L'insieme delle matrici, anche rettangolari $m \times n$, dotato dell'ordinaria somma tra matrici e dell'ordinario prodotto di una matrice per un numero reale (vedi vol. 2, § 5.2) è uno spazio vettoriale. Per esempio, nello spazio delle matrici 2×2, consideriamo le quattro matrici:

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad M_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \qquad M_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Ogni altra matrice:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

è individuata dai quattro numeri (a, b, c, d) e può essere riconosciuta come:

$$M = a \cdot M_1 + b \cdot M_2 + c \cdot M_3 + d \cdot M_4$$

Anche qui si potrebbe quasi dire che: "lo spazio delle matrici 2×2 è uguale allo spazio $\mathbb{R}^4$ delle quaterne di numeri reali".

52 L'insieme delle trasformazioni lineari con le operazioni di somma e di prodotto per un numero reale definite nel § 6.14 del volume 2 è uno spazio vettoriale. Nel capitolo WEB 3 studieremo un esempio significativo di spazio vettoriale: l'insieme delle n-ple di numeri reali $\mathbb{R}^n$.

Base

Si dice che i vettori:

$$\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$$

costituiscono una **base** di V se ogni vettore di V si può rappresentare in uno ed in un solo modo come loro combinazione lineare.
Il numero di elementi di una base si dice **dimensione** dello spazio.

Esempi

53 I tre polinomi:

$$P_0 = 1 \qquad P_1 = x \qquad P_2 = x^2$$

dell'esempio 50 forniscono una base per lo spazio vettoriale dei polinomi di grado ≤ 2, che pertanto ha dimensione 3.

54 Le quattro matrici:

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad M_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad M_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad M_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

dell'esempio 51 forniscono una base dello spazio vettoriale delle matrici 2×2, che pertanto ha dimensione 4.

Sottospazi

Un sottoinsieme non vuoto S di uno spazio vettoriale V si dice "sottospazio di V" se per ogni coppia di elementi **u** e **v** di S e ogni coppia di numeri reali λ e μ riesce:

$$\lambda\mathbf{u} + \mu\mathbf{v} \in S$$

In particolare, ogni sottospazio contiene il vettore nullo.

Esempio

55 L'insieme S dei polinomi di grado ≤ 1 costituisce un sottospazio dello spazio vettoriale dei polinomi di grado ≤ 2.

11 Isomorfismi

Insiemi isomorfi

Nel § 3 abbiamo già accennato ai gruppi isomorfi, cioè della "stessa forma", nel caso dei gruppi finiti dello stesso ordine.
Per esempio, consideriamo il gruppo $(\mathbb{C}; \times)$ moltiplicativo delle radici quarte complesse dell'unità e il gruppo $(R_4, \cdot)$ delle rotazioni di multipli di 90° di un quadrato intorno al centro, già studiate nel § 3, di cui riportiamo a fianco le tabelle di composizione.
Si osserva subito che le due tabelle si trasformano l'una nell'altra se si stabilisce la corrispondenza biunivoca:

$\times \leftrightarrow \cdot \quad 1 \leftrightarrow 0° \quad i \leftrightarrow 90° \quad -1 \leftrightarrow 180° \quad -i \leftrightarrow 270°$

Tale corrispondenza biunivoca è un isomorfismo e i due gruppi si dicono **isomorfi**. Possiamo quindi dare la seguente

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

$\cdot$	0°	90°	180°	270°
0°	0°	90°	180°	270°
90°	90°	180°	270°	0°
180°	180°	270°	0°	90°
270°	270°	0°	90°	180°

DEFINIZIONE Un'applicazione biunivoca

$$f : M \to S$$

tra due insiemi $(M; \otimes)$ e $(S; \cdot)$ dotati di struttura, che verifichi la relazione:

$$f(a \otimes b) = f(a) \cdot f(b)$$

per ogni coppia di elementi $a, b \in M$ si dice un **isomorfismo** di $(M; \otimes)$ in $(S; \cdot)$.

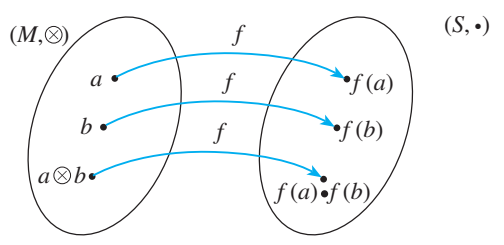

Figura 4

Inoltre:

DEFINIZIONE Due insiemi dotati di strutture $(M; \otimes)$ e $(S; \bullet)$ si dicono **isomorfi** se esiste un isomorfismo dell'uno nell'altro.

Se f è un isomorfismo di $(M; \otimes)$ in $(S; \bullet)$ l'applicazione inversa f^{-1}, che esiste in quanto f è per ipotesi biunivoca, è un isomorfismo: quindi la relazione "essere isomorfi" è una relazione simmetrica.
È facile riconoscere che essa è anche riflessiva e transitiva: si tratta quindi di una relazione d'equivalenza definita sulla famiglia degli insiemi dotati di struttura algebrica.

Esempi

56 Il gruppo R_3 delle rotazioni di un triangolo equilatero su se stesso è isomorfo al gruppo I_3 delle classi resto modulo 3.

57 Siano $(\mathbb{Z}; +)$ il gruppo additivo degli interi relativi, $(P; +)$ il gruppo additivo degli interi relativi pari e

$$f : \mathbb{Z} \to P \mid n \to 2n$$

f è un isomorfismo di $(\mathbb{Z}; +)$ in $(P; +)$ in quanto è biunivoca e qualunque siano n ed $m \in \mathbb{Z}$ risulta:

$$n \to 2n, \quad m \to 2m, \quad (n + m) \to 2(n + m) = 2n + 2m$$

cioè l'immagine della somma di n ed m è la somma delle immagini.

58 Siano ancora $(\mathbb{Z}; +)$ il gruppo additivo degli interi relativi e $(E; \bullet)$ il gruppo moltiplicativo $\{\ldots 2^{-2}; 2^{-1}; 2^0; 2^1; 2^2; \ldots\}$. Sia:

$$f : \mathbb{Z} \to E \mid n \to 2^n$$

L'applicazione è un isomorfismo in quanto è biunivoca e se

$$n \to 2^n, \quad m \to 2^m$$

allora

$$f(n + m) = 2^{n+m} = 2^n \cdot 2^m = f(n) \cdot f(m)$$

59 Sia $I_3 = \{[0]; [1]; [2]\}$, classi resto modulo 3, con l'ordinaria operazione di somma modulo 3.
$S = \{a; b; c\}$ con la tabella di composizione seguente:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

•	a	b	c
a	b	c	a
b	a	a	b
c	c	c	c

$(I_3; +)$ e $(S; \bullet)$ non sono isomorfi. Infatti la legge di composizione in I_3 è commutativa, mentre quella in S non lo è, poiché $a \bullet b = c$ mentre $b \bullet a = a$.
Se f fosse un isomorfismo dovrebbe accadere che:

$$f(c) = f(a \bullet b) = f(a) + f(b) = [0] + [1] = [1] + [0] = f(b) + f(a) = f(b \bullet a) = f(a)$$

contraddicendo la biunivocità.

