Strutture algebriche "rare"

di Antonino Giambò

1. I miei contributi a *Matmedia* sono rivolti solitamente agli studenti delle scuole secondarie di 2° grado e, in particolare, a quelli di loro che intendono intraprendere studi universitari nei quali la Matematica è disciplina caratterizzante o almeno fondamentale.

Questo articolo, pur affrontando argomenti che esulano dai curricoli scolastici, rientra ugualmente in quella categoria, anche se gli argomenti qui trattati sono oggetto di studio solamente nei corsi di laurea in Matematica.

Ritengo in ogni caso che non faccia male alla salute se qualche studente ne prende conoscenza, anche se non si laureerà in Matematica.

Ora, siccome l'articolo si occupa di "strutture algebriche", è necessario chiarire anzitutto di cosa andiamo a parlare. Lo faccio – e spero senza offesa alcuna per coloro che queste cose già sanno – in modo spicciativo per affrontare poi nella seconda parte la questione che giustifica il titolo di questo contributo.

2. Com'è noto, l'addizione e la moltiplicazione sono operazioni definite nell'insieme dei numeri naturali, nel senso che si ottengono ancora numeri naturali addizionando o moltiplicando due numeri naturali qualsiasi.

In generale, si denomina **operazione (binaria) definita** in un dato insieme A una relazione che ad ogni coppia ordinata di elementi di A associa uno ed un solo elemento di A. Si denomina anche **legge di composizione interna** ad A o **operazione interna** ad A.

L'elemento associato ai due elementi dati è detto il *risultato* dell'operazione e, in base alla medesima definizione di operazione, esso è unico. Gli elementi della coppia si dicono *termini* dell'operazione.

Per denotare un'operazione si usano, oltre ai simboli consueti $+$, $\cdot$, $-$, $:$, vari altri simboli come per esempio i seguenti:

$$\ast \quad \circ \quad \perp \quad \oplus \quad \otimes \quad \text{ed altri ancora}$$

e per indicare che alla coppia ordinata $(x, y) \in A^2$ l'operazione "$\ast$" associa $z \in A$ si scrive: $x \ast y = z$ e, se l'operazione è un'operazione generica non meglio identificata, si legge: « x composto con y è uguale a z ».

S'intende che, se l'operazione è accertata, come per esempio l'operazione "+" di addizione, allora si scrive $x+y=z$ e si legge « x più y è uguale a z ». Ugualmente in altri casi analoghi.

L'insieme A, nel quale è definita una determinata operazione, si dice ***chiuso*** rispetto a quell'operazione.

Per esempio, l'insieme $\mathbb{Q}$ dei razionali è chiuso rispetto all'addizione, ma non lo è rispetto alla divisione, per la presenza del numero 0, mentre lo diventa se si considera l'insieme $\mathbb{Q}_0 = \mathbb{Q} - \{0\}$.

Un'operazione, definita in un dato insieme, può godere di importanti proprietà. Le andiamo a descrivere.

- L'operazione "$\perp$", definita nell'insieme A, si dice **commutativa** (o che **gode della proprietà commutativa**) se, comunque si prendano $x, y \in A$, risulta:
$$x \perp y = y \perp x\,.$$
L'insieme, in tal caso, si dice *commutativo* o *abeliano* [(1)] rispetto a quell'operazione.
Si possono fornire numerosi esempi di insiemi commutativi rispetto ad un'operazione definita in essi.
- L'operazione "$\perp$", definita nell'insieme A, si dice **associativa** (o che **gode della proprietà associativa**) se, comunque si prendano $x, y, z \in A$, risulta:
$$(x \perp y) \perp z = x \perp (y \perp z)\,.$$
Anche adesso è possibile fornire esempi di insiemi in cui un'operazione definita è associativa.
- Un insieme A, in cui è definita l'operazione "$\perp$" si dice dotato di **elemento neutro** (o **elemento indifferente**) rispetto a quell'operazione se, indicato con u tale elemento e preso un qualsiasi elemento $x \in A$, risulta:
$$x \perp u = u \perp x = x\,.$$
Un esempio banale: nell'insieme $\mathbb{N}$ dei numeri naturali, 0 è elemento neutro rispetto all'addizione, mentre 1 lo è rispetto alla moltiplicazione.

---

1 Da **Abel**, Niels Henrik, geniale quanto sfortunato matematico norvegese, 1802-1829.

Si dimostra che l'elemento neutro di un insieme, rispetto ad una determinata operazione, se esiste, è unico.

