PIANO LAUREE SCIENTIFICHE

PREREQUISITI AGLI SPAZI VETTORIALI PER STUDENTI DEL QUINTO ANNO

Prof. Sara Dragotti

Laboratorio di Autovalutazione

Nel corso di Geometria 1 vengono presentati i primi ambienti in cui la Geometria lavora: spazi euclidei e spazi proiettivi. Nella moderna trattazione questi ambienti poggiano su una fondamentale struttura algebrica che è quella di *Spazio vettoriale* su un *campo*. Per questo motivo il corso di Geometria 1 prevede una parte iniziale di *Algebra lineare*, in cui vengono date le nozioni di campo, con annessi teoremi, spazio vettoriale, con annessi teoremi, e si trattano anche i sistemi lineari a coefficienti in un campo.

Questo Laboratorio introduce alle prime nozioni di Algebra lineare, e premette brevemente quella di applicazione tra insiemi per facilitare il linguaggio successivo.

Molte affermazioni apparentemente elementari saranno lasciate per esercizio agli studenti affinché si rendano conto che certi passaggi non vanno fatti in maniera automatica, ma che sono conseguenza di procedimenti corretti in base alle definizioni di gruppo, campo o altro.

1. Applicazioni

Un'**applicazione** (o funzione) è una terna (S, T, f) dove S è un insieme non vuoto, detto *dominio*, T un insieme non vuoto, detto *codominio*, ed f è una legge che consente di associare ad ogni elemento di S uno, ed un solo, elemento di T.

Si usano le scritture e frasi seguenti:

$f\colon S \to T$, f è un'applicazione di S in T.

$f(a) = a'$, all'elemento a di S corrisponde in f l'elemento a' di T, o anche: a' è l'immagine di a in f.

Riflettere bene sulla definizione di cui sopra e sulle parole sottolineate.

Esempio 1
S = insieme degli studenti presenti in un'aula, T = insieme degli anni tra il 1900 ed il 2013, legge: ad ogni studente si associ il suo anno di nascita.

Esempio 2
S = insieme dei punti di un piano euclideo, T = insieme dei punti di una retta r dello stesso piano, legge: ad ogni punto del piano si associ la sua proiezione ortogonale sulla retta r.

Esempi 3, 4, 5, 6
$S = T = \mathbb{Z}$ (insieme dei numeri interi)

$$f(x) = x^2$$
$$g(x) = 2x$$
$$h(x) = x + 1$$
$$q(x) = \begin{cases} x & \text{se } x \text{ è positivo o nullo} \\ x+1 & \text{se } x \text{ è negativo} \end{cases}$$

Il termine funzione è sinonimo di applicazione, ma, come per tutti i sinonimi, c'è una leggera sfumatura di differenza che fa preferire a volte l'uno, a volte l'altro termine. Si preferisce il termine funzione, ad esempio, quando si vuole sottolineare come il variare dell'elemento $f(x)$ dipenda dal variare di x, ma è l'appropriarsi del concetto e la pratica che suggeriscono quale termine sia più appropriato usare.

Siano A, B, C insiemi qualunque, e siano f un'applicazione di A in B, e g un'applicazione di B in C. Si può considerare l'applicazione **composta** (o **prodotto**) di esse, ottenuta associando ad ogni elemento x di A l'immagine mediante g dell'immagine di x mediante f. Indicando tale applicazione di A in C con il simbolo fg, si avrà pertanto per ogni elemento x dell'insieme A

$$fg(x) = g(f(x))$$

Esercizio 1 Verificare che fg è effettivamente un'applicazione.

Componiamo ora, per fare un esempio, le applicazioni f e g dei precedenti esempi 3 e 4. Si avrà per ogni intero x: $fg(x) = g(f(x)) = g(x^2) = 2x^2$. Componendo invece l'applicazione h di cui all'esempio 5 con g si ottiene: $hg(x) = g(h(x)) = g(x+1) = 2(x+1)$.

Avvertenza Si possono comporre due applicazioni solo se il codominio della prima di esse coincide con il dominio della seconda.

Osservazione Il prodotto di applicazioni non è commutativo, ossia in generale $fg(x)$ non è uguale a $gf(x)$. Vediamo il caso di uno degli esempi di prodotto considerati sopra: risultava $fg(x) = 2x^2$, facendo invece il prodotto gf si otterrà per ogni intero x: $gf(x) = f(g(x)) = f(2x) = 4x^2$.

Esercizio 2 Verificare che il prodotto di applicazioni è associativo, ossia $(fg)h = f(gh)$.

Un'applicazione f si dice **biunivoca** se valgono entrambe le seguenti propretà:

A) elementi distinti del dominio hanno immagini distinte, ovvero

$$x \neq y \Longrightarrow f(x) \neq f(y)$$

B) ogni elemento del codominio è immagine di qualche elemento del dominio.

In altre parole se $f\colon S \to T$ è un'applicazione biunivoca ogni elemento di T è immagine di uno, ed un solo, elemento di S. Negli esempi precedenti f non è biunivoca perché non valgono né A) né B), g non è biunivoca perché vale A) ma non vale B), h è biunivoca, q non è biunivoca perché vale B) ma non vale A) (0 e -1 hanno la stessa immagine). Come sono le prime due applicazioni degli esempi?

