Isomorfismo aritmetico

di Antonino Giambò

1. A chi legge queste pagine non è certamente sconosciuta la nozione di *morfismo* e sicuramente gli sono noti i vari tipi di morfismi, come per esempio l'*isomorfismo*. Ma forse non a tutti è familiare il concetto di *isomorfismo aritmetico*, idea del matematico siciliano Michele Cipolla.

È di questo che intendo occuparmi in questo articolo.

Incomincio, a beneficio di quei due o tre che forse hanno dimenticato di cosa si tratti, a definire il morfismo, ricordando per prima cosa che il termine deriva dal greco μορφή (*morphé*, *forma*).

Eccone la definizione:

Date due strutture algebriche $(A,*)$ e $(B,\perp)$, si definisce ***morfismo*** fra le due strutture una funzione f di A in B tale che, quali che siano $x, y \in A$, risulti: $f(x*y)=f(x)\perp f(y)$.

In realtà, ci sono diversi tipi di morfismi, dei quali non ho interesse ad occuparmi in questa sede. Mi interessa, tuttavia, un particolare tipo di morfismo, il cosiddetto *isomorfismo*.

Ebbene, un ***isomorfismo*** non è altro che un morfismo in cui la funzione f è biiettiva. Vale a dire, una funzione capace di stabilire una corrispondenza biunivoca fra gli elementi di A e quelli di B.

Due strutture algebriche, fra le quali sussiste un isomorfismo, si dicono ***isomorfe***.

Riassumendo:

Due strutture algebriche $(A,*)$ e $(B,\perp)$ si dicono ***isomorfe*** se esiste una biiezione f di A in B tale che, comunque si scelgano x, y in A, risulti: $f(x*y)=f(x)\perp f(y)$.

Approfondiamo il concetto con il supporto di un diagramma.

Consideriamo allora due strutture algebriche $(A,*)$ e $(B,\perp)$ e supponiamo che esista una biiezione f di A in B. Detti x, y due qualsiasi elementi di A, anche $x * y$ appartiene ad A. I corrispondenti in B di tali elementi $x, y, x * y$ sono chiaramente (figura 1): $f(x), f(y), f(x * y)$. Se $f(x*y)=f(x)\perp f(y)$ allora le due strutture sono isomorfe.

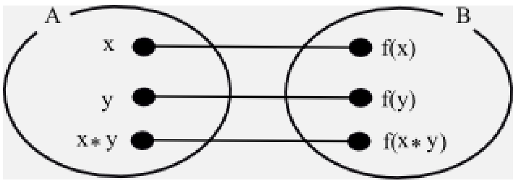

figura 1

Per una migliore comprensione consideriamo due situazioni particolari.

- Prima situazione. Siano le strutture algebriche $(\mathbb{N},+)$ ed $(\mathbb{N}, \times)$, dove $\mathbb{N}$ è l'insieme dei numeri naturali, mentre "+" e "×" sono le ordinarie operazioni di addizione e moltiplicazione. L'applicazione $f: n \rightarrow n$, $\forall n \in \mathbb{N}$, è evidentemente una biiezione di $\mathbb{N}$ in $\mathbb{N}$. Se a, b sono due qualsiasi elementi di $\mathbb{N}$, in genere risulta $f(a+b) \neq f(a) \times f(b)$. Infatti: $f(a+b)=a+b$, mentre $f(a)\times f(b)=a\times b$. E, di norma: $a+b\neq a\times b$.

Le due strutture, dunque, <u>non sono isomorfe</u>.

Un diagramma (figura 2), dove abbiamo posto $a=2$ e $b=3$, visualizza questo fatto.