- Dato un insieme A dotato di elemento neutro u rispetto all'operazione "⊥", definita in A, può accadere che, preso un elemento $x \in A$, esista $x' \in A$ tale che:

$$x \perp x' = x' \perp x = u\,.$$

  Se questo accade, gli elementi x ed x' si dicono l'uno **simmetrico** (o **inverso**) dell'altro rispetto a "⊥", e ciascuno di essi si dice ***simmetrizzabile*** (o ***invertibile***) rispetto all'operazione "⊥".
  Per esempio, ogni elemento α dell'insieme $\mathbb{Z}$ degli interi relativi ammette il simmetrico $-\alpha$ rispetto all'addizione. Più propriamente, questo simmetrico di α è denominato *opposto* di α.
- In un insieme A siano definite due operazioni "⊕" e "⊙", che si leggono rispettivamente "più cerchiato" e "punto cerchiato". Presi tre qualsiasi elementi $x, y, z \in A$, si dice che è:
  - ⊙ **distributiva a sinistra** rispetto a "⊕" se risulta: $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$;
  - ⊙ **distributiva a destra** rispetto a "⊕" se risulta: $(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$;
  - ⊙ **distributiva** rispetto a "⊕" se lo è sia a destra sia a sinistra.

  Per esempio:
  - nell'insieme $\mathbb{Q}$ dei razionali la moltiplicazione è distributiva rispetto all'addizione, mentre l'addizione non lo è rispetto alla moltiplicazione, né a destra né a sinistra;
  - nell'insieme $\mathbb{Q}_0$ dei razionali non nulli, la divisione è distributiva a destra rispetto all'addizione ma non lo è a sinistra.

3. Quando in un insieme A sono definite una o più operazioni interne si dice che l'insieme è *strutturato* (o che è *dotato di struttura*) e l'insieme, preso assieme alla sua operazione interna (o alle sue operazioni interne), si dice che è una **struttura algebrica**. L'insieme è chiamato ***sostegno*** della struttura. La struttura algebrica avente per sostegno l'insieme A ed operazione interna "⊥" si rappresenta con la coppia ordinata $(A, \perp)$.

Una struttura algebrica assume nomi diversi a seconda che si consideri rispetto ad una sola operazione o a due operazioni ed a seconda delle proprietà di cui godono le operazioni medesime. Noi fermeremo la nostra attenzione sulle seguenti strutture algebriche: semigruppo, monoide, gruppo, anello, corpo, campo. Che però, occorre precisarlo, non sono le uniche strutture algebriche.

- Un **semigruppo** è una struttura algebrica con una sola operazione interna che sia *associativa*.
- Un **monoide** è un semigruppo dotato di *elemento neutro*.
- Un **gruppo** è un monoide nel quale ogni elemento è *simmetrizzabile* rispetto all'operazione che lo caratterizza.

Se l'operazione è l'addizione il gruppo si dice *additivo*, se è la moltiplicazione si dice *moltiplicativo*.
Se poi l'operazione è anche commutativa il semigruppo o il monoide o il gruppo si dicono *abeliani* (o *commutativi*).

- Un **anello** è una struttura algebrica con due operazioni interne, rappresentato dalla terna ordinata $(A, \perp, \ast)$, tale che:
  - la struttura $(A, \perp)$ è un *gruppo abeliano*;
  - la struttura $(A, \ast)$ è un *semigruppo*;
  - la seconda operazione "⁎" è *distributiva* rispetto alla prima ⊥.

Se poi anche la seconda operazione " ⁎ " è *commutativa*, l'anello si dice *abeliano* (o *commutativo*).
Se inoltre esiste in A l'elemento neutro rispetto alla seconda operazione, vale a dire se la struttura $(A, \ast)$ è un *monoide*, allora l'anello si denomina *anello unitario* (o *anello dotato di unità*).

- Un **corpo** è una struttura algebrica con due operazioni interne $(A, \perp, \ast)$ tale che:
  - la struttura $(A, \perp)$ è un *gruppo abeliano*; sia u l'elemento neutro;
  - la struttura algebrica $(A_u, \ast)$ è un *gruppo*, essendo $A_u = A - \{u\}$;
  - la seconda operazione "⁎" è d*istribuita* rispetto alla prima "⊥".

