

**Algebra. Corso di Laurea in Informatica.
Canale 1. Prof. P. Piazza. a.a. 2023-24.**

Semigrupperi, gruppi, anelli, campi.

Definizione 1. Un semigruppero (S, \star) è un insieme dotato di un'operazione¹ \star verificante le seguenti proprietà:

- (1) l'operazione è associativa: $\forall s_1, s_2, s_3 \in S$, si ha $(s_1 \star s_2) \star s_3 = s_1 \star (s_2 \star s_3)$
- (2) esiste un elemento $e \in G$ tale che $s \star e = s = e \star s \forall s \in S$

Se accade che

- (4) $g_1 \star g_2 = g_2 \star g_1 \forall g_1, g_2 \in G$, il semigruppero è detto *commutativo* o anche *abeliano*.

Osservazione. Abbiamo verificato in classe che l'elemento e di cui in (2) è unico. Tale elemento è detto *elemento neutro*.

Esempi.

1. $(\mathbb{N}, +)$ con elemento neutro 0 è un semigruppero commutativo.
2. Sia X un insieme, e sia $S = \{f : X \rightarrow X, f \text{ applicazione}\}$. Sia id_X l'applicazione che associa a $x \in X$ l'elemento x : $\text{id}_X(x) = x$. Dotiamo S di un'operazione ponendo²

$$f \star g := f \circ g$$

dove \circ denota la composizione di applicazioni. La coppia (S, \star) è un semigruppero; l'associatività è una nota proprietà della composizione; l'elemento neutro è l'applicazione Id_X . Questo semigruppero non è, in generale, commutativo.

Definizione 2. Un gruppo (G, \star) è un insieme dotato di un'operazione \star verificante le seguenti proprietà:

- (1) l'operazione è associativa: $\forall g_1, g_2, g_3 \in G$, si ha $(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3)$
- (2) esiste un elemento $e \in G$ tale che $g \star e = g = e \star g \forall g \in G$
- (3) $\forall g \in G \exists g' \in G$ tale che $g \star g' = e = g' \star g$.

Se accade che

- (4) $g_1 \star g_2 = g_2 \star g_1 \forall g_1, g_2 \in G$, il gruppo è detto *commutativo* o anche *abeliano*.

Esercizio 1. Verificare che dato $g \in G$, l'elemento g' di cui in (3) è unico. Esso è detto *inverso di g* ed è denotato g^{-1} .

Suggerimento: assumete che ce ne siano due e dimostrate che devono essere uguali.

Esercizio 2. Verificare che $(g \star h)^{-1} = h^{-1} \star g^{-1} \forall g, h \in G$.

Suggerimento: utilizzate l'unicità dell'inverso.

Notazioni semplificate. L'elemento neutro e viene spesso denotato con il simbolo 1 (con abuso di notazione; qui 1 è un elemento del gruppo G e **non** il numero 1). Inoltre l'operazione è spesso denotata semplicemente con \cdot (di nuovo, questa **non** è l'usuale operazione di moltiplicazione fra numeri ma un'applicazione $\cdot : G \times G \rightarrow G$). In un gruppo commutativo, si utilizza usualmente la notazione $+$ per denotare l'operazione; inoltre l'elemento neutro è spesso denotato con il simbolo 0 mentre

¹Un'operazione è una legge che associa ad ogni coppia ordinata di elementi di S , siano essi s_1, s_2 , uno ed un solo elemento di S , denotato $s_1 \star s_2$. Un'operazione è quindi un'applicazione $\star : G \times G \rightarrow G$

²il simbolo $:=$ viene utilizzato per definire un oggetto matematico con ciò che compare a destra di questo simbolo; si legge "uguale per definizione a"

l'inverso è denotato con il simbolo $-a$ ed è chiamato *opposto*. Ancora una volta, questi sono tutti abusi di notazione³ ma sono largamente utilizzati nei testi. Li utilizzeremo anche noi in quanto segue.

Esempio 3. L'insieme dei numeri interi $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\rho$ con l'operazione di somma vista a lezione è un gruppo commutativo, con elemento neutro il numero $0 = [(0, 0)]$ e opposto di $k \equiv [(k, 0)] \in \mathbb{N} \equiv \mathbb{Z}^+ \subset \mathbb{Z}$ uguale a $-k \equiv [(0, k)]$ e opposto di $-\ell = [0, \ell] \in \mathbb{Z}^-$, $\ell \in \mathbb{N}$, uguale a $\ell = [(\ell, 0)]$.

Esempio 4. Sia X un qualsiasi insieme e sia $G = \{f : X \rightarrow X, f \text{ biunivoca}\}$. Come nell'esempio 2 dotiamo G di un'operazione ponendo $f \cdot g := f \circ g$. La coppia (G, \cdot) è un gruppo con l'inverso di f uguale all'applicazione inversa f^{-1} . Qui sto utilizzando una nota proprietà della funzione inversa di f (applicazione biunivoca di X in X) e cioè che

$$f \circ f^{-1} = \text{Id}_X \quad f^{-1} \circ f = \text{Id}_X .$$

Questo gruppo **non** è, in generale, commutativo.

Definizione 3. Un anello $(A, +, \cdot)$ è un insieme dotato di due operazioni, denotate $+$ e \cdot , con le seguenti proprietà:

- (1) $(A, +)$ è un gruppo commutativo, con elemento neutro rispetto a $+$ denotato 0 .
- (2) l'operazione \cdot gode della proprietà associativa.
- (3) valgono le proprietà distributive:

$$(a + a') \cdot b = a \cdot b + a' \cdot b, \quad a \cdot (b + b') = a \cdot b + a \cdot b'. \quad \forall a, a', b, b' \in A$$

Notare che stiamo seguendo le notazioni semplificate.

Se vale la proprietà commutativa per l'operazione \cdot allora $(A, +, \cdot)$ è detto un *anello commutativo*.

Se esiste un elemento neutro rispetto all'operazione \cdot , denotato usualmente con il simbolo 1 , allora A è un anello *unitario*.

Se $(A, +, \cdot)$ è un anello commutativo unitario allora esso è detto un dominio di integrità se

$$a \cdot b = 0 \Rightarrow a = 0 \text{ oppure } b = 0 .$$

Esempio 5. $(\mathbb{Z}, +, \cdot)$, l'insieme dei numeri interi con le usuali operazioni di somma e prodotto, è un anello commutativo unitario. Esso è anche un dominio di integrità. Vedremo altri esempi durante il corso.

³ad esempio, 0 è un elemento del gruppo e non il numero 0 ; similmente, la notazione $+$ denota l'operazione nel gruppo commutativo G e non, in generale, la somma fra numeri