2 Definizioni ed Esempi di Strutture Algebriche

Nel seguito del corso tratterò in linea di massima due strutture: gli interi e i polinomi. Conviene fissare sin da ora alcune definizioni che utilizzerò in maniera non troppo formale nel seguito.

Definizione 2.1 *Sia M un insieme. Una funzione $f : M \times M = M^2 \to M$ viene detta una* ***operazione binaria*** *su M.*

1. *M si dice* ***semigruppo*** *se esiste un'operazione binaria, di solito chiamata prodotto e si usa scrivere $a \cdot b$ invece di $\cdot(a, b)$, associativa, ossia $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;*
2. *M diventa* ***monoide*** *se esiste 1_M tale che $a \cdot 1_M = a = 1_M \cdot a$ per ogni $a \in M$ - 1_M viene detto l'****elemento neutro*** *di M;*
3. *diventa* ***gruppo*** *se per ogni a esiste a^{-1} tale che $a \cdot a^{-1} = a^{-1} \cdot a = 1_M$, tale elemento dicesi* ***inverso*** *di a;*
4. *un gruppo G si dice* ***ciclico*** *se esiste $a \in G$ tale che $G = \{a^k : k \in \mathbb{Z}\}$ - a viene detto un* ***generatore*** *di G;*
5. *un monoide M si dice* ***abeliano*** *se il prodotto è commutativo, ossia $a \cdot b = b \cdot a$, per ogni $a, b \in M$.*

Se l'operazione è commutativa la si chiama solitamente somma. Questa viene denotata con $+$, l'elemento neutro si scrive 0_M, l'inverso di a viene detto **opposto** e indicato con $-a$.

Esercizio 2.2 *Scrivere in dettaglio la definizione di 0_M e di opposto.*

Esercizio 2.3 *Dimostrare che un gruppo ciclico è abeliano. Esibire gruppi abeliani che non sono ciclici.*

Definizione 2.4 *Sia A un gruppo abeliano rispetto alla somma. Allora viene detto un* ***anello*** *se*

1. *A è un monoide rispetto al prodotto. In particolare esiste 1_A tale che $a \cdot 1_a = 1_A \cdot a = a$;*
2. *valgono le leggi distributive del prodotto rispetto alla somma, ossia*
$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a;$$
3. *se il prodotto è commutativo si dice che l'anello è commutativo;*
4. *se inoltre per ogni $a \neq 0_M$ esiste a^{-1}. In tal caso A viene detto* ***campo****.*

Esercizio 2.5 *Sia A un anello. Manipolando $(0_A + 0_A) \cdot a$, provate che $0_A \cdot a = 0_A$ per ogni $a \in A$. Dedurre che 0_A non ammette (quasi) mai inverso. Perché scrivo (quasi)?*

È buona cosa avere esempi di queste definizioni.

Esempio 2.6 *1.* $\mathbb{N}$ *rispetto alla somma è un monoide;*

2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *rispetto alla somma sono gruppi abeliani;*
3. $\mathbb{Z}$ *rispetto alla somma è gruppo ciclico;*
4. $\mathbb{R}^n$ *rispetto alla somma di vettori è un gruppo abeliano;*
5. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *sono campi*
6. $Mat_n(\mathbb{R})$ *le matrici quadrate di ordine* n *su* $\mathbb{R}$ *sono un anello, non commutativo se* $n > 1$*;*
7. B_n *è un anello commutativo;*
8. $\mu_n = \{\exp(\frac{2\pi\iota k}{n}) : k \in \mathbb{Z}\}$ *è un gruppo ciclico.*
9. $\mathbb{R}[x]$ *l'insieme dei polinomi a coefficienti reali è un anello commutativo;*
10. $\mathbb{R}[[x]]$ *l'insieme delle serie di potenze a coefficienti reali è un anello commutativo;*

Esercizio 2.7 *Mostrare che* $|\mu_n| = n$*. Determinare tutti i generatori di* μ_n*.*

Ricordo che negli ultimi due esempi la somma avviene componente per componente, ossia

$$\sum_i a_i x^i + \sum_k b_k x^k = \sum_j (a_j + b_j) x^j.$$

È giusto chiamare j l'indice nella somma a destra?

Invece il prodotto non è definito come $\sum_i a_i b_i x^i$ (questo introduce un'operazione poco interessante ciononostante meritevole di un nome, ossia **prodotto di Hadamard**) ma come

$$\sum_i a_i x^i * \sum_k b_k x^k = \sum_j c_j x^j,$$

ove $c_j = \sum_{i+k=j} a_i b_k$ è definito mediante una somma che coinvolge un numero finito di addendi e chiamato anche prodotto di **convoluzione** o di **Cauchy**.