STRUTTURE ALGEBRICHE

Una operazione unaria è una operazione che trasforma un elemento di un insieme in un elemento dello stesso, o di un altro, insieme; quindi possiamo identificare una operazione unaria con una funzione.

Una operazione binaria, che denotiamo con # è una operazione che trasforma una coppia di elementi (a,b) in un terzo elemento a # b: (a,b) → a # b

Sia A un insieme. Si dice che l'operazione binaria # è interna ad A, o che è definita in A, se esiste una legge che associa ad ogni coppia (a,b) di elementi di A uno ed un solo elemento a # b appartenente ad A: (a,b) ∈ AxA → a # b ∈ A.

A si dice una struttura algebrica se in A sono definite una o più operazioni interne, e altre eventuali operazioni "in qualche modo" collegate ad A.

Se le operazioni interne sono denotate con i simboli $+, \#, \times, \bullet, \ldots$ scriveremo

$(A, \#, +, \times, \bullet, \ldots)$.

Le strutture algebriche più semplici sono quelle con una, o al massimo due, operazioni interne.

Anelli

Sia (A,+,·) una struttura algebrica con due operazioni binarie interne + e · , che diciamo rispettivamente *addizione* e *moltiplicazione*. A si dice un **anello** se :

1) L'addizione è associativa e commutativa, cioè

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

$a+b=b+a$, $\forall\ a,b \in A$

2) Esiste un elemento neutro per l'addizione, che chiamiamo *zero* e denotiamo con 0, tale che $a+0=0+a=a$, $\forall\ a \in A$

3) $\forall$ a ∈ A , esiste un elemento, che denotiamo con $-a$ e diciamo *opposto* di a, tale che

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

4) La moltiplicazione è associativa e distributiva rispetto alla somma ovvero

$(a\cdot b)\cdot c=a\cdot(b\cdot c)$, $a\cdot(b+c)=a\cdot b+a\cdot c$, $(b+c)a = ba + ca$, $\forall\ a,b,c \in A$

Si dimostra che lo 0 e l'opposto $-a$ di un elemento a, se esistono, sono unici.

Un anello si dice *unitario* se esiste l'elemento neutro per la moltiplicazione, cioè un elemento, che diciamo di solito *unità* e denotiamo col simbolo 1, tale che $a1=1a=a$, $\forall\ a \in A$. L'elemento neutro

per la moltiplicazione si denota a volta anche con altri simboli come i, oppure ι, oppure I. Si dimostra che, se esiste, è unico.

Un anello si dice <u>*commutativo*</u> se vale la proprietà commutativa per il prodotto, ovvero

$ab = ba$, $\forall\, a, b \in A$.

Un anello commutativo unitario si dice un <u>*dominio di integrità*</u> se vale la legge di annullamento del prodotto, ovvero se

$$ab = 0 \Leftrightarrow a=0 \text{ oppure } b=0.$$

Un elemento a si dice <u>*invertibile*</u> in A se esiste in A un elemento, che denotiamo con a^{-1} e diciamo *inverso* di a, tale che $aa^{-1}=a^{-1}a=1$.

Teorema. a) *L'inverso di un elemento, se esiste, è unico.*

Dim. Siano a' e a'' inversi di a. Proviamo che $a' = a''$.

$a' = a' \cdot 1 = a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = 1 \cdot a'' = a''$.

b) *Il prodotto di due elementi invertibili* a *e* b *è invertibile e*

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

Dim. Basta osservare che

$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = 1.$

Analogamente si prova che $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = 1$. Segue $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Esempi

1) L'anello degli interi $(\mathbb{Z}, +, \cdot)$
2) L'anello dei numeri pari $(P, +, \cdot)$
3) L'anello dei polinomi nella indeterminata x, $(\mathbb{R}[x], +, \cdot)$
4) Sia $\mathbb{Z}_n = \{0,1, \dots, n-1\}$, definiamo in $\mathbb{Z}_n$ due operazioni, una di somma, una di prodotto nel modo seguente: a+b= rest(a+b:n), ab = rest(ab:n). Si vede che $(\mathbb{Z}_n, +, \cdot)$ è un anello commutativo unitario, ma non è, in generale, un dominio di integrità. Si dice anello dei resti modulo n.
5) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$

Da ora in poi ometteremo, di solito, il simbolo · e scriveremo semplicemente *ab* invece che *a·b*.

Osservazione: Non è richiesto che l'operazione · sia commutativa!

Proprietà elementari degli anelli

1) $a+b=a+c \Rightarrow b=c$; $b+a=c+a \Rightarrow b=c$ *(leggi di cancellazione)*

Dim. Sia $-a$ l'opposto di a. Allora, applicando le proprietà dell'addizione si ha:

$$a + b = a + c \Rightarrow (-a) + (a + b) = (-a) + (a + c) \Rightarrow [(-a) + a] + b = [(-a) + a] + c$$
$$\Rightarrow 0 + b = 0 + c \Rightarrow b = c$$

L'altra implicazione si dimostra allo stesso modo.