Se poi anche la seconda operazione " $*$ " è commutativa, il corpo si dice *abeliano* (o *commutativo*). Un corpo commutativo è chiamato anche **campo**.

Nel caso del corpo, ci si potrebbe domandare legittimamente perché è necessario prendere l'insieme A_u privato dell'elemento neutro u rispetto alla prima operazione. Il fatto è che quell'elemento, composto sia a destra sia a sinistra con un qualsiasi elemento dell'insieme sostegno per mezzo della seconda operazione "$*$", riproduce lo stesso elemento neutro. Insomma, l'elemento u è tale che, per ogni $x \in A$, risulta: $x * u = u * x = u$. E, per questo, u non è simmetrizzabile rispetto all'operazione "$*$".Si dice che l'elemento u è *elemento assorbente* (o *elemento nullifico*) rispetto all'operazione "$*$".

Prima di fornire qualche esempio, ritengo opportuna una precisazione. A rigore di logica, un gruppo è anche un monoide, così come un corpo è anche un anello. Tuttavia, quando, negli esempi che vado a riportare, si parla di monoide lo si intende in senso stretto, nel senso cioè che la struttura che stiamo considerando non è un gruppo. Parimenti quando si parla di anello, s'intende che non è un corpo. E ugualmente quando diciamo che è un semigruppo intendiamo che non è un monoide.

Ciò detto, passiamo ad alcuni esempi. Chi legge, se ne ha voglia, può verificare:

- l'operazione "$*$" che ad ogni coppia di numeri razionali associa la loro media aritmetica, vale a dire l'operazione tale che:
$$a * b = \frac{a+b}{2}\ ,\quad \text{con } a, b \in \mathbb{Q}\ ,$$
è un'operazione interna all'insieme $\mathbb{Q}$ dei numeri razionali, ma non è associativa e non ha l'elemento neutro; questo significa che la struttura algebrica $(\mathbb{Q}, *)$ non è neppure un semigruppo; alcuni definiscono *gruppoide* o *magma* una struttura siffatta;
- è invece un modello di *semigruppo* la struttura $(\mathbb{N}, *)$, dove $\mathbb{N}$ è l'insieme dei numeri naturali e "$*$" è la legge di composizione definita dalla seguente relazione: $a * b = \max(a, b)$, cioè: $a * b$ è il valore massimo fra a e b;
- le strutture $(\mathbb{N}, +)$ e $(\mathbb{N}, \cdot)$ sono modelli di *monoidi*;
- le strutture $(\mathbb{Z}, +)$ e $(\mathbb{Z}, \cdot)$, dove $\mathbb{Z}$ è l'insieme degli interi, sono nell'ordine un *gruppo additivo* e un *monoide*;
- le strutture $(\mathbb{Q}, +)$ e $(\mathbb{Q}_0, \cdot)$, dove $\mathbb{Q}$ è l'insieme dei numeri razionali e $\mathbb{Q}_0$ è l'insieme $\mathbb{Q} - \{0\}$, sono modelli di *gruppo*, *additivo* il primo, *moltiplicativo* il secondo;
- parimenti, sono modelli di *gruppo*, *additivo* il primo e *moltiplicativo* il secondo, le strutture $(\mathbb{R}, +)$ e $(\mathbb{R}_0, \cdot)$, dove $\mathbb{R}$ è l'insieme dei numeri reali e $\mathbb{R}_0$ è l'insieme $\mathbb{R} - \{0\}$;
- sono ancora modelli di *gruppo* le strutture $(T, \circ)$ e $(R, \circ)$, dove T è l'insieme delle **traslazioni piane** ed R quello delle **rotazioni piane di dato centro**, mentre "$\circ$" è la legge di composizione di due trasformazioni geometriche;
- un modello di *anello unitario* è l'*anello degli interi* $(\mathbb{Z}, +, \cdot)$;
- se indichiamo con $2\mathbb{Z}$ l'insieme degli interi pari, la struttura $(2\mathbb{Z}, +, \cdot)$ è un *anello*, ma non unitario;
- indicato con $\mathbb{Z}[x]$ l'insieme dei polinomi nell'indeterminata x, con coefficienti in $\mathbb{Z}$, la struttura algebrica $(\mathbb{Z}[x], +, \cdot)$ è ancora un modello di *anello unitario*: è denominato *anello dei polinomi* nell'indeterminata x con coefficienti in $\mathbb{Z}$;
- tra i modelli di *campo* ricordiamo il *campo razionale* $(\mathbb{Q}, +, \cdot)$, il *campo reale* $(\mathbb{R}, +, \cdot)$ e il *campo complesso* $(\mathbb{C}, +, \cdot)$.

