Facoltà di Ingegneria

Precorso di Matematica

Parte II : Strutture algebriche e insiemi numerici

1. Gruppi

In prima approssimazione, una struttura algebrica è un insieme dotato di una o più operazioni. Nel caso in cui le operazioni siano più di una, esse dovranno essere compatibili (nel senso che sarà precisato più avanti).

Diamo come noto il fatto che $\mathbb{N}$ è dotato di due operazioni interne, somma e prodotto, cioè per ogni $a, b \in \mathbb{N}$: $a + b \in \mathbb{N}$ e $ab \in \mathbb{N}$.

Il concetto di operazione interna si generalizza ad insiemi qualunque:

1.1. Definizione. Si dice *operazione binaria* $*$ in un insieme G una applicazione

$$f : G \times G \longrightarrow G.$$

Il risultato $f((a, b))$ dell'operazione tra due elementi a e b si denota con $a * b$. In tal caso si dice che G è *chiuso* rispetto all'operazione $*$.

Notazione. Spesso, per indicare che si considera la struttura algebrica data dall'insieme G con l'operazione $*$, si scrive $(G, *)$.

1.1.1. Esempi. E' ben noto che la somma ed il prodotto in $\mathbb{N}$ sono operazioni binarie. Costruiamo un esempio di insieme "non numerico" dotato di operazione binaria. Si consideri un triangolo equilatero ABC e sia R l'insieme delle sue rotazioni che portano a sovrapporre vertici a vertici.

Nella Figura 2 vengono illustrate le 3 possibili rotazioni:

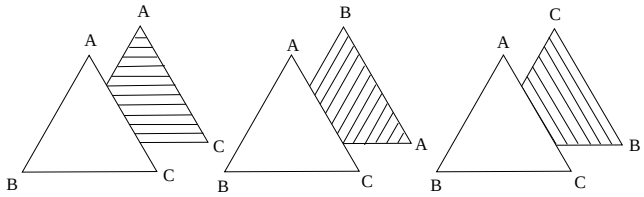

Figura 2

Usiamo la seguente notazione: per designare la rotazione (di $2\pi/3$) che porta il vertice A in B, B in C e C in A, scriveremo:

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}.$$

Quindi gli elementi di R sono 3 ed esattamente:

$$e = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \qquad x = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \qquad y = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}.$$

L'operazione che introduciamo in R è la composizione di rotazioni, che indicheremo con $\circ$; ad esempio $x \circ y$ è la rotazione che si ottiene operando prima y e poi x. Dunque $x \circ y = e$. La seguente tabella indica i risultati delle operazioni:

$\circ$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

tabella 1

1.2. Osservazione. Le strutture $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ godono delle ben note proprietà:
$a + (b + c) = (a + b) + c$, per ogni $a, b, c \in \mathbb{N}$.
$a + b = b + a$, per ogni $a, b \in \mathbb{N}$.
Inoltre vi sono elementi dal comportamento speciale: 0 e 1; infatti
$0 + a = a$ e $1a = a$, per ogni $a \in \mathbb{N}$.

In generale diamo le seguenti definizioni.

1.3. Definizione. Sia G un insieme dotato di un'operazione binaria $*$. Diciamo che $*$ è *associativa* se

$$a * (b * c) = (a * b) * c, \quad \text{per ogni} \quad a, b, c \in G.$$

Diciamo che $*$ è *commutativa* se

$$a * b = b * a, \quad \text{per ogni} \quad a, b \in G.$$

1.4. Definizione. Sia $(G, *)$ come sopra. Un elemento e di G è detto *elemento neutro* rispetto a $*$ se

$$a * e = e * a = a, \quad \text{per ogni} \quad a \in G.$$

Se $(G, *)$ ha elemento neutro e, scriveremo: $(G, *, e)$.

Si osservi che l'elemento e della tabella 1 è elemento neutro di R. Inoltre, ancora dalla tabella 1, si vede che per ogni elemento $r \in R$, esiste $r' \in R$ tale che $r \circ r' = r' \circ r = e$, infatti $e \circ e = e$, $x \circ y = y \circ x = e$.

1.5. Definizione. Sia $(G, *, e)$ come sopra e sia a un suo elemento. Un elemento $\overline{a} \in G$ tale che

$$a * \overline{a} = \overline{a} * a = e.$$

si dice, a seconda dell'operazione $*$, *inverso* di a e si indica con a^{-1} (ad esempio se $*$ è un prodotto); oppure *opposto* di a e si indica con $-a$ (ad esempio se $*$ è una somma).