Esercizio 3 Verificare che la composta di applicazioni biunivoche è biunivoca.

Per ogni applicazione biunivoca f di S in T si può definire l'applicazione di T in S che associa ad ogni elemento x di T quell'unico elemento y di S che lo ha per immagine in f. Più chiaramente, indicando con f^{-1} tale applicazione, si avrà

$$f^{-1}(x) = y \Longleftrightarrow f(y) = x$$

Esercizio 4 Verificare che f^{-1} è un'applicazione biunivoca.

L'applicazione f^{-1} si dice **inversa** di f.

Avvertenza La definizione di inversa si può dare solo per un'applicazione biunivoca. Se, ad esempio, pensiamo alla già citata applicazione di $\mathbb{Z}$ in sé $g(x) = 2x$, all'elemento 5, come ad un qualunque altro intero dispari, non potremmo associare nessun intero, e quindi non si avrebbe una applicazione. Così pure se pensiamo alla funzione di $\mathbb{Z}$ in sé $f(x) = x^2$, nell'ipotetica inversa un numero negativo non

avrebbe immagine ed inoltre un positivo come 4 ne dovrebbe avere due. In conclusione non è possibile: per poter definire la funzione inversa è indispensabile che per la funzione data valgano entrambe le proprietà A) e B). Ad esempio la funzione biunivoca $h(x) = x + 1$ di $\mathbb{Z}$ in sé ha per inversa la funzione $h^{-1}(x) = x - 1$.
Per quanto detto sopra un'applicazione biunivoca si dice anche **invertibile**.
Riflettere ancora e fare altri esempi.

Un'applicazione biunivoca di un insieme S in sé è detta spesso una **permutazione** di S.

Per ogni insieme non vuoto S si può definire l'applicazione di S in sé che associa ad ogni suo elemento x lo stesso x. Si tratta ovviamente di un'applicazione biunivoca, che è detta applicazione identica (o **identità**) di S. Se la indichiamo con id_S si avrà pertanto per ogni elemento x di S $id_S(x) = x$.

È veramente banale rendersi conto che per ogni applicazione f di S in un qualunque altro insieme T si ha: $id_S f = f id_T = f$, circostanza che in altre parole si esprime dicendo che *ogni identità è neutra per il prodotto.*

Inoltre se $f\colon S \to T$ è un'applicazione biunivoca, e quindi invertibile, è immediato verificare la relazione $ff^{-1} = id_S$ e l'analoga $f^{-1}f = id_T$.

2. Gruppi

Sia S un insieme non vuoto. Una **operazione interna definita in S** è un'applicazione f dell'insieme S^2 delle coppie di elementi di S nell'insieme S.

Nell'uso corrente per indicare una operazione si preferisce un simbolo grafico come $*$ oppure $+$, $\wedge$, $\times$, $\bullet$ al posto di una lettera latina o greca con cui si indica solitamente un'applicazione, e scrivere $a + b$ al posto di $+((a, b))$ e simili.

Definizioni

Un'operazione $*$ definita in un insieme S si dice **associativa** se vale la proprietà

$$\textit{Per ogni terna } a, b, c \textit{ di elementi di } S\colon\ (a * b) * c = a * (b * c)$$

Un'operazione $*$ definita in un insieme S si dice **commutativa** se vale la proprietà

$$\textit{Per ogni coppia } a, b \textit{ di elementi di } S\colon\ a * b = b * a$$

Un elemento e di S si dice **neutro** per un'operazione $*$ definita in S se per ogni elemento x di S si ha: $x * e = e * x = x$.

Un elemento x' di S si dice **inverso** di un elemento x rispetto ad un'operazione $*$ definita in S e per la quale esista un elemento neutro e se si ha: $x * x' = x' * x = e$.

Dicesi *gruppo* una coppia $(G, *)$ dove G è un insieme non vuoto e $*$ è un'operazione definita in G per cui valgano le proprietà:

1) $*$ è associativa
2) esiste un elemento e di G neutro per $*$
3) ogni elemento g di G ha inverso g' rispetto a $*$.

Un gruppo per cui l'operazione è anche commutativa si dice gruppo *commutativo* o *abeliano*.

Se in un gruppo l'operazione è indicata con il simbolo $+$, diremo che si è adottata la notazione additiva. In questo caso indicheremo con 0 l'elemento neutro e con $-a$ l'inverso dell'elemento a.

Se in un gruppo l'operazione è indicata con il simbolo $\bullet$, diremo che si è adottata la notazione moltiplicativa. In questo caso indicheremo con 1 l'elemento neutro e con a^{-1} l'inverso dell'elemento a.

Facciamo allora alcuni esempi di gruppi e non gruppi.