4. Un cenno adesso ad alcune strutture speciali.

- Nell'insieme $Z_3 = \{0, 1, 2\}$ sono definite le operazioni "$\oplus$" e "$\odot$" tali che $x \oplus y = r_1$ e $x \odot y = r_2$, dove r_1 e r_2 sono i resti della **divisione per 3** dei numeri rispettivamente x+y e $x \cdot y$.
  Ebbene, le strutture $(Z_3, \oplus)$, $(Z_3, \odot)$, $(Z_3, \oplus, \odot)$ sono, nell'ordine, un *gruppo*, un *monoide*, un *campo*. Chi legge può verificarlo, se ne ha voglia, e al riguardo possono far comodo le tabelle di composizione.

- Nell'insieme $Z_4 = \{0, 1, 2, 3\}$ sono definite le operazioni "$\oplus$" e "$\odot$" tali che $x \oplus y = r_1$ e $x \odot y = r_2$, dove r_1 e r_2 sono i resti della **divisione per 4** dei numeri rispettivamente x+y e $x \cdot y$.

  Ebbene, le strutture $(Z_4,\ \oplus)$, $(Z_4,\ \odot)$, $(Z_4,\ \oplus,\ \odot)$ sono, nell'ordine, un *gruppo*, un *monoide*, un *anello unitario*.

  Come sopra per una possibile ed eventuale verifica e per capire anche perché la struttura $(Z_3,\ \oplus,\ \odot)$ è un campo mentre la struttura $(Z_4,\ \oplus,\ \odot)$ è invece un anello unitario, ma non un campo.

5. Se si esaminano i vari modelli di semigruppo, monoide, gruppo, anello e corpo, che ho elencato nelle righe precedenti, si constata una circostanza interessante: sono tutti modelli di *strutture commutative*. E l'elenco potrebbe continuare. Nessun esempio è stato fornito di struttura non commutativa.

Ora, mentre è ancora abbastanza semplice fornire qualche esempio di gruppo non commutativo, non è semplicissimo trovare modelli di semigruppo o monoide o anello o corpo non commutativi.

Ci soffermiamo perciò su questa ricerca, che giustifica per l'appunto il titolo di questo contributo.

- Incominciamo con qualche esempio di gruppo non commutativo:
  - Un modello di *gruppo non commutativo* è costituito dalla struttura $(A, *)$ dove A è il seguente insieme:
  $$A = \left\{ a,\ \frac{1}{a},\ 1-a,\ \frac{1}{1-a},\ \frac{a-1}{a},\ \frac{a}{a-1} \right\},$$
  essendo a un qualsiasi numero reale diverso da 0 e da 1 ed essendo " $*$ " l'operazione tale che $x * y$, con $x, y \in A$, rappresenti l'espressione che si ottiene sostituendo al posto della lettera a, che figura in x, l'espressione rappresentata da y. Così, per esempio:
  $$\frac{1}{a} * \frac{1}{1-a} = \frac{1}{\frac{1}{1-a}},\ \text{ perciò: } \frac{1}{a} * \frac{1}{1-a} = 1-a\,.$$
  La *tabella di composizione* (tabella 1) mostra che l'insieme A, è chiuso rispetto all'operazione " $*$ ", che esiste l'elemento neutro, che ogni elemento è simmetrizzabile e che l'operazione non è commutativa. Che l'operazione sia associativa lo si può provare o accettarlo sulla fiducia.

$*$	a	$\frac{1}{a}$	$1-a$	$\frac{1}{1-a}$	$\frac{a-1}{a}$	$\frac{a}{a-1}$
a	a	$\frac{1}{a}$	$1-a$	$\frac{1}{1-a}$	$\frac{a-1}{a}$	$\frac{a}{a-1}$
$\frac{1}{a}$	$\frac{1}{a}$	a	$\frac{1}{1-a}$	$1-a$	$\frac{a}{a-1}$	$\frac{a-1}{a}$
$1-a$	$1-a$	$\frac{a-1}{a}$	a	$\frac{a}{a-1}$	$\frac{1}{a}$	$\frac{1}{1-a}$
$\frac{1}{1-a}$	$\frac{1}{1-a}$	$\frac{a}{a-1}$	$\frac{1}{a}$	$\frac{a-1}{a}$	a	$1-a$
$\frac{a-1}{a}$	$\frac{a-1}{a}$	$1-a$	$\frac{a}{a-1}$	a	$\frac{1}{1-a}$	$\frac{1}{a}$
$\frac{a}{a-1}$	$\frac{a}{a-1}$	$\frac{1}{1-a}$	$\frac{a-1}{a}$	$\frac{1}{a}$	$1-a$	a