2) $a0 = 0a = 0$, $\forall\, a \in A$

Dim. $a0 + 0 = a0 = a(0 + 0) = a0 + a0 \Rightarrow a0 = 0$ per la legge di cancellazione.
L'altra uguaglianza si dimostra allo stesso modo.

3) $a(-b) = (-a)b = -(ab)$, $\forall\, a, b \in A$

Dim. $ab + (-ab) = 0 = a0 = a[b + (-b)] = ab + a(-b) \Rightarrow a(-b) = -ab$ per la legge di cancellazione. Allo stesso modo si dimostra l'altra uguaglianza.

Osservazione: per la prima delle proprietà elementari degli anelli 0 non è mai invertibile!

Campi

Un anello commutativo unitario $(K,+,\bullet)$ si dice un *campo* se ogni elemento diverso da 0 è invertibile.

Teorema. *In un campo vale la legge di annullamento del prodotto, ovvero*

$ab=0 \Leftrightarrow a=0$ oppure $b=0$.

Dim. La implicazione $\Leftarrow$ segue dalle proprietà elementari degli anelli. Proviamo la implicazione $\Rightarrow$. Sia $ab = 0$. Se $a = 0$ non c'è niente da dimostrare. Sia $a \neq 0$, poiché K è un campo a è invertibile. Sia a^{-1} l'inverso di a. Allora

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow 1b = 0 \Rightarrow b = 0.$$

Esempi.

1) $(R, +, \bullet)$ e $(Q, +, \bullet)$ sono campi, detti rispettivamente campo reale e campo razionale

2) $(Z, +, \bullet)$ è un anello commutativo unitario, è un dominio di integrità, ma non è un campo. Gli unici elementi invertibili sono 1 e -1.

3) L'anello dei numeri pari non è un anello unitario, 1 non è un numero pari.

4) $(C, +, \cdot)$ è un campo, detto campo complesso. Le operazioni di addizione e moltiplicazione sono definite nel modo seguente:

$(a+ib) + (c+id) = (a+c) + i(b+d)$

$(a+ib)(c+id) = (ac-bd) + i(ad+bc)$

5) $(\mathbb{Z}_n, +, \cdot)$ è un campo se e solo se n = p è un numero primo.

6) Sia $R[x]$ l'insieme dei polinomi nella indeterminata x con le ordinarie operazioni di somma e prodotto di polinomi, allora $R[x]$ è un anello unitario, ma non è un campo. L'elemento neutro

rispetto alla somma è 0, l'elemento neutro rispetto al prodotto è 1. Se f(x) e g(x) sono polinomi di grado m ed n rispettivamente il polinomio f(x)g(x) ha grado m+n, quindi nessun polinomio di grado maggiore di 0 è invertibile, se f(x) è un polinomio di grado maggiore di 0, 1/f(x) esiste ma non è un polinomio, quindi non appartiene a R[x].

L'anello dei resti modulo n

Sia $n \in N$ un numero naturale positivo e $Z_n = \{0,1, \dots , n-1\}$ l'insieme dei possibili resti della divisione per n. Si definiscono in Z_n una operazione di somma ed una di prodotto nel modo seguente.

Se a e b $\in Z_n$ si definiscono

$$a+b = \text{rest } (a+b:n) \quad \text{e} \quad ab = \text{rest } (ab:n).$$

Si vede che $(Z_n,+,\cdot)$ è un anello commutative unitario. Se n non è un numero primo allora $(Z_n, + \cdot)$ non è un dominio di integrità, per esempio in Z_6 risulta $2\cdot3=0$, in Z_8 risulta $2\cdot4=0$.

Se n=p è un numero primo allora $(Z_p,+,\cdot)$ è un campo, cioè ogni elemento diverso da 0 è invertibile.

Esempi ed esercizi

1) Determinare l'opposto di un elemento a $\in Z_n$ significa determinare in Z_n l'unica soluzione dell'equazione x+a=a+x=0.

   Esercizio. Determinare in Z_5 l'opposto di 2.

   Sol. Bisogna determinare in Z_5 l'unica soluzione dell'equazione 2+x=0 che è 3, infatti in Z_5 risulta 2+3=0.

2) Determinare l'inverso di un elemento a $\in Z_n$ significa trovare in Z_n una soluzione (se esiste è unica) dell'equazione $a\cdot x=1$.

   Esercizio. Determinare in Z_6 l'inverso, se esiste, di 2 e 5.

   Sol. L'equazione 2x=1 non ha soluzioni in Z_6 infatti $2\cdot1=2$, $2\cdot2=4$, $2\cdot3=0$, $2\cdot4=2$, $2\cdot5=4$, quindi 2 non è invertibile. Si noti anche che da quanto scritto segue che l'equazione 2x=2 ha due soluzioni, x=1 e x=4.