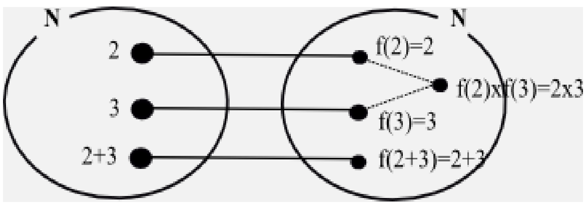

figura 2

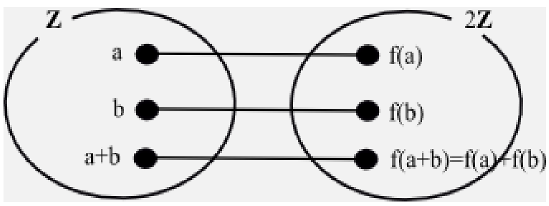

figura 3

- Seconda situazione. Siano le strutture algebriche $(\mathbb{Z},+)$ e $(2\mathbb{Z},+)$, dove $\mathbb{Z}$ è l'insieme degli interi e $2\mathbb{Z}$ è l'insieme degli interi pari. L'applicazione $f: z \rightarrow 2z$, $\forall z \in \mathbb{Z}$, è una biiezione di $\mathbb{Z}$ in $2\mathbb{Z}$. Se a, b sono due qualsiasi elementi di $\mathbb{Z}$, risulta $f(a+b)=f(a)+f(b)$ (figura 3). Infatti: $f(a+b) = 2(a+b) = 2a+2b = f(a)+f(b)$.

Le due strutture, dunque, sono isomorfe.

2. A questo punto sorge una domanda: **Perché è importante sapere che due strutture sono isomorfe?**

Prima di passare alla risposta, una precisazione: il termine "isomorfismo" è composto di due parole greche: ἴσος (*isos*, *uguale*) e, di nuovo, μορφή (*morphé, forma*). Significa quindi letteralmente "uguale forma".

Riprendendo la domanda precedente, fornisco due risposte, una intuitiva ed una formale.

Sul piano intuitivo, è interessante la definizione di isomorfismo formulata da Hofstadter (n. 1945), matematico, filosofo e divulgatore scientifico statunitense, nella sua opera più conosciuta [2, pag. 54]:

«Si parla di "isomorfismo" quando due strutture complesse si possono [...] far corrispondere l'una all'altra, in modo tale che per ogni parte di una delle strutture ci sia una parte corrispondente nell'altra struttura; in questo contesto diciamo che due parti sono "corrispondenti" se hanno un ruolo simile nelle rispettive strutture.»

Ma questa formulazione intuitiva, che forse non dice tutto, è espressa in forma più rigorosa dal seguente teorema:

TEOREMA. **Siano date due strutture algebriche isomorfe. Se l'operazione di una di esse gode di certe proprietà (commutativa, associativa, …) anche l'operazione dell'altra struttura gode delle stesse proprietà.**

DIMOSTRAZIONE. Siano $(A,*)$ e $(B,\perp)$ due strutture algebriche isomorfe. Questo implica che:

esiste una biiezione f di A in B; $f(x*y)=f(x)\perp f(y),\ \forall x,y\in A$.

Fermiamo l'attenzione su una delle proprietà di cui eventualmente gode l'operazione "$*$" in A, per esempio la proprietà associativa e facciamo vedere che anche l'operazione "$\perp$" in B gode della stessa proprietà.

Dunque, $\forall x,y,z\in A$:

$$(x*y)*z = x*(y*z) \ \rightarrow\ f\big((x*y)*z\big) = f\big(x*(y*z)\big) \ \rightarrow\ f(x*y)\perp f(z) = f(x)\perp f(y*z) \ \rightarrow$$
$$\rightarrow\ (f(x)\perp f(y))\perp f(z) = f(x)\perp\big(f(y)\perp f(z)\big).$$

Come volevasi dimostrare. Analogamente per altre eventuali proprietà.

3. Se l'isomorfismo tra due strutture algebriche è importante perché le parti corrispondenti delle due strutture svolgono ruoli similari, come dice Hofstadter, ancora più importante è l'*isomorfismo aritmetico* tra due strutture numeriche, perché adesso le parti corrispondenti delle due strutture si possono considerare addirittura identiche.