tabella 1

  - Un altro modello di *gruppo non commutativo* è costituito dalla struttura $(\mathrm{D}, \circledast)$, dove D è il seguente insieme di coppie ordinate:
  $$\mathrm{D} = \{(0,0), (1,0), (2,0), (0,1), (1,1), (2,1)\},$$
  mentre "$\circledast$" è l'operazione così definita:
  $$(\mathrm{a}, 0) * (\mathrm{b}, \mathrm{c}) = (\mathrm{r}, \mathrm{c}),\quad (\mathrm{a}, 1) * (\mathrm{b}, \mathrm{c}) = (\mathrm{s}, \mathrm{d}),$$
  essendo r il resto della divisione per 3 del numero a+b; s il resto della divisione per 3 del numero a – b se a – b ≥ 0, di a – b+3 se a – b <0; d il resto della divisione per 2 del numero 1+c.

La *tabella di composizione* (tabella 2) mostra che l'insieme D, è chiuso rispetto all'operazione " $*$ ", che esiste l'elemento neutro, che ogni elemento è simmetrizzabile e che l'operazione non è commutativa. Che l'operazione sia associativa lo si può provare.
Si tratta di un gruppo artificioso, ne convengo, ma comunque è un esempio di gruppo non commutativo.

$*$	**(0,0)**	**(1,0)**	**(2,0)**	**(0,1)**	**(1,1)**	**(2,1)**
(0,0)	(0,0)	(1,0)	(2,0)	(0,1)	(1,1)	(2,1)
(1,0)	(1,0)	(2,0)	(0,0)	(1,1)	(2,1)	(0,1)
(2,0)	(2,0)	(0,0)	(1,0)	(2,1)	(0,1)	(1,1)
(0,1)	(0,1)	(2,1)	(1,1)	(0,0)	(2,0)	(1,0)
(1,1)	(1,1)	(0,1)	(2,1)	(1,0)	(0,0)	(2,0)
(2,1)	(2,1)	(1,1)	(0,1)	(2,0)	(1,0)	(0,0)

Tabella 2

- Sono modelli di *gruppo non commutativo* le seguenti strutture algebriche: $(I, \circ)$, dove I è l'insieme delle **isometrie piane;** $(S, \circ)$, dove S è l'insieme delle **similitudini piane**; $(A, \circ)$, dove A è l'insieme delle **affinità piane.** L'operazione "∘" è la legge di composizione di due trasformazioni geometriche.
- L'insieme dei **movimenti che mutano un triangolo equilatero** in sé (o, più in generale, un poligono regolare in sé), strutturato con la legge di composizione di due movimenti, è un modello di *gruppo non commutativo.*

- Occupiamoci adesso di altre strutture non commutative.

Un modello di *semigruppo non commutativo* è fornito dalla struttura $(\mathbb{Z},\ \circledast)$, dove "⊛" è l'operazione tale che $a * b = |a| \cdot b$.

Al fine di trovare modelli di monoide, anello o corpo non commutativi, consideriamo l'insieme M delle matrici quadrate del 2° ordine, con coefficienti nell'insieme $\mathbb{Q}$ dei razionali, strutturato con le due operazioni "somma" (simbolo +) e "prodotto" (simbolo ×) [2].

Ebbene, si verifica che le strutture algebriche (M, +), (M, ×) e (M, +, ×) sono, nell'ordine, un gruppo commutativo, un *monoide non commutativo* e un *anello unitario non commutativo.*

Verifiche che lascio a chi legge queste righe, se ne ha voglia, limitandomi a fornire qualche semplice ragguaglio. Come, per esempio, il fatto che l'elemento neutro rispetto a "+" e l'elemento nutro rispetto a "×" sono rispettivamente le cosiddette *matrice nulla* e *matrice unità*, ossia: $\begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix}$ e $\begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}$ e che la matrice simmetrica della matrice $\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$ è la cosiddetta *matrice opposta* $\begin{Vmatrix} -a & -b \\ -c & -d \end{Vmatrix}$.