1.5.1. Esempi. Osserviamo che negli esempi precedenti ogni insieme con operazione ammette un elemento neutro: $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$, $(R, \circ, e)$. Osserviamo che, in R, y è l'inverso di x e x è l'inverso di y; mentre in $(\mathbb{N}, +, 0)$ e in $(\mathbb{N}, \cdot, 1)$ nessun elemento, eccetto quello neutro, ha opposto (risp. inverso).

Come è ben noto, si può ampliare in modo naturale $(\mathbb{N}, +, 0)$ affinché ogni elemento abbia opposto; l'insieme così ottenuto è quello degli *interi relativi* che si denota con $\mathbb{Z}$ ed è definito da $\mathbb{Z} = \{\pm n \mid n \in \mathbb{N}\}$.

1.6. Definizione. Sia G un insieme dotato di un'operazione binaria $*$. Se valgono le seguenti proprietà :
a) $*$ è associativa ;
b) esiste in G un elemento e che sia neutro rispetto a $*$;
c) ogni elemento di G ammette inverso (risp. opposto),
allora $(G, *, e)$ si dice *gruppo.*
Se vale anche la proprietà commutativa :
d) $a * b = b * a$ per ogni $a, b \in G$,
allora $(G, *, e)$ si dice *gruppo commutativo* o *abeliano.*

1.7. Osservazione. $(\mathbb{Z}, +, 0)$, $(R, \circ, e)$ sono gruppi commutativi.

Si prova facilmente il seguente risultato (lasciato come esercizio):

1.8. Proposizione. *Sia $(G, *, e)$ un gruppo. Allora:*
i) l'elemento neutro è unico;
ii) l'inverso di ogni elemento è unico. •

2. Anelli

E' noto che in $\mathbb{Z}$ sono definite due operazioni, somma e prodotto, compatibili tra loro, nel senso che il prodotto è distributivo rispetto alla somma.
Vogliamo definire una nuova nozione per insiemi dotati di due operazioni che si comportano "sostanzialmente" come la somma e il prodotto di $\mathbb{Z}$.

2.1. Definizione. Sia $(A, +, 0, \cdot, 1)$ un insieme dotato di due operazioni binarie, dette somma (denotata con $+$) e prodotto (denotato con $\cdot$), e di due elementi 0 e 1, tali che :
a) $(A, +, 0)$ è un gruppo commutativo ;
b) il prodotto è associativo;
c) 1 è elemento neutro rispetto al prodotto;
d) $a \cdot (b + c) = a \cdot b + a \cdot c$, per ogni $a, b, c \in A$.
In tal caso A si dice *anello.* Se inoltre il prodotto è commutativo, A si dice *anello commutativo.*

2.1.1. Esempio. $(\mathbb{Z}, +, 0, \cdot, 1)$ è ovviamente un anello.

2.1.2. Esempio. Un altro esempio fondamentale di anello è dato da $\mathbb{Z}[X]$. Con tale simbolo si denota l'insieme dei polinomi in una variabile X a coefficienti in $\mathbb{Z}$, cioè l'insieme delle espressioni:

$$\sum_{i=0}^{n} a_i X^i = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

con $a_i \in \mathbb{Z}$, $n \in \mathbb{N}$. Come è ben noto, in $\mathbb{Z}[X]$ sono definite le seguenti operazioni: siano $p(X) = \sum_{i=0}^{n} a_i X^i$ e $q(X) = \sum_{i=0}^{m} b_i X^i$ elementi di $\mathbb{Z}[X]$; supponendo $n \leq m$ si definisce allora:

$$p(X) + q(X) = \sum_{j=0}^{m} c_j X^j,$$

ove $c_j = a_j + b_j$ per $0 \leq j \leq n$ e $c_j = b_j$ per $n < j \leq m$;

$$p(X) \cdot q(X) = \sum_{h=0}^{m+n} d_h X^h$$

ove $d_h = \sum_{i+j=h} a_i b_j$. Con tali operazioni, $\mathbb{Z}[X]$ è un anello, come si verifica facilmente, ed è detto *anello dei polinomi a coefficienti interi*.

Notazione. Se A è un anello, con A^* si indica $A \setminus \{0_A\}$.