Osservazione 5

Se (M; ⊗) e (S; •) sono isomorfi, la legge di composizione • definita su S è deducibile:

- da quella ⊗ assegnata su M;
- dall'isomorfismo f.

Siano infatti α e β due elementi di S, stante la biunivocità di f esistono a e b in M tali che $\alpha = f(a)$ e $\beta = f(b)$, quindi $\alpha \bullet \beta = f(a \otimes b)$.

Esempi

60 L'unica struttura algebrica che rende S = {a; b; c} isomorfo a (M; +) con $a \leftrightarrow [0]$, $b \leftrightarrow [1]$, $c \leftrightarrow [2]$, è quella riportata nella tabella a fianco.
Infatti, per esempio:

$$f(c \bullet b) = f(c) + f(b) = [2] + [1] = [0] = f(a)$$

quindi deve essere:

$$c \bullet b = a$$

•	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

61 *Sia* (M; ⊗) *il gruppo* {a; a^2; a^3; 1} *(Tab. 1) e sia* (S; •) *il gruppo sempre di quattro elementi, costituito dalle quattro radici quarte dell'unità:* {i; –1; $-i$; 1} *strutturato con l'ordinaria moltiplicazione tra numeri complessi (Tab. 2).*
Esaminare se (M; ⊗) *e* (S; •) *sono isomorfi.*

Tab. 1

⊗	a	a^2	a^3	1
a	a^2	a^3	1	a
a^2	a^3	1	a	a^2
a^3	1	a	a^2	a^3
1	a	a^2	a^3	1

Tab. 2

•	i	–1	$-i$	1
i	–1	$-i$	1	i
–1	$-i$	1	i	–1
$-i$	1	i	–1	$-i$
1	i	–1	$-i$	1

Per dichiarare che i due gruppi sono isomorfi occorre un isomorfismo:

$$f: \{a; a^2; a^3; 1\} \rightarrow \{i; -1; -i; 1\}$$

Osserviamo che poiché ogni isomorfismo tra due gruppi trasforma necessariamente l'elemento neutro di un gruppo nell'elemento neutro dell'altro, cioè:

$$f(1) = 1$$

le possibili "immagini" $f(a)$ di a sono:

$$f(a) = i \quad \text{oppure} \quad f(a) = -1 \quad \text{oppure} \quad f(a) = -i$$

La seconda di tali scelte non è accettabile: se fosse $f(a) = -1$, dovendo riuscire

$$f(a^3) = f(a) \cdot f(a) \cdot f(a) = -1$$

sarebbe $f(a^3) = f(a)$, perdendo la biunivocità.
Le altre due scelte forniscono due isomorfismi f e g diversi:

$$f(a) = i \qquad f(a^2) = -1 \qquad f(a^3) = -i \qquad f(1) = 1$$

e

$$g(a) = -i \qquad g(a^2) = -1 \qquad g(a^3) = i \qquad g(1) = 1$$

Gli automorfismi

Nel caso:

$$(M; \otimes) = (S; \cdot)$$

in cui i due insiemi dotati di struttura coincidano, gli isomorfismi f di $(M; \otimes)$ in $(M; \otimes)$ prendono il nome di **automorfismi**.
L'automorfismo più semplice è quello rappresentato dall'applicazione identica.
È evidente che se f e g sono due automorfismi di $(M; \otimes)$ allora anche le applicazioni composte $f \cdot g$ e $g \cdot f$ sono automorfismi di $(M; \otimes)$.
L'insieme degli automorfismi di $(M; \otimes)$ costituisce un gruppo, che prende naturalmente il nome di **gruppo degli automorfismi** di $(M; \otimes)$.

Esempio

62 *Sia* $(M; \otimes) = \{a; a^2; a^3; 1\}$. *Determinare il gruppo dei suoi automorfismi.*

Come nel precedente problema cerchiamo "empiricamente" le possibili immagini $f(a)$ dell'elemento a tramite l'automorfismo f:

$$f(a) = a \quad \text{oppure} \quad f(a) = a^2 \quad \text{oppure} \quad f(a) = a^3$$

La seconda scelta $f(a) = a^2$ porterebbe $f(a) = 1 = f(1)$ contraddicendo alla biunivocità. Delle altre due scelte, la prima produce:

$$f(a) = a \qquad f(a^2) = a^2 \qquad f(a^3) = a^3 \qquad f(1) = 1$$

automorfismo identico, la terza:

$$g(a) = a^3 \qquad g(a^2) = a^2 \qquad g(a^3) = a \qquad g(1) = 1$$

Dunque, il gruppo $\{a; a^2; a^3; 1\}$ ha due automorfismi: l'identità f e l'applicazione g che porta:

$$1 \to 1 \qquad a \to a^3 \qquad a^2 \to a^2 \qquad a^3 \to a$$

È evidente che tale famiglia di automorfismi costituisce, a sua volta, un gruppo molto semplice di due elementi f e g tali che: $g \cdot g = f$.

Quesiti di verifica

1 Date le seguenti leggi:

a) $a * b = a^2 b$ $\quad (a, b \in \mathbb{Z})$

b) $a \odot b = \sqrt{ab}$ $\quad (a, b \in \mathbb{Q}^+)$

c) $a \circ b = \dfrac{1}{ab}$ $\quad (a, b \in \mathbb{Q}_0)$

quale delle seguenti affermazioni è corretta?

[a] le tre leggi sono interne
[b] solo la legge *a*) è interna
[c] solo le leggi *a*) e *b*) sono interne
[d] solo le leggi *a*) e *c*) sono interne

2 Nell'insieme $\mathbb{R}_0^+$ la legge $*$ così definita:

$$a * b = \sqrt{a} + \sqrt{b}$$

è:

[a] commutativa
[b] associativa
[c] commutativa e associativa
[d] né commutativa né associativa

3 Nell'insieme $\mathbb{R}_0$ la legge $*$ così definita:

$$a * b = \frac{1}{a} + \frac{1}{b}$$

è:

[a] solo associativa
[b] associativa e commutativa
[c] solo commutativa
[d] né associativa né commutativa

4 Date le leggi definite in $\mathbb{Z}$:

a) $a \circ b = a^2 b$
b) $a \odot b = a + 2b$
c) $a * b = a^2 - ab$

quale delle seguenti affermazioni è corretta?

