© 88-08-16270-2

CAPITOLO 4

Gli anelli

Che per un uomo il meglio è certo nascere
pien di saggezza, ma tal sorte è rara,
e bello è pur da chi ben dice apprendere.
Sofocle, Antigone.

Nei due capitoli precedenti abbiamo studiato gli interi, i polinomi in una o più indeterminate, le classi resto modulo un intero n: tali insiemi sono tutti esempi di anelli. In questo capitolo studieremo gli anelli (commutativi) generali, nel senso che dalla loro definizione assiomatica dedurremo varie proprietà che hanno quindi validità generale. Come esempi guida è sempre bene tener presenti gli anelli studiati nei capitoli precedenti.

4.1. Prime definizioni ed esempi

Partiamo dalla definizione *assiomatica* di anello.

4.1.1 Definizione. Un *anello* $(R, +, \cdot)$ è un *insieme* dotato di *due operazioni binarie*, indicate con $+$ e $\cdot$,

$$R \times R \longrightarrow R \qquad R \times R \longrightarrow R$$
$$(a,b) \longmapsto a+b \qquad (a,b) \longmapsto a \cdot b$$

che prendono il nome di *addizione* e *moltiplicazione*, tali che valgano le seguenti condizioni:

(i) (a) $+$ è *associativa*, ossia $(a+b)+c = a+(b+c)$ $\forall a,b,c \in R$;
(b) esiste un elemento 0 che è *neutro* rispetto a $+$, ossia $a+0 = 0+a = a$ $\forall a \in R$;
(c) $\forall a \in R$ esiste un elemento, $-a$, tale che $a+(-a) = 0$ (*esistenza dell'opposto*);
(d) $+$ è *commutativa*, ossia $a+b = b+a$ $\forall a,b \in R$;

(ii) $\cdot$ è *associativa*, cioè $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall a, b, c \in R$;
(iii) valgono le seguenti leggi *distributive*:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (a + b) \cdot c = a \cdot c + b \cdot c \qquad \forall a, b, c \in R\,.$$

D'ora in poi in genere scriveremo ab invece di $a \cdot b$.

Un insieme dotato di un'operazione che gode di (a), (b) e (c) prende il nome di *gruppo*: quindi $(R, +)$ è un gruppo. Il punto (d) dice che il gruppo è *abeliano* cioè *commutativo*. Parleremo spesso di $(R, +)$ come del *gruppo additivo* dell'anello. Nella seconda parte del corso parleremo di gruppi *generali* (ossia senza la richiesta che siano abeliani).

Un anello in cui la *moltiplicazione* sia commutativa prende il nome di anello *commutativo*. □

Abbiamo già visto che esistono delle proprietà ulteriori che si possono aggiungere alla definizione di anello (senza che però siano obbligatorie). Le raccogliamo in un elenco per comodità:

(1) un anello si dice *commutativo* se vale la proprietà commutativa della moltiplicazione;
(2) un anello R si dice *unitario* o *con unità* se esiste 1 in R tale che $1 \cdot a = a \cdot 1 = a$ per ogni a in R;
(3) un anello commutativo si dice *dominio di integrità* se non possiede divisori dello zero, cioè se $ab = 0 \Longrightarrow a = 0$ o $b = 0$;
(4) Un *campo* è un anello commutativo con unità che contiene l'inverso di ogni elemento non nullo.
(5) Un *corpo* è un anello (non necessariamente commutativo) con unità che contiene l'inverso di ogni elemento non nullo.