Strutture algebriche fondamentali

Sia G un qualsiasi insieme di elementi a,b,c,… Definiamo operazione binaria o legge di composizione interna in G qualsiasi legge che associa ad ogni coppia ordinata (a,b) di elementi di G un unico elemento c dello stesso insieme G.
Indicando con $*$ una generica operazione binaria in G, avremo:

$a*b=c$ od anche

$*:(a,b)\longrightarrow c$

Si dice anche che G è chiuso rispetto alla operazione $*$.

Proprietà associativa

L'operazione $*$ gode della proprietà associativa se

$\forall a,b,c\in G \qquad a*(b*c)=(a*b)*c$

Elemento neutro

Un elemento *e* di G è chiamato elemento neutro se

$\forall a\in G \qquad e*a=a*e=a$

Se G possiede un elemento neutro, esso è unico.
Supponiamo per assurdo che esistano due elementi neutri e ed e' distinti.
Essendo e elemento neutro avremo:

$e*e'=e'*e=e'$

Inoltre se e' è elemento neutro avremo:

$e'*e=e*e'=e$

per cui dovrà essere

$e=e'$

Pertanto è impossibile che esistano due elementi neutri tra loro distinti.

Elemento inverso o simmetrico

Se $a\in G$ un inverso di a è un elemento $a'\in G$ tale che

$a'*a=a*a'=e$

Se a'' è un altro inverso di *a* si avrà

$a''=a''*e=a''*(a*a')=(a''*a)*a'=e*a'=a'$

pertanto l'inverso di a, se esiste, è unico.

Proprietà commutativa

L'operazione $*$ gode della proprietà commutativa se

$a*b=b*a$

Proprietà distributiva

Diciamo che la legge $\circ$ gode della proprietà distributiva rispetto alla legge $*$ se

$\forall a,b,c\in G$ si ha $a\circ(b*c)=(a\circ b)*(a\circ c)$

Legge di composizione esterna

Si dice legge di composizione esterna fra elementi di un insieme di operatori o scalari L e di un insieme E, un'applicazione di un sottoinsieme di $L\times E$ in E.
Se il suo dominio è $L\times E$ si dice ovunque definita.
Il risultato della composizione di $\alpha\in L$ ed $a\in E$ è il seguente

$b=\alpha\circ a$

Strutture algebriche

Un insieme A dotato di leggi di composizione interna prende il nome di struttura algebrica.
L'insieme A si dice sostegno della struttura. Si indica $(A;*,\circ,\bullet)$.

Monoide
Definiamo monoide o semigruppo una struttura algebrica $(A;*)$ la cui operazione è associativa (altri definiscono monoide una struttura algebrica che gode della proprietà associativa ed è dotata di elemento neutro)

Gruppi
Dicesi gruppo un insieme non vuoto $(G;*)$ dotato di un'operazione interna binaria che gode delle seguenti proprietà.
i) proprietà associativa
$\forall a,b,c \in G \qquad a*(b*c)=(a*b)*c$
ii) esistenza dell'elemento neutro
$\forall a \in G \qquad e*a=a*e=a$
iii) esistenza dell'elemento simmetrico
$\forall a \in G\ \exists\, a' : a*a'=a'*a=e$
Se inoltre l'operazione $*$ è commutativa il gruppo si dice commutativo o abeliano (dal nome del matematico norvegese Niels Erik Abel)
Sottogruppi
Sia $(G;*)$ un gruppo ed S un sottoinsieme non vuoto di G. Se S è un gruppo rispetto alla stessa operazione di G, diremo che $(S;*)$ è un sottogruppo di $(G;*)$.
Proprietà fondamentali dei gruppi
Teorema 1
In un gruppo $(G;*)$ valgono le leggi di cancellazione a sinistra e a destra.
Cancellazione a sinistra
$x*a=x*b \Rightarrow a=b \qquad \forall a,b,x \in G$
Cancellazione a destra
$a*x=b*x \Rightarrow a=b \qquad \forall a,b,x \in G$
La distinzione fra cancellazione a sinistra e a destra deriva dal fatto che l'operazione può non essere commutativa.
Se $x \in G$ esiste il suo simmetrico x' tale che
$x*x'=e$
Essendo per ipotesi
$x*a=x*b$
moltiplichiamo a sinistra per x'
$x'*(x*a)=x'*(x*b)$
essendo l'operazione associativa avremo
$(x'*x)*a=(x'*x)*b$
essendo $x*x'=e$ otteniamo
$e*a=e*b$ e quindi
$a=b$
In modo analogo si dimostra la regola di cancellazione a destra.
Teorema 2
In un gruppo ogni elemento ha un solo simmetrico.
Sia $x \in G$, supponiamo per assurdo che esistano due elementi simmetrici distinti di x, siano essi x ed x'
Essendo x' simmetrico di x si ha
$x*x'=e$
essendo x'' simmetrico di x si ha
$x*x''=e$

quindi

$x * x' = x * x''$

per la regola di cancellazione a sinistra avremo

$x = x'$

contro l'ipotesi che $x \neq x'$

Quindi si ha un assurdo e dovrà essere $x = x'$

Anelli

Sia A un insieme non vuoto in cui siano definite due leggi di composizione interne $*$ e $\circ$.

Si dice che $(A;*,\circ)$ è un anello se sono verificati i seguenti assiomi

1) A è un gruppo abeliano rispetto all'operazione $*$
2) La legge $\circ$ è associativa
3) La legge $\circ$ è distributiva a destra e a sinistra rispetto all'operazione $*$

Elencando per esteso le proprietà formali avremo:

Per l'operazione $*$

1) proprietà associativa

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

2) $\exists$ l'elemento neutro

$\forall a \in G \; \exists e: \quad e*a = a*e = a$

3) $\exists$ l'elemento simmetrico

$\forall a \in A \; \exists a' \in A: a'*a = a*a' = e$

4) proprietà commutativa

$\forall a \in A \qquad a*b = b*a$

Per l'operazione $\circ$

5) proprietà associativa

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

6) proprietà distributive

$\forall a,b,c \in A \qquad a \circ (b*c) = (a \circ b)*(a \circ c)$

$(b*c) \circ a = (b \circ a)*(c \circ a)$

Se la legge $\circ$ è commutativa l'anello si dice commutativo o abeliano.

Se esiste l'elemento neutro rispetto all'operazione $\circ$ l'anello si dice unitario o con unità.

Esempi di anelli:

a) l'insieme dei numeri razionali $(\mathbb{Q};+,\bullet)$ è un anello commutativo unitario;
b) l'insieme degli interi relativi $(\mathbb{Z};+,\bullet)$
c) l'insieme dei numeri reali $(\mathbb{R};+,\bullet)$ ecc..

Corpi e campi

Una struttura algebrica $(A;*,\circ)$ viene chiamata corpo se sono verificati i seguenti assiomi.

1) la struttura $(A;*)$ è un gruppo abeliano;
2) la struttura $(A-\{0\};\circ)$ è un gruppo;
3) valgono le leggi distributive dell'operazione $\circ$ rispetto alla $*$.

Se vale la proprietà commutativa dell'operazione $\circ$ la struttura si dice campo.