Inoltre, l'*isomorfismo aritmetico* svolge un ruolo fondamentale nell'operazione di ampliamento degli insiemi numerici, nel passaggio cioè da $\mathbb{N}$ a $\mathbb{Z}$ a $\mathbb{Q}$ a $\mathbb{R}$.

L'isomorfismo aritmetico è un'idea del matematico siciliano **Michele Cipolla** (1880-1947).

Michele Cipolla

Prima di procedere, mi sembra giusto fornire qualche nozione biografica su questo matematico, forse poco conosciuto al grande pubblico.

Michele Cipolla nacque a Palermo, dove condusse con risultati eccellenti gli studi pre-universitari. Frequentò per un periodo la Scuola Normale Superiore di Pisa ma, dopo la morte del padre, si vide costretto a trasferirsi a quella di Palermo, dove si laureò all'età di 22 anni. Dopo circa un decennio d'insegnamento delle scuole medie superiori, dal 1911 ricoprì la cattedra di Analisi Algebrica nell'Università di Catania, per passare poi, dal 1923, a quella di Palermo, dove chiuse la sua carriera accademica.

Il dibattito sull'aritmetizzazione dell'Analisi, cioè la possibilità di fondare l'Analisi sui numeri reali, avviato da tempo per merito soprattutto di Weierstrass, diventa di attualità negli anni a cavallo del 1910, quando, con Peano e Frege, si tenta di ricondurre tutta la Matematica ai numeri naturali. Oggi sappiamo che questo programma fallì. Comunque sia, dati per acquisiti i numeri naturali, Cipolla formulò una brillante teoria sulla costruzione dei numeri reali per successivi ampliamenti a partire appunto dai numeri naturali. Fu precisamente in questo studio che egli maturò l'idea di introdurre la relazione di *isomorfismo aritmetico*. Relazione che permette di rendere rigoroso l'ampliamento da $\mathbb{N}$ a $\mathbb{Z}$ a $\mathbb{Q}$ a $\mathbb{R}$. Lo fece nel suo trattato dal titolo *Analisi algebrica e introduzione al calcolo infinitesimale* (1914).

L'isomorfismo aritmetico è, in realtà, un doppio isomorfismo fra due strutture numeriche. Lo precisiamo meglio.

Due strutture numeriche $(A,+,\times)$ e $(B,+,\times)$ si dicono in ***isomorfismo aritmetico*** se esiste una funzione f di A in B che stabilisca fra le due strutture due isomorfismi, ognuno rispetto a ciascuna operazione. Vale a dire (figura 4):

$$f \text{ è una biiezione di } A \text{ in } B; \quad f(a+b) = f(a)+f(b) \ \text{ e } \ f(a\times b) = f(a)\times f(b), \ \ \forall a,b\in A.$$

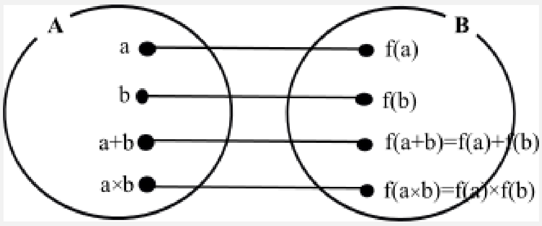

figura 4

Pertanto, in virtù del teorema dimostrato sopra, possiamo concludere con la seguente affermazione:

Due strutture numeriche in isomorfismo aritmetico hanno la stessa aritmetica.

Questo, in altre parole, significa che le due strutture presentano le stesse proprietà formali sia rispetto all'addizione sia rispetto alla moltiplicazione. Inoltre, cosa che può essere dimostrata agevolmente, se la moltiplicazione è distributiva rispetto all'addizione in una delle due strutture lo è anche nell'altra.

