0.1 Anelli

Definizione 1. Sia A un insieme non vuoto, e siano

$$+ : A \times A \to A \qquad \cdot : A \times A \to A$$

due leggi di composizione interne su A. Si dice che la terna ordinata $(A, +, \cdot)$ è un *anello* se:

(A_1) $(A, +)$ è un gruppo abeliano

(A_2) $(A, \cdot)$ è una struttura associativa

(A_3) valgono le proprietà distibutive, ovvero $\forall a, b, c \in A$ si ha

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Se $(A, \cdot)$ ammette l'elemento neutro, allora si parla di *anello con unità*; se $(A, \cdot)$ è commutativo, allora $(A, +, \cdot)$ si dice *anello commutativo.*

Osservazione 1. L'elemento neutro rispetto a $+$ di una anello $(A, +, \cdot)$ si indica in generale con 0_A o semplicemente 0; l'elemento neutro rispetto a $\cdot$ (se esiste) si indica con 1_A o semplicemente 1.

Nel seguito ci si riferirà sempre ad anelli con unità.

Esempio 1. Sono esempi di anelli commutativi con unità gli insiemi $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$.

Tra le proprietà di un anello, che per ragioni di tempo vengono tralasciate, si evidenzia la seguente:

Proposizione 1. *Sia $(A, +, \cdot)$ un anello. Allora si ha:*

$$\forall\ a \in A \quad a \cdot 0_A = 0_A \cdot a = .$$

Dimostrazione. Sia $A \in A$. Per la proprietà distributiva, si ha:

$$a \cdot 0_A = a \cdot (0_A + 0_A) = a \cdot 0_A + a \cdot 0_A$$

e, per le leggi di cancellazione applicate al gruppo $(A, +)$, segue $a \cdot 0_A = 0_A$; analogamente si vede che $0_A \cdot a = 0_A$.

Definizione 2. Si dice che un anello con unità $(A, +, \cdot)$ è un *corpo* se ogni elemento non nullo di A è invertibile rispetto a $\cdot$; un corpo commutativo si chiama *campo.*

Esempio 2. Sono campi, per esempio, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$, p numero primo.

Osservazione 2. Nell'anello $(\mathbb{Z}_6, +, \cdot)$ il prodotto $[3]_6 \cdot [2]_6 = [0]_6$, pur essendo $[3]_6 \neq [0]_6$ e $[2]_6 \neq [0]_6$; d'altra parte $[5]_6$ ammette come inverso moltiplicativo $[5]_6$. Pertanto hanno senso le seguenti definizioni:

Definizione 3. Sia $(A, +, \cdot)$ un anello. Un elemento $a \in A$ si dice *divisore dello zero* se

1. $a \neq 0_A$
2. $\exists\ b \in A,\ b \neq 0_A,$ tale che $a \cdot b = 0_A$.

In tal caso b si dice *codivisore dello zero* di a

Osservazione 3. Si noti che un divisore dello zero di un anello in generale ammette più di un codivisore dello zero: nell'anello $(\mathbb{Z}_6, +, \cdot)$, si può notare che $[2]_6$ e $[4]_6$ sono entrambi codivisori dello zero di $[3]_6$.

Definizione 4. Sia $(A, +, \cdot)$ un anello con unità. Un elemento $a \in A$ si dice *unitario* se è inveritibile rispetto a $\cdot$.

Proposizione 2. *Siano $(A, +, \cdot)$ un anello con unità, $a \in A$. Risulta:*

- *se a è unitario, allora a non può essere un divisore dello zero*
- *se a è un divisore dello zero, allora a non può essere unitario.*

Dimostrazione. Si suppone che a sia unitario. Se per assurdo a fosse un divisore dello zero, sarebbe $a \neq 0_A$ ed inoltre esisterebbe $b \in A$, $b \neq 0_A$ tale che

$$a \cdot b = 0_A. \tag{1}$$

Moltiplicando per a^{-1}, da (1) si avrebbe

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0_A = 0_A$$

ovvero, per l'associatività di $\cdot$,

$$b = (a^{-1} \cdot a) \cdot b = 0$$

che dà luogo a contraddizione.
Per provare la seconda affermazione, si suppone che a sia un divisore dello zero. Allora $a \neq 0_A$ e esiste $b \in A$, $b \neq 0_A$ tale che $a \cdot b = 0_A$. Se a fosse unitario, esisterebbe a^{-1}, l'elemento inverso di a e si avrebbe:

$$b = (a^{-1} \cdot a) \cdot b = a^{-1}(\cdot a \cdot b) = a^{-1} \cdot 0_A = 0_A$$

che contraddice $b \neq 0_A$.

Corollario 1. *In un campo non ci sono divisori dello zero.*

Osservazione 4. L'anello $(\mathbb{Z}, +, \cdot)$ non ha divisori dello zero: per questo motivo si chiama *dominio di integrità.*

Osservazione 5. Si dimostra che in un anello *finito* ogni elemento non nullo è divisore dello zero oppure è unitario. Per esempio si è osservato che in $\mathbb{Z}_n$, n non primo, sono unitari gli elementi primi con n e quindi gli elementi unitari sono in numero di $\varphi(n)$ (φ funzione di Eulero); i rimanenti $n - 1 - \varphi(n)$ elementi non nulli di $\mathbb{Z}_n$ sono quindi divisori dello zero.