[a] la legge $\circ$ è distributiva rispetto alla legge $\odot$
[b] la legge $\circ$ è distributiva rispetto alla legge $*$
[c] la legge $\odot$ è distributiva rispetto alla legge $*$
[d] le tre affermazioni precedenti sono false

5 Sia definita in $\mathbb{R} - \{-2\}$ la legge:

$$x \odot y = xy + 2(x + y) + 2$$

L'elemento neutro è:

[a] $\frac{1}{2}$
[b] -1
[c] 1
[d] non esiste elemento neutro

6 Sia data in $E = \mathbb{R} - \left\{-\frac{1}{2}\right\}$ la legge:

$$x \odot y = 2xy + x + y$$

Quale delle seguenti affermazioni è falsa?

[a] la legge $\odot$ è associativa
[b] l'elemento neutro è 0
[c] il reciproco di x è $\dfrac{-x}{2x+1}$
[d] E è un gruppo non commutativo rispetto all'operazione $\odot$

7 Sia $E \subset \mathbb{Z}$ l'insieme dei multipli di 7. Quale delle seguenti affermazioni è vera?

[a] l'insieme E è un gruppo commutativo rispetto alla somma
[b] l'insieme E è un gruppo commutativo rispetto al prodotto
[c] l'insieme E è un gruppo rispetto al quoziente
[d] le precedenti affermazioni sono false

8 Sia P l'insieme dei numeri pari relativi dotato delle ordinarie operazioni + e × di somma e prodotto tra interi. Allora...

[a] P è un anello unitario
[b] non esiste l'elemento neutro rispetto a +
[c] P è un anello
[d] non esiste l'opposto di ogni elemento di P

9 L'insieme E delle coppie $(x; 0)$, $x \in \mathbb{Z}$, in cui sono definite le operazioni:

$$(x; 0) + (y; 0) = (x + y; 0)$$
$$(x; 0) \times (y; 0) = (xy; 0)$$

è:

[a] un campo
[b] un anello non commutativo
[c] un corpo
[d] un anello commutativo

Laboratorio di **informatica**

Comandi → **DERIVE**
MOD
Collect
Crea matrice
Identity_matrix

1. Il campo delle classi resto modulo p

Le classi resto modulo p sono semplicemente i p interi

$$0, 1, 2, ..., p - 1$$

addizionati, sottratti o moltiplicati fra loro con le ordinarie regole dell'aritmetica prendendo sempre i risultati

$$... \text{ modulo } p$$

DERIVE possiede l'operazione MOD e quindi consente di sperimentare facilmente l'aritmetica sulla classi resto.

La tavola pitagorica Mod *p*
Costruiamo la tabella dei prodotti Mod p servendoci della funzione:

MOD(u, p)

che fornisce il valore dell'intero u Mod p. Useremo due volte il comando VECTOR:

- la prima per costruire le righe della tabella dei prodotti $1 * j$, $2 * j$, ... $(p - 1) * j \mod p$;
- la seconda per raccogliere le $p - 1$ righe in una unica tabella.

Per costruire le righe in corrispondenza a qualunque intero p useremo *Dichiara - Definisci funzione*:

riga_prodotti(i, p):=VECTOR(MOD(i * j, p), j, 1, p – 1)

Per produrre l'intera tabella in corrispondenza a qualunque intero p, di nuovo, *Dichiara - Definisci funzione*:

prodotto(p):=VECTOR(riga_prodotti(i, p), i, 1, p – 1)

Una scoperta sorprendente...
Stampata la tabella moltiplicativa delle classi Mod 7 (fig. 1), si vede come in ogni colonna ed – evidentemente per simmetria – in ogni riga si trovi uno ed un solo 1: l'osservazione può essere letta nel modo seguente:

$$\forall i \in [1, 6] \quad \exists j \in [1, 6] \rightarrow i * j \equiv 1 \text{ Mod } 7$$

Il numero j corrispondente merita il nome di...

$$\frac{1}{i}$$

Questo vuol dire che nell'aritmetica delle classi resto Mod p, con p numero primo, ogni elemento, naturalmente diverso da 0 e da p stesso, è dotato di inverso moltiplicativo.
Si ricordi che invece, nell'ordinaria aritmetica, solo i numeri 1 e –1 possiedono inverso moltiplicativo: per tutti gli altri infatti si sono dovuti inventare i numeri razionali!

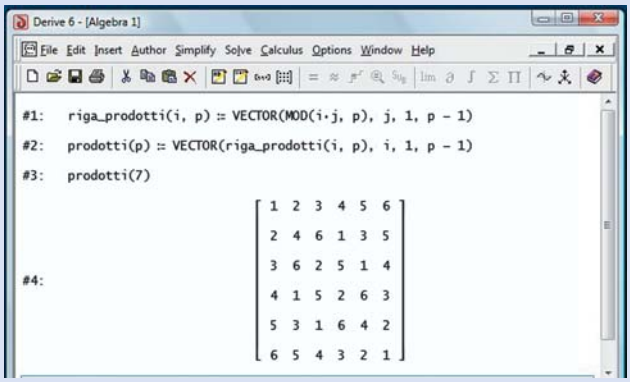

Figura 1.

La divisione
Scoperto che ogni elemento diverso da zero è dotato di inverso moltiplicativo, ha senso eseguire le divisioni, naturalmente sempre con divisore diverso da zero:

$$\frac{i}{j} = i * \frac{1}{j}$$

La tavola pitagorica della divisione
Costruiamo ora con DERIVE la tabella delle divisioni fra interi nell'aritmetica Mod p: il comando fondamentale di cui servirsi è:

SOLVE_MOD(a.x=b, x, p)

che produce un vettore contenente le soluzioni dell'equazione:

$$a \cdot x = b$$

nell'aritmetica Mod p:

- una e una sola $\forall a \neq 0$ Mod p se p è primo;
- nessuna, una o a volte più di una se p non è primo.