Faccio poi notare che la struttura $(M_p, \times)$ è un modello di *semigruppo non commutativo* se M_p è l'insieme delle matrici quadrate di ordine 2, i cui elementi siano però numeri interi pari. E anche la verifica di questo lascio a chi legge.

Ma, ritornando alla struttura (M, +, ×), ci chiediamo: è forse un corpo?

Affinché lo sia, dovrebbe esistere di ogni matrice non nulla la matrice simmetrica rispetto all'operazione "×". Vale a dire che, presa una qualsiasi matrice non nulla $\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$, dovrebbe esistere la matrice $\begin{Vmatrix} x & y \\ z & t \end{Vmatrix}$ tale che risulti:

$$\begin{Vmatrix} a & b \\ c & d \end{Vmatrix} \times \begin{Vmatrix} x & y \\ z & t \end{Vmatrix} = \begin{Vmatrix} x & y \\ z & t \end{Vmatrix} \times \begin{Vmatrix} a & b \\ c & d \end{Vmatrix} = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}$$

2 Ho fatto un cenno ad alcune di queste strutture, come anche alla seguente, relativa ai quaternioni, in un articolo, dal titolo *Ancora sui Quaternion*i, pubblicato qualche tempo fa su questa medesima rubrica.

Poiché:

$$\begin{Vmatrix} a & b \\ c & d \end{Vmatrix} \times \begin{Vmatrix} x & y \\ z & t \end{Vmatrix} = \begin{Vmatrix} a\,x+b\,z & a\,y+b\,t \\ c\,x+d\,z & c\,y+d\,t \end{Vmatrix} \quad \text{e} \quad \begin{Vmatrix} x & y \\ z & t \end{Vmatrix} \times \begin{Vmatrix} a & b \\ c & d \end{Vmatrix} = \begin{Vmatrix} x\,a+y\,c & x\,b+y\,d \\ z\,a+t\,c & z\,b+t\,d \end{Vmatrix}$$

dovrebbe dunque risultare contemporaneamente:

$$\{a\,x + b\,z = 1,\ \ a\,y + b\,t = 0,\ \ c\,x + d\,z = 0\,,\ \ c\,y + d\,t = 1\,\}$$

e la soluzione di questo sistema nelle incognite x, y, z, t dovrebbe soddisfare il seguente sistema nelle medesime indeterminate:

$$\{x\,a + y\,c = 1,\ \ x\,b + y\,d = 0,\ \ z\,a + t\,c = 0\,,\ \ z\,b + t\,d = 1\,\}.$$

Ora, il primo sistema ammette soluzione (una ed una soltanto) se e solo se risulta $\Delta = a\,d - b\,c \neq 0$, vale a dire se il determinante Δ della matrice è diverso da 0, e sotto questa condizione la soluzione è la seguente:

$$x = \frac{d}{\Delta}\,,\ \ y = -\frac{b}{\Delta}\,,\ \ z = -\frac{c}{\Delta}\,,\ \ t = \frac{a}{\Delta}.$$

E questa quaterna soddisfa anche il secondo sistema, come si può verificare.

Pertanto, solamente sotto la condizione che sia $\Delta = a\,d - b\,c \neq 0$, ogni matrice $\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$ ammette la matrice simmetrica rispetto all'operazione "×", matrice che è denominata più propriamente *matrice inversa*. Sotto questa condizione, la matrice $\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$ si dice *regolare*.

Indicato allora con M_r *l'insieme delle matrici regolari* del 2° ordine e controllato che è chiuso rispetto alle solite operazioni "+" e "×", si può concludere che la struttura algebrica (M_r, +, ×) è un modello di *corpo non commutativo.*

Il discorso fatto per le matrici quadrate del 2° ordine vale, tale e quale, per le matrici quadrate di un qualsiasi ordine n e con coefficienti non solo in $\mathbb{Q}$ ma anche nell'insieme $\mathbb{R}$ dei numeri reali o nell'insieme $\mathbb{C}$ dei numeri complessi.

Vale a dire che, se M è una matrice quadrata di ordine n (con coefficienti in $\mathbb{Q}$ o in $\mathbb{R}$ o in $\mathbb{C}$), allora le strutture algebriche (M, +), (M, ×) e (M, +, ×) sono, nell'ordine, un gruppo commutativo, un *monoide non commutativo* e un *anello unitario non commutativo*.