Esempio 1 La somma ordinaria di numeri interi, per cui si preferisce il simbolo $+$, è una operazione definita nell'insieme $\mathbb{Z}$ dei numeri interi. È associativa, esiste un intero neutro per questa somma, il numero 0, ed ogni intero ha un inverso rispetto a tale operazione. L'inverso di a è il numero $-a$. Pertanto $(\mathbb{Z}, +)$ è un gruppo, il *gruppo additivo degli interi*.

Esempio 2 La somma ordinaria di numeri naturali, per cui si preferisce il simbolo $+$, è una operazione definita nell'insieme $\mathbb{N}$ dei numeri naturali. È associativa, ma non esiste un elemento neutro, a meno che non includiamo 0 in $\mathbb{N}$ (come alcuni fanno). Anche in tale caso però mancano gli inversi. Pertanto $(\mathbb{N}, +)$ non è un gruppo.

Esempio 3 Il prodotto ordinario di numeri interi, per cui si preferisce il simbolo $\bullet$, è una operazione definita nell'insieme $\mathbb{Z}$ dei numeri interi. È associativo, esiste un intero neutro per il prodotto, il numero 1, ma solo 1 e -1 hanno inverso rispetto a $\bullet$. Pertanto $(\mathbb{Z}, \bullet)$ non è un gruppo.

Esempio 4 La somma ordinaria di numeri razionali, per cui si usa il simbolo $+$, è un'operazione associativa definita nell'insieme $\mathbb{Q}$ dei numeri razionali. Per essa 0 è elemento neutro ed ogni razionale a/b ha inverso $-a/b$. Pertanto $(\mathbb{Q}, +)$ è un gruppo, il *gruppo additivo dei razionali*.

Esempio 5 Il prodotto ordinario di numeri razionali, per cui si usa il simbolo $\bullet$, è un'operazione associativa definita nell'insieme $\mathbb{Q}$ dei numeri razionali. Per essa 1 è elemento neutro, però $(\mathbb{Q}, \bullet)$ non è un gruppo. Perché? Perché 0 non ha inverso. Se però "restringiamo" l'operazione di prodotto a $\mathbb{Q} - \{0\}$ (e si può fare perché il prodotto di razionali non nulli è non nullo) si ottiene un gruppo, il *gruppo moltiplicativo dei razionali non nulli*.

Esempio 6 Sia dato un insieme di 4 elementi $S = \{a, b, c, d\}$ con l'operazione $*$ definita dalla tabellina

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	a	b	d
d	d	c	a	b

$(S, *)$ è un gruppo?

Esempio 7 L'insieme delle permutazioni di un insieme non vuoto S costituisce un gruppo rispetto al prodotto di applicazioni. L'elemento neutro è l'applicazione identica.

3. Campi

Un campo è una struttura algebrica con sostegno un insieme K contenente almeno due elementi, e due operazioni interne di cui indichiamo con $+$ la prima (che chiamiamo somma) e con $\bullet$ la seconda (che chiamiamo prodotto), per le quali valgano le seguenti proprietà:

1) $(K, +)$ è un gruppo abeliano
2) il prodotto $\bullet$ è associativo
3) il prodotto $\bullet$ è distributivo rispetto alla somma sia a destra che a sinistra
$$a \bullet (b + c) = a \bullet b + a \bullet c \quad \forall a, b, c \in K$$
$$(b + c) \bullet a = b \bullet a + c \bullet a \quad \forall a, b, c \in K$$
4) esiste in K un elemento, che indichiamo con 1, neutro per il prodotto $\bullet$:
$$1 \bullet a = a \bullet 1 = a \quad \forall a \in K$$
5) ogni elemento a di $K - \{0\}$ è dotato di inverso rispetto al prodotto $\bullet$, che indichiamo con a^{-1}:
$$a \bullet a^{-1} = a^{-1} \bullet a = 1 \quad \forall a \in K - \{0\}$$
6) il prodotto $\bullet$ è commutativo.

4. Esercizi

1. Provare che, qualunque siano gli elementi a e b di un gruppo $(G, +)$, l'equazione $a + x = b$ ammette una, ed una sola, soluzione data da $x = -a + b$. Analogamente l'equazione $x + a = b$ ammette una, ed una sola, soluzione data da $x = b + (-a)$. Dedurre da ciò l'unicità dell'elemento neutro 0 e, per ogni a, l'unicità dell'inverso rispetto a $+$.

2. Dare la versione dell'esercizio 1. quando per l'operazione si è scelta la notazione moltiplicativa.

3. Provare che in un campo $(K; +, \bullet)$, qualunque siano gli elementi a e b con $a \neq 0$, l'equazione $a \bullet x = b$ ammette una, ed una sola, soluzione data da $x = a^{-1} \bullet b$.

4. Provare che, per ogni coppia a e b di elementi di un campo $(K; +, \bullet)$, vale la relazione $(-a) \bullet b = a \bullet (-b) = -(a \bullet b)$.

5. Provare che, per ogni elemento a di un campo $(K; +, \bullet)$, si ha $a \bullet 0 = 0$.

6. Provare che in un campo $(K; +, \bullet)$ vale la legge di annullamento del prodotto:

$$a \neq 0,\ a \bullet b = 0 \implies b = 0$$