La tabella seguente riporta la tabella delle divisioni relative alla scelta $p = 11$.

j/i	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	6	1	7	2	8	3	9	4	10	5
3	4	8	1	5	9	2	6	10	3	7
4	3	6	9	1	4	7	10	2	5	8
5	9	7	5	3	1	10	8	6	4	2
6	2	4	6	8	10	1	3	5	7	9
7	8	5	2	10	7	4	1	9	6	3
8	7	3	10	6	2	9	5	1	8	4
9	5	10	4	9	3	8	2	7	1	6
10	10	9	8	7	6	5	4	3	2	1

I valori in tabella rappresentano i quozienti j/i dei numeri j con cui sono contrassegnate le colonne per i numeri i delle righe.

Osservazione 1
La tabella moltiplicativa è, come l'ordinaria tavola pitagorica, simmetrica. Naturalmente questo non accade per la tabella delle divisioni: la divisione non è operazione commutativa!

2. Le matrici di rotazione

Tra le trasformazioni del piano abbiamo incontrato le rotazioni e abbiamo riconosciuto le matrici ad esse associate.
Abbiamo del resto già imparato:

- ad assegnare una matrice con DERIVE;
- a operare con le matrici.

A una rotazione di un angolo α corrisponde la matrice:

$$A(\alpha) := \begin{pmatrix} \cos\alpha & -\text{sen}\alpha \\ \text{sen}\alpha & \cos\alpha \end{pmatrix}$$

Eseguire successivamente due rotazioni, la prima di un angolo α e successivamente una di angolo β, corrisponde naturalmente ad eseguire una volta sola una rotazione di un angolo $(\alpha + \beta)$.
Verifichiamo il fenomeno facendo calcolare a DERIVE il prodotto delle matrici corrispondenti alle due rotazioni.
La forma sotto cui si presenta il risultato dipende dall'opzione scelta per semplificare le espressioni trigonometriche: la scelta iniziale di DERIVE sarà probabilmente quella Auto (fig. 2).

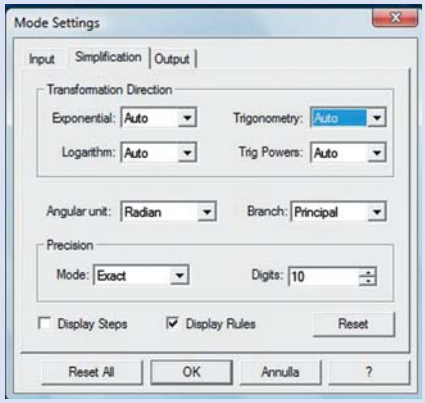

Figura 2.

Con questa scelta il prodotto delle due matrici di rotazione si presenta come in figura 3. Scegliendo invece come *Impostazioni di Semplificazione* per la trigonometria

Collect

si ottiene esattamente la matrice $A(\alpha + \beta)$ di figura 4.

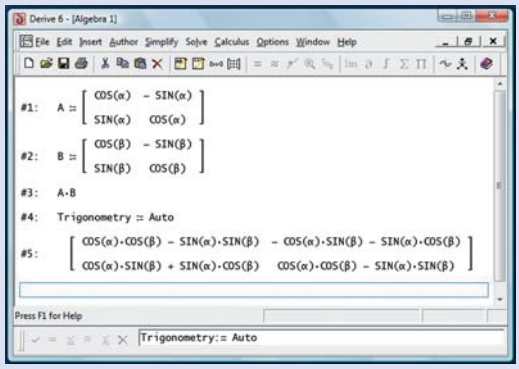

Figura 3.

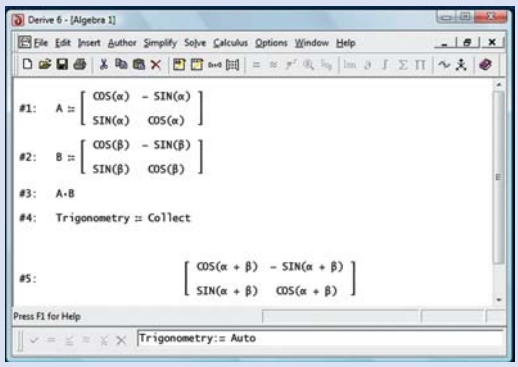

Figura 4.

Osservazione 2
Le due espressioni per il prodotto $A(\alpha) * A(\beta)$ rappresentano naturalmente la stessa matrice. La scelta di svolgere, Expand, le espressioni trigonometriche o di condensarle, Collect, contribuisce semplicemente alla nostra capacità di lettura.

Un esempio
Consideriamo le matrici:

$$A=\begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \qquad B=\begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{1}{2} \end{pmatrix}$$

corrispondenti alle rotazioni $\alpha=30°=\frac{\pi}{6}$ e $\beta=60°=\frac{\pi}{3}$.

Il prodotto

$$A*B=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

corrisponde ovviamente alla matrice $A\left(\frac{\pi}{2}\right)$.

3. Lo spazio vettoriale delle matrici 2 × 2

Le matrici 2×2 si moltiplicano per uno scalare e si sommano... tanto basta a riconoscere che formano uno spazio vettoriale.
Spazio di dimensione 4: infatti, dette A, B, C, D le seguenti 4 matrici:

$$A=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad B=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad C=\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad D=\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

per qualsiasi altra si ha:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}=a\cdot A+b\cdot B+c\cdot C+d\cdot D$$

La tabella moltiplicativa
Le 4 matrici A, B, C, D considerate sopra possono essere moltiplicate fra loro ottenendo la tabella moltiplicativa riportata a fianco, nella quale con il simbolo 0 indichiamo naturalmente la matrice tutta zeri.

•	A	B	C	D
A	A	B	0	0
B	0	0	A	B
C	C	D	0	0
D	0	0	C	D

Usiamo DERIVE
La tabella scritta può essere ricavata anche servendosi di DERIVE:

- assegniamo le quattro matrici A, B, C, D (Crea matrice 2 x 2 ecc.);
- assegniamo la matrice identica (Identity_matrix(2)):

$$U=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- definiamo il vettore:

$$M = [U, A, B, C, D]$$

- a questo punto si ha:

$$M_1 = U, \qquad M_2 = A, \qquad M_3 = B, \qquad M_4 = C, \qquad M_5 = D$$

- definiamo la tabella moltiplicativa:

$$\text{tavola} = \text{VECTOR}(\text{VECTOR}(M_i * M_j, j, 1, 5), i, 1, 5)$$

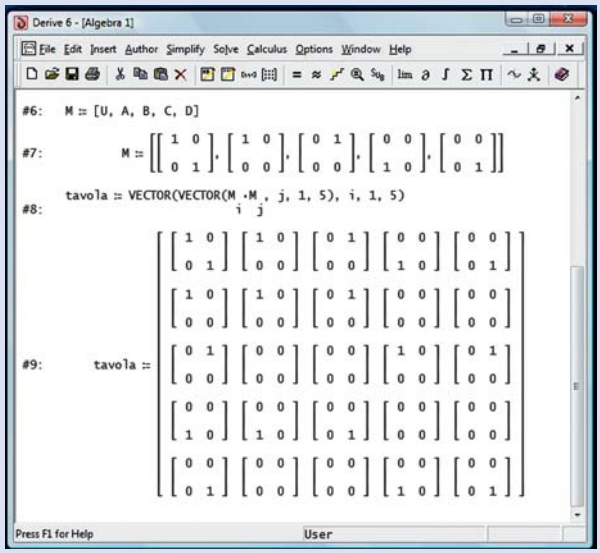

Figura 5.

