Lezione 01 - 29/09/2022

Operazione binaria

Un'operazione binaria $*$ su un insieme S è un'applicazione:

$$\begin{gathered} * : S \times S \to S \\ (a, b) \mapsto a * b \end{gathered}$$

Monoide

Un insieme S dotato di **un'operazione binaria** in cui valgono le proprietà di **associatività** e **esistenza dell'elemento neutro** si dice **MONOIDE**.

- **Proprietà associativa**

$$(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$$

- **Esistenza elemento neutro**

$$\exists e \in S : e * a = a * e = a \quad \forall a \in S$$

Es.:

- $(\mathbb{N}, +)$, con elemento neutro $e = 0$
- $(\mathbb{N}, \cdot)$, con elemento neutro $e = 1$

Più in generale ogni insieme X nella lista

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

rispetto a $+$ o rispetto a $\cdot$ è un monoide.

Lemma - L'elemento neutro è unico

In un monoide S l'elemento neutro è unico

Dimostrazione: Siano e_1, e_2 due elementi neutri

$$e * a \overset{(1)}{=} a * e \overset{(2)}{=} a$$
$$e_1 \overset{(1)}{=} e_1 * e_2 \overset{(2)}{=} e_2$$

Dove, nella seconda equazione:

- Nel primo passaggio vengono posti: $a = e_1$ e $e = e_2$
- Nel secondo passaggio vengono posti: $a = e_2$ e $e = e_1$

Monoide commutativo

Un monoide si dice **commutativo** se

$$a * b = b * a \quad \forall a, b \in S$$

Es.:

X insieme, $F_X = \{f : X \to X\}$ e $f * g = f \circ g$ si ha che

$$(f \circ g) = f(g(x))$$

F_X è un **monoide** perché la composizione di funzioni è associativa. L'elemento neutro è:

$$\mathrm{Id}_x(x) = x \quad \forall x \in X$$

Infatti:

$$f \circ \mathrm{Id}_x = \mathrm{Id}_x \circ f = f$$

Es.:

$$(f \circ \mathrm{Id}_x)(x) = f(\mathrm{Id}_x(x)) = f(x)$$
$$(\mathrm{Id}_x \circ f)(x) = \mathrm{Id}_x(f(x)) = f(x)$$

Gruppo e gruppo abeliano

Un **monoide** $(G, *)$ si dice **GRUPPO** se

$$\forall g \in G \; \exists g' \in G : g * g' = g' * g = e$$

Ovvero g' è l'**elemento inverso** di g.

Se G è **commutativo**, diciamo anche che è un **GRUPPO ABELIANO**.
Es.:

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{Q} \setminus \{0\}, \cdot)$

Esempio: Sia $F_x \supset S_x = \{f : X \to X, \text{ f biiettiva}\}$

Biiettiva siginifica che: $\exists g : X \to X \text{ t.c. } f \circ g = g \circ f = \mathrm{Id}_X$

$$f^{-1}(B) = \{x \in X | f(x) = B\}$$

Prendiamo:

- f biunivoca
- $B = \{y\}$

Si ha che $f^{-1}(y)$ ha un solo elemento.

Notazione - gruppo simmetrico

S_n è un gruppo simmetrico su $X = \{1, 2, ..., n\}$, dove S_n indica le permutazioni su $\{1, 2, ..., n\}$

Lemma - Inverso unico

In un gruppo G l'inverso di ogni elemento è unico

Dimostrazione: supponiamo che g_1, g_2 siano entrambi inversi di g, per ipotesi

$$g * g_1 = g_1 * g = e$$
$$g * g_2 = g_2 * g = e$$

Si avrà la seguente cosa:

$$g_1 = g_2 * e = g_1 * (g * g_2) \overset{assoc.}{=} (g_1 * g) * g_2 = e * g_2 = g_2$$

Anello, anello commutativo con unità e campo

Un anello con unità R è un insieme dotato di due operazioni binarie $+$ e $\cdot$ tali che:

1. $(R, +)$ è un **gruppo abeliano**,
2. $(R, \cdot)$ è un **monoide**

Valgono le proprietà distributive:

$$\begin{aligned} (a+b)c = ac + bc \quad \forall a, b, c \in R \\ a(b+c) = ab + ac \quad \forall a, b, c \in R \end{aligned}$$

Se $(R, \cdot)$ è un **monoide commutativo**, diciamo che R è un **anello commutativo con unità**.
Es.:

- $(\mathbb{Z}, +, \cdot)$

Se $(R \setminus \{0\}, \cdot)$ è un **gruppo abeliano**, diciamo che R è un **campo**.
Es.:

- $(\mathbb{Q}, +, \cdot)$
- $(\mathbb{R}, +, \cdot)$

In un anello $0 \cdot a = 0, \forall a \in R$, infatti:

$$\begin{aligned} 0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a \\ (-0 \cdot a) + 0 \cdot a = (-0 \cdot a) + (0 \cdot a + 0 \cdot a) \\ 0 = (-0 \cdot a + 0 \cdot a) + 0 \cdot a \\ 0 = 0 + 0 \cdot a \\ 0 = 0 \cdot a \end{aligned}$$