Si osserva che, se M_p è una matrice quadrata di ordine n, i cui elementi sono però numeri interi pari, allora la struttura (M_p, ×) è un *semigruppo non commutativo*.

Se infine si considera l'insieme M_r delle matrici regolari (con coefficienti in $\mathbb{Q}$ o in $\mathbb{R}$ o in $\mathbb{C}$), ossia l'insieme di quelle matrici il cui determinante è non nullo, allora la struttura (M_r, +, ×) è un *corpo non commutativo*.

Altri modelli di strutture non commutative si ottengono prendendo in considerazione i cosiddetti *quaternioni di Hamilton* [3]. Ho avuto modo di farne qualche cenno, come ho già detto, ma preferisco riprenderli.

Ebbene, per comprendere di cosa si tratti, generalizziamo il concetto di numero complesso e consideriamo al riguardo gli enti **i, j, k** per i quali vale l'operazione "•" di moltiplicazione, come definita nella sottostante tabella (tabella 2).

•	1	**i**	**j**	**k**
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

tabella 2

3 **Hamilton**, William Rowan, astronomo e matematico tedesco, 1821-1881.

Cosicché risulta: $i \bullet j = k$, $j \bullet i = -k$, $i \bullet k = -j$, $k \bullet i = j$, $j \bullet k = i$, $k \bullet j = -i$; inoltre: $i^2=j^2=k^2=-1$

Si chiama *quaternione di Hamilton* (con componenti razionali) ogni entità del tipo:

$$a + b\,i + c\,j + d\,k$$

dove $a, b, c, d \in \mathbb{Q}$, mentre i, j, k sono enti che si comportano come descritto sopra.

I numeri a, b, c, d sono denominati componenti del quaternione. Il quaternione di componenti a, b, c, d è indicato anche con la quaterna ordinata (a, b, c, d).

Nell'insieme H dei quaternioni di Hamilton si possono definire due operazioni: *somma* (simbolo +) e *prodotto* (simbolo ·), i cui risultati si ottengono considerando i loro termini come polinomi di 1° grado nelle indeterminate i, j, k con coefficienti in $\mathbb{Q}$ e operando con essi con le ordinarie addizione e moltiplicazione, ma con l'accorgimento di sostituire ai prodotti $i \bullet i$, $i \bullet j$, $i \bullet k$, ecc., i risultati esplicitati dalla tabella 2.

L'elemento neutro rispetto all'operazione "+" è il *quaternione nullo* $(0, 0, 0, 0)$; l'elemento neutro rispetto all'operazione "·" è il *quaternione unità* $(1, 0, 0, 0)$.

Orbene, indicato con H_0 l'insieme H privato del quaternione nullo, si dimostra che la struttura $(H_0, \bullet)$ è un *gruppo non commutativo*, mentre la struttura $(H, +, \bullet)$ è un *corpo non commutativo*.

Si ottengono ancora modelli di *gruppo non commutativo* e di *corpo non commutativo* se i quaternioni sono presi con componenti in $\mathbb{R}$.

6. Trovare altri modelli di semigruppo, monoide, gruppo, anello o corpo non commutativi non è semplice.

In particolare, non lo è per gli anelli, almeno se se ne cercano di accessibili a studenti liceali. Il che, in effetti, è paradossale poiché i matematici hanno dimostrato che la famiglia degli anelli non commutativi è più ampia di quella degli anelli commutativi.

Ma qui stiamo entrando in un campo troppo specialistico per poterne parlare in un articolo rivolto prevalentemente a studenti delle scuole superiori, per cui la chiudo qui, lasciando ai futuri laureandi in Matematica i necessari approfondimenti.

BIBLIOGRAFIA.

[1] Antonino Giambò, *La prova di matematica nei concorsi di scuola media*, Torino, SEI, 1988.

[2] Antonino Giambò – Roberto Giambò, *Matematica pre-universitaria, Storia e didattica*, Bologna, Pitagora, 2005.

[3] AA.VV., *Tendenze attuali dell'insegnamento della matematica* (a cura dell'UNESCO – traduzione di Giuseppe Festa), Torino, SEI, ristampa 1983.

[4] Francesco Speranza, *Relazioni e strutture*, Bologna, Zanichelli, ristampa 1975.