4. Il gruppo delle radici *n*-sime dell'unità

Si dicono radici n-sime dell'unità i numeri complessi z tali che:

$$z^n = 1 \qquad n \in \mathbb{N}$$

È stato visto, occupandosi dei numeri complessi, che esistono n numeri complessi diversi $z_1, z_2, \ldots, z_n$ radici n-sime dell'unità.
La loro espressione con DERIVE è, da *Author*, la seguente:

```
VECTOR(cos(2k*pi/n)+sin(2k*pi/n), k, 0, n–1)
```

Si tratta degli n numeri complessi rappresentati sul piano dai vertici del poligono regolare di n lati inscritto nella circonferenza di centro l'origine e raggio 1 con un vertice nel punto A (1; 0).
Il grafico del poligono regolare che ha tali radici come vertici si ottiene:

- costruendo il vettore:

```
VECTOR([cos(2k*pi/n),sin(2k*pi/n)], k, 0, n)
```

  il primo e l'ultimo punto, coincidenti, servono a disegnare completamente il poligono;

- chiedendone la semplificazione, pulsante [≈];
- chiedendo il grafico del vettore ottenuto.

Gli n numeri complessi radici n-sime dell'unità, composti fra loro con la moltiplicazione, formano un gruppo di n elementi, commutativo.
Il calcolo diretto delle radici dell'unità può essere fatto con DERIVE anche a partire dalla formula:

$$z = \cos\left(\frac{2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{n}\right)$$

che fornisce il secondo degli n valori, ovvero il primo dopo 1 stesso.
I successivi si determinano eseguendo le successive potenze:

$$z^2, z^3, \ldots, z^n = 1$$

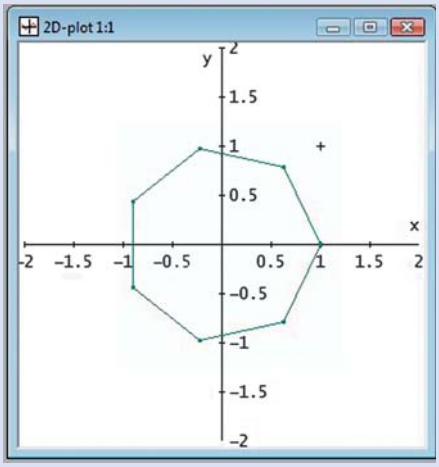

Figura 6.

5. Esercizi

1. Assegnate due matrici 2×2, A e B, servendosi della capacità di DERIVE di calcolare le matrici inverse, determinare la matrice X tale che:

$$A \cdot X = B$$

a) Il problema $X \cdot A = B$ ha la stessa soluzione?

b) Si riduca il problema alla risoluzione di un sistema di 4 equazioni in 4 incognite che si potrà risolvere con il SOLVE di DERIVE.

c) Assegnate tre matrici 2×2, A, B, C, si consideri il problema:

$$A \cdot X \cdot B = C$$

2. Assegnato un primo p e assegnata un'equazione di grado m:

$$x^m + a_1 x^{m-1} + \ldots + a_0 = 0$$

si cerchino empiricamente, cioè sperimentando con DERIVE i p valori $x = 0, 1, 2, \ldots, p-1$, le radici nell'aritmetica modulo p.

3. Assegnato n:

a) determinare con DERIVE le n radici complesse dell'unità $z_1, z_2, \ldots, z_n$;

b) costruire di fianco a ogni z_k l'insieme $z_k^2, z_k^3, z_k^4, \ldots$ delle relative potenze.

6. Programmi

I programmi di questo Laboratorio riguardano il gruppo delle radici n-sime dell'unità. I programmi consentono di riconoscere quali di tali radici siano primitive e quali no.

esercizi

Leggi di composizione

Quesiti

1. Si dia la definizione di *legge di composizione interna* definita in un insieme e si forniscano esempi. Quali sono le proprietà di una legge di composizione interna? Si forniscano esempi di leggi che godono della proprietà *commutativa*, *associativa*, *distributiva*.

2. Si dia la definizione di *elemento neutro*. Si dimostri che l'elemento neutro, se esiste, è unico.

3. Si dia la definizione di *elemento inverso* o *simmetrico*.
Supponiamo che la legge interna $\otimes$ definita nell'insieme E sia associativa e ammetta l'elemento neutro e che siano a^{-1} e b^{-1} i simmetrici di a e di b. Si dimostri che il simmetrico di $a \otimes b$ è $b^{-1} \otimes a^{-1}$.

4. Si dimostri che se la legge di composizione interna è associativa e ammette l'elemento neutro, allora l'inverso di un elemento, se esiste, è unico.

Sia $\mathbb{Z}$ l'insieme degli interi relativi. Per ciascuna delle seguenti leggi di composizione interna, indicata con il simbolo $*$, stabilire se è commutativa, associativa, se esiste l'elemento neutro, se esiste il simmetrico di ogni elemento di $\mathbb{Z}$.

1 $a * b = ab - a$
[*Poiché $b * a = ba - b \neq a * b$ l'operazione $*$ non è commutativa...*]

2 $a * b = 3ab$

3 $a * b = a^2 + b$

4 $a * b = a + b - ab$

5 $a * b = a^2 + b^2$

6 $a * b = a^2b^2$

7 $a * b = a + b + ab$

8 Siano $\mathbb{Z}$ l'insieme degli interi relativi e H l'insieme delle coppie $(a; b)$ con $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, in cui siano definite le due leggi $+$ e $\times$ di composizione interna:

$$(a; b) + (a'; b') = (a + a'; b + b')$$
$$(a; b) \times (a'; b') = (aa' - bb'; ab' - a'b)$$

Studiare le proprietà delle due leggi e stabilire se la legge $\times$ è distributiva rispetto alla legge $+$.