Questo fatto – la circostanza cioè che l'aritmetica che vale in una struttura numerica si conserva in un'altra in isomorfismo aritmetico con essa – unito alla corrispondenza biunivoca che sussiste fra i sostegni delle due strutture – permette di ritenere IDENTICHE le strutture medesime, anche se in realtà sono concettualmente distinte, e pertanto di identificare ogni elemento del sostegno di una di esse con il corrispondente elemento del sostegno dell'altra.

4. A questo punto, giusto per fornire un esempio, può essere interessante stabilire come si costruisce l'insieme $\mathbb{Z}$ degli interi relativi mediante un ampliamento dell'insieme $\mathbb{N}$ dei naturali, utilizzando per l'appunto l'isomorfismo aritmetico e spiegare perché si può ritenere corretta l'inclusione $\mathbb{N} \subset \mathbb{Z}$.

- Incominciamo allora a prendere in considerazione l'insieme $\mathbb{N}\times\mathbb{N}$ e due suoi qualsiasi elementi (a,b) e (c,d). Si dice che (a,b) è *equidifferente* (o *equivalente per differenza*) a (c,d) se e solo se a+d=b+c. In simboli:

$$(a,b) \doteq (c,d) \iff a+d=b+c\,, \quad (a,b),(c,d) \in \mathbb{N}\times\mathbb{N}.$$

Si dimostra che la relazione così definita è una relazione di equivalenza propriamente detta, ragion per cui opera una ripartizione di $\mathbb{N}\times\mathbb{N}$ in classi di equivalenza. Ognuna di esse – vale a dire ogni insieme di coppie equidifferenti – si denomina *numero intero relativo* (o semplicemente *numero intero*).

Naturalmente, ogni coppia $(a,b)\in\mathbb{N}\times\mathbb{N}$ individua uno ed un solo numero intero – lo indichiamo provvisoriamente con $<a.b>$ – ed è individuato da ogni altra coppia di naturali equidifferente ad (a,b). Per esempio:

$$<3,2> = \{(3,2), (2,1), (1,0), (4,3), \ldots\}, \quad <2,4> = \{(2,4), (1,3), (0,2), (3,5), \ldots\}.$$

- È evidente che, presa una qualsiasi coppia $(a,b)\in\mathbb{N}\times\mathbb{N}$, per ogni numero naturale m, che non superi il minore dei due numeri a, b, risulta:

$$(a, b) \doteq (a - m,\ \ b - m).$$

Si desume da ciò che esiste una coppia avente nulla almeno una componente in ogni insieme di coppie equidifferenti di $\mathbb{N}\times\mathbb{N}$: basta infatti sottrarre da ciascuna componente della coppia quella componente che non supera l'altra. Una tale coppia si denomina *coppia ridotta*. Di solito è quella che si assume come rappresentante del numero intero. Cosicché, considerata una qualsiasi coppia $(a,b)\in\mathbb{N}\times\mathbb{N}$:

- se $a=b$ la forma ridotta del numero intero è $<0,0>$; questo numero è chiamato *zero* ed è indicato solitamente con 0;
- se $a>b$ la forma ridotta del numero intero è $<r,0>$, dove $r=a-b$; questo numero si definisce *positivo* ed è indicato con $+r$;
- se $b>a$ la forma ridotta del numero intero è $<0,r>$, dove $r=b-a$; questo numero si definisce *negativo* ed è indicato con $-r$.

La forma 0, +r, –r dei numeri interi $<0,0>$, $<r,0>$, $<0,r>$ si dice *forma canonica*. È quella generalmente usata per scrivere i numeri interi.

Attenzione! L'aver definito positivo ogni numero $<r,0>$ e negativo ogni numero $<0,r>$, dove r è un numero naturale non nullo, non autorizza ancora un confronto con 0. La cosa va ovviamente approfondita.

