STRUTTURE ALGEBRICHE

OPERAZIONE INTERNA SU UN INSIEME

Dato l'insieme A, la funzione φ: $A \times A \to A$ è detta *operazione interna*; denotiamo $\varphi(a,b) = a \oplus b$

$\forall\ a, b, c$ appartenenti ad A:

L'operazione $\oplus$ si dice: *associativa* se $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
commutativa se $a \oplus b = b \oplus a$

L'elemento $e \in A$ si dice *elemento neutro* per $\oplus$ se $\forall a$ vale $a \oplus e = e \oplus a = a$.

L'elemento $a' \in A$ si dice *simmetrico* di a rispetto a $\oplus$ se $\exists\ a' \in A$ tale che $a \oplus a' = a' \oplus a = e$.

L'elemento $r \in A$ si dice *regolare* rispetto a $\oplus$ se $r \oplus a = r \oplus b$, $a \oplus r = b \oplus r \Leftrightarrow a = b$

L'elemento $s \in A$ si dice *singolare* rispetto a $\oplus$ se $s \oplus a = a \oplus s = s$.

L'operazione ® si dice *distributiva* rispetto a $\oplus$ se a ® $(b \oplus c) = (a$ ® $b) \oplus (a$ ® $c)$

GRUPPOIDI E SEMIGRUPPI

Un insieme G e un'operazione interna $\oplus$ ad esso associata definiscono la struttura $(G,\oplus)$ detta *gruppoide.*

Se $\oplus$ è associativa la struttura è un *semigruppo*.

Se $\oplus$ è anche commutativa il gruppoide e il semigruppo si dicono *commutativi* (o *abeliani*)

MONOIDI

La struttura $(G,\oplus)$ è detta *monoide* se $\oplus$ è associativa ed esiste l'elemento neutro e di $\oplus$

Se $\oplus$ è anche commutativa il monoide si dice *commutativo* (o *abeliano*)

GRUPPI

La struttura $(G,\oplus)$ è detta *gruppo* se valgono le seguenti proprietà:

- $\oplus$ è associativa.
- esiste l'elemento neutro e di $\oplus$
- esiste il simmetrico rispetto a $\oplus$

Se $\oplus$ è anche commutativa il gruppo si dice *commutativo* (o *abeliano*).

Proprietà dei gruppi:
- $\forall x \in G$, x è regolare.
- $\forall x \in G$, x' è il simmetrico di $x \Rightarrow \forall a,b \in G$, $(a \oplus b)' = b' \oplus a'$
- $a,b \in G$, valgono: $a \oplus x = b \Rightarrow x = a' \oplus b$, $x \oplus a = b \Rightarrow x = b \oplus a'$
- $\forall a \in G$, f: $G \to G$ con $f(x) = a \oplus x \Rightarrow$ f è biettiva.

SOTTOGRUPPI E CLASSI LATERALI

Dati il gruppo $(G,\oplus)$ e l'insieme $S \subseteq G$, $(S,\oplus)$ si dice *parte stabile* di G se S è chiuso rispetto a $\oplus$.

Dati il gruppo $(G,\oplus)$ e l'insieme $S \subseteq G$, $(S,\oplus)$ si dice *sottogruppo* di G se S è chiuso rispetto a $\oplus$, S contiene l'elemento neutro di G e $\forall x \in S$ esiste il suo simmetrico rispetto a $\oplus$.

Dati il gruppo $(G,\oplus)$ e il suo sottogruppo $(S,\oplus)$ si dicono

Un sottogruppo si dice *normale* se le sue classi laterali destre coincidono con le sinistre.

Se il gruppo $(G,\oplus)$ è commutativo ogni sottogruppo è normale.

ANELLI

Un insieme A e due operazioni interne $\oplus$ e $\otimes$ ad esso associate definiscono la struttura $(A,\oplus,\otimes)$ detta *anello* se:

- $(A,\oplus)$ è un gruppo commutativo
- $(A,\otimes)$ è un semigruppo
- vale la proprietà distributiva di $\otimes$ rispetto a $\oplus$.

Se il semigruppo $(A,\otimes)$ è commutativo, l'anello si dice *commutativo.*

Se $(A,\otimes)$ è un monoide, l'anello si dice *unitario.*

L'anello $(A,\oplus,\otimes)$ contiene: 0 (elemento neutro rispetto a $\oplus$)
$-a$ (simmetrico di a rispetto a $\oplus$)
1 (elemento neutro rispetto a $\otimes$)

L'elemento a si dice *unitario* se $a' \otimes a = a \otimes a' = 1$

Dati $a,b \neq 0$, a e b si dicono *divisori dello zero* se $a \otimes b = 0$ oppure $b \otimes a = 0$

Un anello commutativo privo di divisori dello zero è detto *anello d'integrità*.

Proprietà di un anello:
- $\forall a \in A$, $a \otimes 0 = 0 \otimes a = 0$
- $\forall a,b \in A$, $a \oplus (-b) = (-a) \oplus b = -(a \oplus b)'$
- $\forall a,b \in A$, $(-a) \oplus (-b) = a \oplus b$

SOTTOANELLI E IDEALI
Dati L'anello $(A,\oplus,\otimes)$ e l'insieme $S \subseteq A$, $(S,\oplus,\otimes)$ si dice *sottoanello* di A se:
- $(S,\oplus)$ è sottogruppo del gruppo $(A,\oplus)$
- $(S,\otimes)$ è parte stabile di $(A,\otimes)$

Il sottoanello $(I,\oplus,\otimes)$ si dice *ideale* dell'anello A se $\forall a \in A$, $\forall i \in I$ vale $(i \otimes a)$ et $(a \otimes i) \in I$

CORPI E CAMPI
L'insieme K è detto *corpo* rispetto alle operazioni interne $\oplus$ e $\otimes$ se:
- K è un gruppo commutativo rispetto a $\oplus$.
- $K \setminus \{e\}$ è un gruppo rispetto a $\otimes$ (dove e = elemento neutro per $\oplus$).
- vale la proprietà distributiva di $\otimes$ rispetto a $\oplus$. $\forall a,b,c \in K$, $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Se $\otimes$ è anche commutativa, K si dice corpo commutativo (o *campo*).

Proprietà di un corpo K:
1. $\forall a \in K$, $a \otimes e = e \otimes a = e$
2. $\otimes$ è associativa
3. $\forall a,b \in K$, $a \otimes b = e \Rightarrow a = e$ oppure $b = e$ oppure entrambi
4. $\forall a,b \in K$, $a' \oplus b = a \oplus b' = (a \oplus b)'$; $a' \oplus b' = a \oplus b$
5. $\forall a \in K$, $a \neq e$, $(a')'' = (a'')'$