3. I numeri razionali e la nozione di campo

Abbiamo già visto che si può ampliare $\mathbb{N}$ con gli opposti dei suoi elementi, fino a ottenere il gruppo additivo $(\mathbb{Z}, +, 0)$, che si può verificare essere il più piccolo gruppo additivo contenente $\mathbb{N}$. Ci poniamo lo stesso problema rispetto alla struttura moltiplicativa di $\mathbb{Z}$. Innanzitutto osservia- mo che non esiste un gruppo moltiplicativo che contenga $\mathbb{Z}$, infatti 0 non può avere inverso moltiplicativo. Consideriamo pertanto $\mathbb{Z}^* = \mathbb{Z}\setminus\{0\}$; è quindi naturale chiedersi se esistono gruppi moltiplicativi contenenti $\mathbb{Z}^*$ e, in caso affermativo, qual è il più piccolo tra questi.
Supponiamo che esista un gruppo moltiplicativo G che contenga $\mathbb{Z}^*$; dovrà contenere gli inversi degli interi, cioè tutti gli elementi del tipo n^{-1}, denotati usualmente con $1/n$. Quindi, dovendo essere chiuso rispetto al prodotto, conterrà anche le frazioni del tipo m/n, ottenute come prodotto di $m \in \mathbb{Z}^*$ e dell'inverso di $n \in \mathbb{Z}^*$. Osserviamo, però, che ogni elemento del tipo m/n si può scrivere in infiniti modi, ad esempio $5/3 = 10/6 = \ldots = 5n/3n$, con $n \in \mathbb{Z}^*$. Dunque tali elementi si comportano come classi di equivalenza.
Da quanto precede, il candidato naturale per G è un insieme quoziente dell'insieme delle frazioni di numeri interi non nulli. Precisiamo meglio:

3.1. Definizione. Nell'insieme $\mathbb{Z}^* \times \mathbb{Z}^*$ poniamo la seguente relazione :

$$(a, b)\mathcal{R}(c, d) \Leftrightarrow ad = bc.$$

E' facile provare che $\mathcal{R}$ è una relazione d'equivalenza. L'insieme quoziente $(\mathbb{Z}^* \times \mathbb{Z}^*)/\mathcal{R}$ si denota con $\mathbb{Q}^*$. Usualmente la classe di equivalenza $[(a, b)]$ di una coppia (a, b) si denota con a/b e si dice *numero razionale*.

Definiamo rigorosamente in $\mathbb{Q}^*$ il ben noto prodotto di frazioni.

3.2. Definizione. Se a/b, $c/d \in \mathbb{Q}^*$, definiamo $(a/b) \cdot (c/d) = (ac)/(bd)$.

Mostriamo che è una buona definizione, cioè non dipende dalla scelta dei rappresentanti. Siano $a'/b' = a/b$ e $c'/d' = c/d$. Dobbiamo provare che $(a'c')/(b'd') = (ac)/(bd)$.
Per ipotesi $a'b = ab'$ e $c'd = cd'$, dunque, moltiplicando membro a membro, segue la tesi.

3.3. Osservazione. C'è una "inclusione canonica" $\mathbb{Z}^* \subset \mathbb{Q}^*$, infatti ogni intero n si può pensare come il numero razionale $n/1$. Quindi in seguito, con abuso di notazione, indicheremo $n/1$ semplicemente con n.

Si verifica facilmente la seguente:

3.4. Proposizione. $(\mathbb{Q}^*, \cdot, 1)$ *è un gruppo abeliano.* •

Dall'osservazione e dalla proposizione precedenti, segue che $\mathbb{Q}^*$ è un particolare gruppo moltiplicativo contenente $\mathbb{Z}^*$. In effetti si può verificare che $\mathbb{Q}^*$ è il più piccolo di tali gruppi. Aggiungendo a $\mathbb{Q}^*$ lo 0, possiamo dotare l'insieme ottenuto, denotato con $\mathbb{Q}$, di struttura di anello. Più precisamente:

3.5. Definizione. Poniamo $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\mathcal{R}$, ove $\mathcal{R}$ è la relazione definita da

$$(a, b)\mathcal{R}(c, d) \Leftrightarrow ad = bc.$$

Tale insieme è detto *insieme dei numeri razionali.*

3.6. Definizione. Se $a/b, c/d \in \mathbb{Q}$, definiamo

$$a/b + c/d = (ad + bc)/bd \quad ; \qquad (a/b)(c/d) = (ac)/(bd).$$

Si osservi che il prodotto in $\mathbb{Q}$ è ben definito (la verifica è analoga a quella vista per $\mathbb{Q}^*$). Mostriamo che la somma è ben definita, cioè non dipende dalla scelta dei rappresentanti. Siano $a'/b' = a/b$ e $c'/d' = c/d$.
Dobbiamo provare che $(ad + bc)/bd = (a'd' + b'c')/b'd'$, o equivalentemente, che $(ad + bc)b'd' = (a'd' + b'c')bd$. Per ipotesi $a'b = ab'$ e $c'd = cd'$; dunque $(ad + bc)b'd' = adb'd' + bcb'd' = a'bdd' + bb'c'd = (a'd' + b'c')bd$, come volevamo.