Considerate, al riguardo, due coppie ordinate di numeri naturali (a,b) e (c,d), la coppia (a,b) si dice *prevalente per differenza* alla coppia (c,d) se e solo se $a+d>b+c$. Si scrive: $(a,b)\succ(c,d)$. In tal caso il numero intero $<a,b>$ si dice *maggiore* del numero $<c,d>$; si dice pure che il numero $<c,d>$ è *minore* del numero $<a,b>$. Posto $x=<a,b>$ e $y=<c,d>$, si scrive rispettivamente: $x>y$ o $y<x$.

Osservando poi che, per ogni naturale x non nullo, risulta $(x,0)\succ(0,0)$ e $(0,0)\succ(0,x)$, si può concludere che si ha:

$$+x > 0 \quad \text{e} \quad -x < 0.$$

Vale a dire:

Ogni numero definito positivo *è maggiore di 0, mentre ogni numero definito* negativo *è minore di 0.*

Indichiamo con i simboli seguenti:

$$\mathbb{Z} \quad \mathbb{Z}^{+} \quad \mathbb{Z}^{-}$$

rispettivamente l'insieme dei numeri interi, quello degli interi x non negativi (cioè $x\geq 0$), quello infine degli interi x non positivi (cioè $x\leq 0$).

- Consideriamo adesso due qualsiasi numeri interi non negativi: $+a=<a,0>$ e $+b=<b,0>$, dove ovviamente a, b sono numeri naturali. Ragion per cui anche $a+b$ e $a\times b$ sono numeri naturali e, di conseguenza, i numeri interi $<a+b,\ 0>$ e $<a\times b,\ 0>$ sono essi pure interi non negativi. Da tutto ciò discende che le operazioni definite dalle seguenti relazioni:

$$<a,0> \oplus <b,0> = <a+b,\ 0> \quad \text{ossia} \quad (+a)\oplus(+b)=+(a+b)$$
$$<a,0> \otimes <b.0> = <a\times b,\ 0> \quad \text{ossia} \quad (+a)\otimes(+b)=+(a\times b)$$

sono leggi di composizione interne all'insieme $\mathbb{Z}^{+}$ degli interi non negativi.

Ora, messe a confronto le due strutture numeriche $(\mathbb{Z}^{+},\oplus,\otimes)$ e $(\mathbb{N},+,\times)$, si dimostra facilmente che sono in isomorfismo aritmetico. Di conseguenza, per quanto già detto in precedenza, è legittimo identificare i due insiemi $\mathbb{Z}^{+}$ e $\mathbb{N}$, anche se sono concettualmente distinti. Scriveremo perciò, ogni volta che lo riterremo opportuno, a al posto di +a, ponendo per l'appunto $+a=a$.

È in questo senso che affermiamo che $\mathbb{N}\subset\mathbb{Z}$, anche se, in realtà, $\mathbb{N}$ è in isomorfismo aritmetico con un sottoinsieme di $\mathbb{Z}$. Come dire, insomma, che $\mathbb{Z}$ contiene un sottoinsieme, $\mathbb{Z}^{+}$, che si comporta in tutto e per tutto come $\mathbb{N}$.

Inoltre, le due operazioni "$\oplus$" e "$\otimes$", introdotte in $\mathbb{Z}^{+}$, per analogia con le corrispondenti operazioni in $\mathbb{N}$, possono essere indicate più semplicemente con i simboli "+" e "×".

- Si introducono in $\mathbb{Z}$ le operazioni di addizione e moltiplicazione come naturale estensione di tali operazioni in $\mathbb{N}$.

Consideriamo, al riguardo, due qualsiasi interi non negativi: <a,b> e <c,d>. Si ha, in sequenza:

$$<a,b> + <c,d> = <a-b, 0> + <c-d, 0> = <(a-b)+(c-d), 0> = <a+c, b+d>.$$

Questa relazione, vale a dire:

$$<a,b> + <c,d> = <a+c, b+d>,$$

non è altro che un modo diverso di rappresentare l'addizione in $\mathbb{Z}^+$. La si assume, tuttavia, come definizione di addizione in $\mathbb{Z}$. Questo perché è possibile dimostrare che l'operazione è ben definita, vale a dire che è invariante al variare delle coppie scelte. Ossia:

$$\text{se } <a,b> = <a',b'> \text{ e } <c,d> = <c',d'> \text{ allora } <a,b> + <c,d> = <a',b'> + <c',d'>.$$