9 Siano a, b, c numeri reali fissati, tali che $ab \neq 0$. Si definisca in $\mathbb{R}$ una legge di composizione interna, tale che:

$$x \circ y = axy + b(x + y) + c$$

a) Quale condizione devono verificare a, b, c, affinché la legge sia associativa?
b) Nel caso in cui tale condizione sia verificata, mostrare che la legge $\circ$ ammette un elemento neutro e che ogni numero reale, eccettuato uno solo che va determinato, ammette un simmetrico.

a) [*Perché valga la proprietà associativa deve risultare:* $(x \circ y) \circ z = x \circ (y \circ z)$; *si ha:*
$(x \circ y) \circ z = (axy + b(x + y) + c) \circ z = az(axy + b(x + y) + c) + b(axy + b(x + y) + c + z) + c =$
$= a^2xyz + ab(xz + xy + yz) + b^2x + b^2y + z(b + ac) + bc + c$
$x \circ (y \circ z) = x \circ (ayz + b(y + z) + c) = ax(ayz + b(y + z) + c) + b(x + ayz + b(y + z) + c) + c =$
$= a^2xyz + ab(xz + xy + yz) + b^2z + b^2y + x(b + ac) + bc + c...]$ $ac - b^2 + b = 0$;

b) $e = -\frac{c}{b}$; $x^{-1} = -\frac{c(1+b)+b^2x}{b(ax+b)}$; $x \neq -\frac{b}{a}$

10 Siano $x = (m; \alpha)$ e $y = (n; \beta)$ elementi dell'insieme $\mathbb{Z} \times \mathbb{Q}$, essendo $\mathbb{Z}$ l'insieme degli interi relativi e $\mathbb{Q}$ l'insieme dei numeri razionali. Si definiscano in $\mathbb{Z} \times \mathbb{Q}$ le seguenti leggi di composizione interna:

$$x + y = (m + n; \alpha\beta)$$
$$x \times y = (mn; \alpha + \beta)$$

Dimostrare che le due leggi sono commutative, associative e ammettono un elemento neutro. Determinare per ogni legge l'insieme degli elementi aventi un simmetrico. Stabilire se la legge $\times$ è distributiva rispetto alla legge $+$.

[*Se* $e = (n; \beta)$ *è l'elemento neutro, deve risultare:* $x + e = e + x = x = (m; \alpha)$, *cioè* $(m + n; \alpha\beta) = (m; \alpha)$...]

per la legge $+$: elemento neutro $(0; 1)$; il simmetrico di $(m; \alpha)$ è $-x = \left(-m; \frac{1}{\alpha}\right)$ con $\alpha \neq 0$;

per la legge $\times$: elemento neutro $(1; 0)$; il simmetrico di $(m; \alpha)$ è $x^{-1} = \left(\frac{1}{m}; -\alpha\right)$ con $m \neq 0$; la legge $\times$ non è distributiva rispetto alla legge $+$

Vero o falso?

1.	L'elevamento a potenza tra numeri reali è una legge commutativa.	V	F
2.	La legge $\otimes$ definita su $\mathbb{R}$ da $a \otimes b = a^2 + b$ è commutativa.	V	F
3.	La legge $\otimes$ definita su $\mathbb{R}$ da $a \otimes b = a^2 + b$ è associativa.	V	F
4.	L'elevamento a potenza tra numeri reali è una legge associativa.	V	F
5.	Nell'insieme $\mathbb{R}_0$ strutturato con l'operazione di quoziente non esiste né l'elemento neutro né il simmetrico.	V	F

Gruppi

Quesiti

1. Si dia la definizione di *gruppo* e si forniscano esempi di gruppi *abeliani*.

2. L'insieme dei numeri complessi rispetto all'operazione di addizione forma gruppo. Giustificare questa affermazione. È un gruppo abeliano? Quale è il simmetrico del numero $z = x + i\,y$?

3. L'insieme delle radici seste dell'unità forma gruppo rispetto alla moltiplicazione tra numeri complessi. Dopo aver scritto le sei radici, giustificare questa affermazione.

4. Sia $M(n)$ l'insieme delle matrici quadrate di ordine n a determinante diverso da zero. L'insieme A è un gruppo rispetto all'operazione di prodotto tra matrici? Il sottoinsieme di $M(n)$ delle matrici a determinante uguale a 1 è un sottogruppo di $M(n)$?

5. L'insieme delle funzioni biunivoche di $\mathbb{R}$ in sé forma gruppo rispetto alla composizione di funzioni. Giustificare questa affermazione dimostrando che la composizione di funzioni gode della proprietà associativa e specificando quali sono l'elemento neutro e l'elemento simmetrico di una data biiezione.

6. Sia A l'insieme delle funzioni $f_m : \mathbb{R} \to \mathbb{R} \mid x \to mx$, con $m \in \mathbb{R}_0$, munito dell'operazione di composizione di funzioni. Si dimostri che A è un gruppo e si definisca l'elemento neutro e l'inversa di f_m.

11 Nell'insieme $\mathbb{R}$ dei numeri reali sia definita la seguente legge di composizione interna:

$$x \cdot y = x + y + 3xy \qquad \forall x, y \in \mathbb{R}$$

a) Dimostrare che la legge $\cdot$ è commutativa e associativa.

b) Sia A l'insieme $\mathbb{R} - \left\{-\frac{1}{3}\right\}$.

Dimostrare che A è un gruppo abeliano rispetto all'operazione $\cdot$.

b) [*Se* $e \in \mathbb{R}$ *è l'elemento neutro, allora* $x \cdot e = e \cdot x = x$, *quindi* $x + e + 3ex = x$ *se* $e = 0$; *se* x^{-1} *è il reciproco di* x *allora* $x \cdot x^{-1} = x^1 \cdot x = 0$, *pertanto* $x + x^{-1} + 3x \cdot x^{-1} = 0$...]

$e = 0$; $x^{-1} = \frac{-x}{1+3x}$, con $x \neq -\frac{1}{3}$

esercizi

12 Sia A l'insieme delle coppie $(a; b)$ di numeri reali, con $a \neq 0$, munito della legge di composizione interna:

$$(a; b) * (a'; b') = (aa'; ab' + b)$$

Dimostrare che A è un gruppo. A è un gruppo commutativo?
Dimostrare inoltre che l'insieme B delle coppie $(a; 0)$ di elementi A è un gruppo rispetto alla legge $*$.

A non è commutativo; $e = (1; 0)$; reciproco $\left(\frac{1}{a}; -\frac{b}{a}\right)$

13 Sia G l'insieme costituito dagli elementi $G = \{1; -1\}$. Dimostrare che G è un gruppo rispetto all'ordinaria moltiplicazione tra numeri.