Si verifica facilmente la seguente:

3.7. Proposizione. *Rispetto alle operazioni precedenti,* $\mathbb{Q}$ *è un anello commutativo.* •

Anche $\mathbb{Z}$ è un anello, ma $\mathbb{Q}$ ha una struttura più ricca: ogni elemento non nullo è invertibile rispetto al prodotto. Infatti se $a/b \neq 0$, cioè $a \neq 0$, esiste b/a e $(a/b) \cdot (b/a) = 1$; quindi $b/a = (a/b)^{-1}$.

3.8. Definizione. Se K è un anello commutativo tale che ogni elemento non nullo ammette inverso moltiplicativo, allora K si dice *campo.*
Equivalentemente K è un campo se e solo se $(K, +, 0)$ e $(K^*, \cdot, 1)$ sono gruppi abeliani e il prodotto è distributivo rispetto alla somma.

Da quanto visto prima, si deduce che $\mathbb{Q}$ è un campo.

Altri esempi di campi sono l'insieme $\mathbb{R}$ dei numeri reali e l'insieme $\mathbb{C}$ dei numeri complessi, che saranno trattati a parte.

Nei paragrafi precedenti, abbiamo visto le motivazioni algebriche che ci hanno portato dal concetto intuitivo di numero naturale ($n \in \mathbb{N}$) attraverso quello di intero relativo ($p \in \mathbb{Z}$) fino a quello di numero razionale ($a/b \in \mathbb{Q}$).

L'introduzione dei numeri reali, invece, nasce essenzialmente dalla esigenza di misurare segmenti. Più precisamente si identificano i numeri reali con i punti di una retta nel modo seguente: si consideri una retta r e su di essa si fissi un punto O ed una unità di misura $u = OA$. Per ogni punto P di r, la misura (con segno) del segmento OP rispetto all'unità di misura u è il corrispondente numero reale. In tal modo si ottiene la ben nota corrispondenza biunivoca tra i punti di una retta e i numeri reali. L'insieme dei numeri reali si indica con $\mathbb{R}$. E' altresì ben noto che $\mathbb{Q} \subset \mathbb{R}$, infatti, ad esempio, $\sqrt{2} \in \mathbb{R}$, ma $\sqrt{2} \notin \mathbb{Q}$: si ricordi che la diagonale di un quadrato ed il suo lato non ammettono sottomultipli comuni.
Ci sono vari modi per introdurre formalmente $\mathbb{R}$: le sezioni di Dedekind, la rappresentazione decimale, le successioni di Cauchy, etc. Descriviamo brevemente quest'ultimo metodo, rimandando al corso di Analisi per ulteriori dettagli e approfondimenti.

4.1. Definizione. Una *successione* di numeri razionali è un'applicazione $f : \mathbb{N} \longrightarrow \mathbb{Q}$. Usualmente tale successione si denota con $\{a_n\}_{n\in\mathbb{N}}$, o brevemente con $\{a_n\}$, intendendo che $a_n = f(n)$. Il numero a_n è detto *termine n-esimo* della successione.

4.1.1. Esempio. Sono successioni $A = \{n\}$, $B = \{1/n\}$, $C = \{3\}$; quest'ultima è la successione costante, in cui ogni termine è uguale a 3.

E' intuitivo che il termine generale della successione A tende a crescere al crescere di n, mentre quello della successione B tende a 0 e quello della successione C resta costantemente uguale a 3. Tale idea è resa più precisa dalla seguente
4.2. Definizione. Si dice che la successione di numeri razionali $\{a_n\}$ *converge* al numero $l \in \mathbb{Q}$ se

per ogni $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, esiste $n_0 \in \mathbb{N}$ tale che se $n > n_0$
allora $|a_n - l| < \epsilon$.

In tal caso si dice anche che $\{a_n\}$ è *convergente* e l è il *limite* della successione $\{a_n\}$; ciò si scrive

$$\lim_{n\to\infty} a_n = l.$$

4.2.1. Esempio. E' facile verificare che $\lim_{n\to\infty} 1/n = 0$, $\lim_{n\to\infty} 3 = 3$, mentre le successioni $A = \{n\}$ e $D = \{(-1)^n\}$ non hanno per limite alcun numero razionale. E' chiaro, comunque, che le ultime due successioni non hanno limite in quanto A "tende" all'infinito, mentre D oscilla tra -1 e 1. Ci sono però dei casi in cui una successione non ha limite in $\mathbb{Q}$ anche se i termini diventano infinitamente vicini al crescere di n.