Si dimostrano conseguentemente le note relazioni che esprimono le regole per l'addizione dei numeri interi. In effetti:

$$(+a) + (+b) = < a, 0 > + < b, 0 > = < a + b, 0 > = +(a + b),$$
$$(-a) + (-b) = < 0, a > + < 0, b > = < 0, a + b > = -(a + b),$$
$$(+a) + (-b) = < a, 0 > + < 0, b > = < a, b > = \begin{cases} < a - b, 0 > = +(a - b) \text{ se } a \geq b \\ < 0, b - a > = -(b - a) \text{ se } b \geq a \end{cases}$$

Con un ragionamento analogo si dimostra che (per comodità scriviamo pq invece di p×q):

$$<a,b> \times <c,d> = <ac+bd, ad+bc>,$$

e da qui le note regole per la moltiplicazione dei numeri relativi.

Si possono poi dimostrare tutte le proprietà che fanno della struttura numerica $(\mathbb{Z}, +, \times)$ un modello di anello commutativo dotato di elemento unità.

5. Con un ragionamento concettualmente simile a quello che ci ha portati a concludere che $\mathbb{N} \subset \mathbb{Z}$, ma in verità un po' più complicato a causa di calcoli più complessi, possiamo stabilire che risulta:

$$\mathbb{Z} \subset \mathbb{Q}, \quad \mathbb{Q} \subset \mathbb{R}.$$

Inclusioni valide, come l'inclusione $\mathbb{N} \subset \mathbb{Z}$, a meno di un isomorfismo aritmetico.

6. Ribadisco che è l'isomorfismo aritmetico che consente l'identificazione di due strutture numeriche e non un semplice isomorfismo, che pure è una cosa notevole.

Basta un contro-esempio, banale se si vuole, per comprenderlo.

Consideriamo al riguardo le due strutture numeriche $(\mathbb{Z}, +, \times)$ e $(2\mathbb{Z}, +, \times)$.

Abbiamo già visto che sono isomorfe le due strutture $(\mathbb{Z}, +)$ e $(2\mathbb{Z}, +)$.

Non lo sono invece le due strutture $(\mathbb{Z}, \times)$ e $(2\mathbb{Z}, \times)$. Infatti, ritornando all'applicazione $f: z \to 2z$ e prendendo $a, b \in \mathbb{Z}$, risulta $f(a \times b) = 2ab$, mentre $f(a) \times f(b) = (2a) \times (2b) = 4ab$.

Pertanto $f(a \times b) \neq f(a) \times f(b)$.

Dunque è provato che non sono in isomorfismo aritmetico le due strutture $(\mathbb{Z}, +, \times)$ e $(2\mathbb{Z}, +, \times)$.

Cosicché, pur essendo isomorfe le due strutture $(\mathbb{Z}, +)$ e $(2\mathbb{Z}, +)$, non è possibile identificare i due insiemi sostegno $\mathbb{Z}$ e $2\mathbb{Z}$. Cosa che, ad onore del vero, non ha nulla di sorprendente. Caso mai, sarebbe stato sorprendete il contrario, che cioè essi fossero identificabili.

Ma questo controesempio evidenzia che l'isomorfismo aritmetico fra due strutture numeriche è, quando c'è, qualcosa di veramente notevole.

BIBLIOGRAFIA.

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

[2] Douglas R. HOFSTADTER, *Gödel, Escher, Bach: un'eterna ghirlanda brillante*, Milano, Adelphi, 1990.

[3] Richard SPRECKELMEYER, *I numeri interi*, Milano, Progresso Tecnico Editoriale, 1967.

[4] Friedrich WAISMANN, *Introduzione al pensiero matematico*, Torino, Boringhieri, 1971.