14 Sia G l'insieme $\left\{1; -\frac{1}{2}+i\frac{\sqrt{3}}{2}; -\frac{1}{2}-i\frac{\sqrt{3}}{2}\right\}$ dove i è l'unità immaginaria.

Dimostrare che G è un gruppo rispetto alla moltiplicazione tra numeri complessi (G è l'insieme delle radici cubiche dell'unità).

15 Sia G l'insieme costituito dalle 4 sostituzioni:

$$k_1 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}; \quad k_2 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}; \quad k_3 = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}; \quad k_4 = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

Definiamo come "moltiplicazione" la sostituzione che si ottiene come applicazione sucessiva di due sostituzioni date, in un ordine dato, così per esempio:

$$k_2 \cdot k_4 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

Dimostrare che l'insieme $G = \{k_1; k_2; k_3; k_4\}$ è un gruppo rispetto alla moltiplicazione così definita. G è un gruppo abeliano?

Quesiti

1. Le rotazioni di multipli di 60° di un esagono regolare intorno al suo centro costituiscono un insieme di 6 trasformazioni dell'esagono in sé, che moltiplicate con l'ordinaria composizione, cioè applicando successivamente le due rotazioni componenti, formano gruppo. Scrivere la tabella moltiplicativa. Qual è la rotazione simmetrica di 120°?

2. Si dimostri che l'insieme delle similitudini dirette nel piano formano gruppo. È un gruppo commutativo?

3. L'insieme delle inversioni circolari rispetto allo stesso centro forma gruppo?

Vero o falso?

1. L'insieme dei pari è un gruppo rispetto all'operazione di prodotto. V F

2. L'insieme V dei vettori del piano è un gruppo rispetto al prodotto scalare. V F

Nell'insieme delle trasformazioni del piano:

3. le traslazioni formano un gruppo commutativo. V F

4. le rotazioni attorno allo stesso centro formano gruppo. V F

5. le rotazioni formano gruppo. V F

6. le isometrie formano gruppo. V F

7. Se G è un gruppo allora, se $a, b, c \in G$:

$ab = ac \quad \Rightarrow \quad b = c$ V F

$ab = ca \quad \Rightarrow \quad b = c$ V F

8. Sia V il gruppo dei vettori del piano rispetto alla somma vettoriale.
Se $\mathbf{v}$ è un vettore fissato, l'insieme dei vettori del tipo $\mathbf{u} = k\mathbf{v}$, $k \in V$,
è un sottogruppo di V. V F

Gruppi finiti

16 Sia G = {1; *a*; *b*; *c*; *d*} un insieme formato da 5 elementi: determinare su di esso un'operazione di moltiplicazione per la quale l'elemento 1 abbia il ruolo di elemento neutro e che renda G gruppo.

17 Quali sottogruppi può avere il gruppo dell'esercizio precedente?

18 Sia E = {[0]; [1]; [2]; [3]; [4]} l'insieme delle classi resto modulo 5 dotate dell'ordinaria moltiplicazione:

a) determinare gli inversi degli elementi [2], [3], [4];
b) decidere se E costituisce gruppo.

a) [*Costruita la tabella moltiplicativa riportata a fianco, si osserva che la classe* [*1*] *è l'elemento neutro, l'inversa della classe* [*2*] *è la classe* [*3*]...]

•	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

19 Sia G = {[0]; [1]; [2]; [3]} l'insieme delle classi resto modulo 4 dotato dell'ordinaria addizione:

a) determinare gli inversi degli elementi [2], [3];
b) decidere se G costituisce gruppo.

20 Sia G l'insieme delle trasformazioni di un quadrato in sé ottenibili componendo le simmetrie rispetto agli assi dei lati:

a) determinare il numero di elementi di G;
b) riconoscere che G forma gruppo.

21 Sia G il gruppo delle rotazioni di angoli multipli di 30°:

a) determinare tutti gli elementi e la tabella di composizione di G;
b) determinare i sottogruppi di G.

22 Sia G l'insieme delle trasformazioni biunivoche dell'insieme E = {1, 2, 3} di tre elementi in sé:

a) determinare il numero di elementi di G;
b) riconoscere che l'ordinaria composizione di due trasformazioni rende *G* gruppo;
c) determinare i sottogruppi di G.

23 Sia G l'insieme delle trasformazioni di un triangolo equilatero in sé ottenibili componendo le simmetrie rispetto agli assi dei lati:

a) determinare il numero di elementi di G;
b) riconoscere che G forma gruppo.

24 Sia G l'insieme delle trasformazioni di un quadrato in sé ottenibili componendo le simmetrie rispetto alle diagonali e quelle rispetto agli assi dei lati:

a) determinare tutti gli elementi di G;
b) riconoscere che G forma gruppo e determinarne la tabella di composizione.

25 Sia G l'insieme delle rotazioni di angoli multipli interi di 100°:

a) determinare il numero di elementi di G;
b) riconoscere che G forma gruppo.

esercizi

26 Sia G l'insieme delle classi resto modulo 12 composte con l'ordinaria addizione:

a) riconoscere che forma gruppo;
b) determinare il sottogruppo contenente l'elemento [2];
c) determinare il sottogruppo contenente l'elemento [5].

Anelli

Quesiti

1. Si dia la definizione di *anello* e si forniscano esempi di anelli dotati o meno dell'elemento neutro.

2. Gli insiemi dei numeri pari e quello dei dispari strutturati con le usuali operazioni di somma e prodotto sono anelli?

3. L'insieme dei multipli di un intero $p \geq 2$ è un anello rispetto alle operazioni di somma e di prodotto? Giustificare la risposta.

27 Sia G un gruppo rispetto all'operazione +; indichiamo con 0 l'elemento neutro.
Definiamo su G la legge moltiplicativa seguente:

$$a \times b = 0 \qquad \forall\, a, b \in \mathrm{G}$$

Dimostrare che G è un anello rispetto alle operazioni + e $\times$.

28 Detto S l'insieme delle coppie $(x; y)$, con $x, y \in \mathbb{Z}$, definiamo in S le leggi:

$$(x; y) + (x'; y') = (x + x'; y + y')$$
$$(x; y) * (x'; y') = (xx'; xy' + yx')$$

Dimostrare che S è un anello commutativo unitario.
Dimostrare che il sottoinsieme $\mathrm{T} \subset \mathrm{S}$ sostituito dalle coppie $(x; 0)$ è ancora un anello rispetto alle due leggi + e $*$.