4.3. Definizione. Una successione $\{a_n\}$ di dice *successione di Cauchy* se

per ogni $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, esiste $n_0 \in \mathbb{N}$ tale che se $n, m > n_0$ allora $|a_n - a_m| < \epsilon$.

Il seguente teorema (di cui omettiamo la dimostrazione) mette in luce il legame tra le successioni convergenti e quelle di Cauchy:

4.4. Teorema. *Una successione convergente è di Cauchy.*

Tuttavia non è vero il viceversa:

4.4.1. Esempio. Si consideri la successione $S = \{s_n\}$ ove

$$s_n = 1 + 1 + 1/2! + 1/3! + \cdots + 1/n!$$

cioè $s_n = 1 + \sum_{k=1}^{n} 1/k!$. Si verifica che tale successione è di Cauchy; si può comunque provare che non converge ad alcun numero razionale.
Intuitivamente si comprende che gli elementi di una successione di Cauchy si "accumulano" attorno a un punto, che non corrisponde sempre ad un numero razionale. Inoltre possono esistere altre successioni che individuano lo stesso punto. Si definirà "numero reale" quell'oggetto rappresentato da tutte queste successioni.
Operiamo dunque nel seguente modo: definiamo una relazione di equiva- lenza nell'insieme di tutte le successioni di Cauchy, identificando successioni infinitamente vicine al crescere di n. Si dice *numero reale* una classe di equivalenza così ottenuta. Più precisamente:

4.5. Definizione. Sia $\mathcal{C}$ l'insieme di tutte le successioni di Cauchy a elementi in $\mathbb{Q}$. Siano $A = \{a_n\}$, $B = \{b_n\} \in \mathcal{C}$. Poniamo $A \cong B$ se:
per ogni $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, esiste $n_0 \in \mathbb{N}$ tale che se $n > n_0$
allora $|a_n - b_n| < \epsilon$.
Si verifica che tale relazione è una relazione d'equivalenza in $\mathcal{C}$. L'insieme quoziente $\mathcal{C}/\cong$ è detto *insieme dei numeri reali* e si denota con $\mathbb{R}$.

Anche se non è banale, si può verificare che l'insieme dei numeri reali così introdotto corrisponde al modello intuitivo di partenza.

4.6. Osservazione. Se x è un numero razionale, la successione costante $X = \{x\}_{n\in\mathbb{N}}$ ha per limite x, dunque è di Cauchy. In tal caso la sua classe d'equivalenza $[X] \in (\mathcal{C}/\cong) = \mathbb{R}$ si può identificare con lo stesso numero x; in modo più rigoroso, esiste un'applicazione $i : \mathbb{Q} \longrightarrow \mathbb{R}$ definita da $x \mapsto [X]$. Si vede facilmente che tale applicazione è iniettiva e quindi si può identificare $\mathbb{Q}$ con $i(\mathbb{Q}) \subset \mathbb{R}$. Per brevità scriveremo dunque $\mathbb{Q} \subset \mathbb{R}$, per intendere tale "inclusione canonica".

Abbiamo visto, come con le successioni di Cauchy si possa ampliare $\mathbb{Q}$ fino ad ottenere $\mathbb{R}$. E' naturale chiedersi se con le successioni di Cauchy ad elementi reali (ove per *successione di numeri reali* si intende una applicazione $f : \mathbb{N} \longrightarrow \mathbb{R}$) si possa ampliare $\mathbb{R}$.
La risposta è negativa, come d'altro canto ci si poteva aspettare tenendo conto del modello intuitivo di $\mathbb{R}$. Si ha infatti il seguente

4.7. Teorema. *Sia $\{a_n\}_{n\in\mathbb{N}}$ una successione di numeri reali. Allora $\{a_n\}_{n\in\mathbb{N}}$ è di Cauchy se e solo se è convergente.*

Tale proprietà dei reali si esprime dicendo che $\mathbb{R}$ è *completo*. La completezza di $\mathbb{R}$ verrà studiata nel corso di Analisi.
Per quanto riguarda la struttura algebrica di $\mathbb{R}$, si possono definire una somma e un prodotto che estendono le corrispondenti operazioni in $\mathbb{Q}$. Tale definizione fa uso di una nozione di somma e di prodotto tra successioni, che qui omettiamo.
Si può provare che, con tali operazioni, $\mathbb{R}$ è un campo.