   L'equazione 5x=1 ha soluzione in Z_6 ed è x=5, infatti $5\cdot5=1$ in Z_6.

3) Esercizio. Per quanto detto precedentemente $(Z_7,+,\cdot)$ è un campo. Determinare gli opposti e gli inversi di tutti gli elementi di Z_7 diversi da zero.

Matrici quadrate di ordine 2

Denotiamo con M_2 l'insieme delle matrici quadrate di ordine 2 ad elementi reali. Quindi

$$M_2 = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in R \} .$$

Somma di matrici

Le matrici si denotano con le lettere latine maiuscole.
Definiamo in M_2 una operazione di somma nel modo seguente:

$$\text{se } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ e } B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \text{ allora } A+B = \begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix}.$$

In altri termini A+B è la matrice che si ottiene sommando gli elementi di ugual posto.
L'operazione + così definita in M_2 è evidentemente una operazione binaria interna.
Si vede facilmente che l'operazione è associativa e commutativa, ovvero se A, B e C sono elementi qualsiasi di M_2 allora risulta A+(B+C) = (A+B)+C e A+B=B+A.
Esiste l'elemento neutro: la matrice $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ è tale che A+O =O+A =A, qualunque sia A in M_2.
O si dice matrice nulla. Data la matrice $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ la matrice $-A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$ è tale che A+(-A)=(-A)+A=O , -A si dice opposta di A.

Prodotto (righe per colonne) di matrici

Se $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ e $B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ allora si definisce $A \cdot B = \begin{bmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix}$. L'operazione · così definita è una operazione binaria interna in M_2. Si dimostra (ma i calcoli sono estremamente noiosi) che valgono le seguenti proprietà:

1) proprietà associativa: A(BC)=(AB)C, qualunque siano A, B e C in M_2;
2) proprietà distributiva del prodotto rispetto alla somma: A(B+C)=AB+AC e (B+C)A=BA+CA, qualunque siano A, B, C in M_2.

L'anello delle matrici quadrate di ordine 2

Dalle osservazioni precedenti segue subito che $(M_2, +, \cdot)$ è un anello, che si dice anello delle matrici quadrate di ordine 2 sul campo reale.

M_2 è un anello non commutativo. Consideriamo, ad esempio, le matrici $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ risulta
$AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = B$, $BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O$. Se AB = BA le matrici A e B si dicono permutabili.
Dall'esempio si nota anche che non vale la legge di annullamento del prodotto.

Esercizio. Data la matrice $C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, verificare che:

a) $A = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$ è permutabile con C, $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ non è permutabile con C.
b) $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ è permutabile con C se e solo se c=0 e a = d.

M_2 è un anello unitario. Si vede facilmente che se $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ è una qualunque matrice e $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ risulta A·I=I·A=A. I si dice matrice unità.

Matrici invertibili

Ricordiamo definizione e proprietà degli elementi invertibili di un anello unitario, con riferimento alle matrici.

1) A si dice invertibile se esiste una matrice $A' \in M_2$ tale che $A \cdot A' = A' \cdot A = I$.

2) O non è invertibile, I è invertibile.
3) A' , se esiste, è unica, si denota con A^{-1}, e si dice inversa di A.
4) Il prodotto di due matrici invertibili A e B è invertibile e $(AB)^{-1}= B^{-1}A^{-1}$.

Esempi. La matrice $A = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ non è invertibile, la matrice $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ è invertibile.

Il nostro prossimo obiettivo è riconoscere facilmente se una matrice è invertibile oppure no, e, in caso di risposta positiva, trovare un modo facile per determinare l'inversa.

Determinante di una matrice e applicazioni

Sia $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, si dice determinante di A, e si denota con |A| o $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$, il numero reale

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Sia $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, diciamo aggiunta di A, e denotiamo con A*, la matrice

$$A^* = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Si vede facilmente che:

a) $A \cdot A^* = A^* \cdot A = \begin{bmatrix} |A| & 0 \\ 0 & |A| \end{bmatrix}$
b) Se |A|=0 allora $A \cdot A^* = A^* \cdot A = O$.
c) Se $|A| \neq 0$ allora A è invertibile e $A^{-1} = \begin{bmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{bmatrix}$.
d) Se |A| = 0 allora A non è invertibile.

Dim. Se A = O allora A non è invertibile. Sia $A \neq O$. Neghiamo la tesi e supponiamo, per assurdo, che |A|=0 e A sia invertibile, sia A^{-1} l'inversa di A , allora :
$A \cdot A^* = O \Rightarrow A^{-1}(A \cdot A^*) = A^{-1} \cdot O \Rightarrow (A^{-1} A) \cdot A^* = O \Rightarrow I A^* = O \Rightarrow A^* = O \Rightarrow A = O$
una contraddizione.