Corpi. Campi

Quesiti

1. Si dia la definizione di *corpo* e di *campo* e si forniscano esempi.

2. L'insieme delle classi resto modulo 7 è un campo. Giustificare l'affermazione e, dopo aver scritto la tabella moltiplicativa, determinare l'inversa della classe [5].

29 Sia A l'insieme delle quaterne ordinate di numeri reali:

$$\mathrm{A} = \{a_0; a_1; a_2; a_3\}$$

Definiamo in A una addizione + e una moltiplicazione $\cdot$ nel modo seguente:

$$(a_0; a_1; a_2; a_3) + (b_0; b_1; b_2; b_3) = (a_0 + b_0; a_1 + b_1; a_2 + b_2; a_3 + b_3)$$
$$(a_0; a_1; a_2; a_3) \cdot (b_0; b_1; b_2; b_3) = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3; a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2;$$
$$a_0b_2 + a_2b_0 + a_3b_1 - a_1b_3; a_0b_3 + a_3b_0 + a_1b_2 - a_2b_1)$$

L'insieme (A, +, $\cdot$) può essere indicato con il simbolo:

$$a_0 + a_1 i + a_2 j + a_3 k$$

essendo $a_0, a_1, a_2, a_3 \in \mathbb{R}$ e per convenzione:

$$i^2 = j^2 = k^2 = -1 \qquad ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j$$

Dimostrare che l'insieme (A, +, $\cdot$) è un corpo (non è un campo poiché il prodotto non è commutativo).
L'insieme (A, +, $\cdot$) prende il nome di *corpo dei quaternioni*.

Spazi vettoriali

Quesiti

1. Si dia la definizione di *spazio vettoriale* e si forniscano esempi.

2. Si consideri l'insieme A dei numeri reali positivi in cui come legge di composizione interna si consideri il prodotto tra numeri reali e come legge esterna di $x \in$ A per un numero reale k la potenza x^k. L'insieme A è uno spazio vettoriale?

3. Si consideri l'insieme P[x] di tutti i polinomi a coefficienti in $\mathbb{R}$ considerando come legge di composizione interna la somma tra polinomi e come legge esterna il prodotto per un numero reale. P[x] è uno spazio vettoriale?
Esistono n polinomi linearmente indipendenti mediante i quali rappresentare un polinomio qualunque?

30 Dimostrare che, se A e B sono sottospazi vettoriali dello spazio vettoriale V, allora anche $A \cap B$ è un sottospazio vettoriale di V.

31 Determinare l'intersezione di tutti i sottospazi vettoriali di uno spazio vettoriale V.

l'insieme costituito dal solo vettore nullo di V.

32 Dimostrare che l'insieme $\mathbb{Q}$ dei numeri razionali, munito della somma e del prodotto per un numero reale, non è uno spazio vettoriale.

se $a \in \mathbb{Q}$, per esempio, il prodotto $\sqrt{3} \cdot a \notin \mathbb{Q}$

33 Dimostrare che l'insieme delle terne $(x; y; 0)$, aventi l'ultima componente nulla, è un sottospazio vettoriale di $\mathbb{R}^3$.

34 Dimostrare che l'insieme delle coppie $(x; y)$ che verificano ciascuna delle seguenti relazioni:

a) $x + y = 0$ *b*) $x - 2y = 0$ *c*) $3x + y = 0$ *d*) $x^2 + y^2 = 0$ *e*) $2x^2 + 3y^2 = 0$

costituisce un sottospazio vettoriale di $\mathbb{R}^2$.

35 Dimostrare che l'insieme delle coppie $(x; y)$ che verificano ciascuna delle seguenti relazioni:

a) $x^2 - y^2 = 0$ *b*) $x - y < 0$ *c*) $xy = 0$ *d*) $xy > 0$ *e*) $x - 2y + 3 = 0$

non è un sottospazio vettoriale di $\mathbb{R}^2$.

36 Dimostrare che l'insieme delle terne $(x; y; z)$ che verificano ciascuna delle seguenti relazioni:

a) $x + y + z = 0$ *b*) $2x - y - 3z = 0$ *c*) $x^2 + y^2 + z^2 = 0$

costituisce un sottospazio vettoriale di $\mathbb{R}^3$.

37 Dimostrare che l'insieme delle terne $(x; y; z)$ che verificano ciascuna delle seguenti relazioni:

a) $x + y + z + 1 = 0$ *b*) $xyz < 0$ *c*) $x^2 - y^2 + z^2 = 0$

non è un sottospazio vettoriale di $\mathbb{R}^3$.

Vero o falso?

1. L'insieme dei reali è uno spazio vettoriale sui reali stessi. V F

2. La dimensione dello spazio vettoriale dei numeri reali è uguale a 1. V F

3. L'insieme $\mathbb{R}^2$ delle coppie $(a; b)$ di numeri reali sul campo $\mathbb{C}$ dei numeri complessi è uno spazio vettoriale. V F

Sia F l'insieme delle funzioni reali di variabile reale in cui sia definita come legge di composizione interna la somma di funzioni e come legge esterna il prodotto per un numero reale. Allora:

4. F è uno spazio vettoriale. V F

5. il sottoinsieme delle funzioni f tali che $f(0) = 0$ è un sottospazio vettoriale. V F

6. il sottoinsieme delle funzioni pari è uno sottospazio vettoriale. V F

Soluzioni

Quesiti di verifica, p. 24
1. d – **2.** a – **3.** c – **4.** a – **5.** b – **6.** d – **7.** a – **8.** c – **9.** d

Vero o falso?, p. 32
1. F: $a^b \neq b^a$ – **2.** F: infatti $3 \otimes 5 = 14 \neq 5 \otimes 3 = 28$ – **3.** F: infatti, $(a \otimes b) \otimes c = (a^2 + b) \otimes c = (a^2 +$ mentre $a \otimes (b \otimes c) = a^2 + (b \otimes c) = a^2 +$ – **4.** F: se a, b, c sono tre numeri reali risulta: $(a^b)^c \neq a^b$ – **5.** V

Quesiti, p. 32
2. $-x - iy$ – **6.** $(f_m)^{-1} = f_{1/m}$

Quesiti, p. 33
1. 240°

Vero o falso?, p. 33
1. F, non esiste l'elemento neutro – **2.** F, il prodotto scalare tra due vettori non è un vettore – **3.** V – **4.** V – **5.** F, la composizione di due rotazioni è o una rotazione o una traslazione – **6.**V – **7.** V, F – **8.** V

Quesiti, p. 35
2. [3]

Vero o falso?, p. 35
1. V – **2.** V – **3.** F – **4.** V – **5.** V – **6.** V