Capitolo 7

Gli anelli

§ 7.1 Generalità sugli anelli

Definizione 7.1. *Si dice* **anello** *un insieme A dotato di due operazioni, usualmente denotate con $+$ e $\cdot$ e dette somma e prodotto, che soddisfano le seguenti proprietà:*

1. $(A, +)$ *è un gruppo abeliano*

2. $(A, \cdot)$ *è un semigruppo*

3. *valgono le roprietà distributive del prodotto rispetto alla somma:*

$$\forall a,\ b,\ c \in A: \qquad (a+b)\cdot c = a\cdot c + b\cdot c, \qquad c\cdot(a+b) = c\cdot a + c\cdot b$$

Inoltre l'anello A si dice **commutativo con identità** *se soddisfa anche le due ulteriori condizioni:*

4. *Proprietà commutativa del prodotto:* $\forall a,\ b \in A:\ a\cdot b = b\cdot a$

5. *Esistenza dell'identità o elemento neutro per il prodotto, di solito denotato 1_A, tale che $\forall a \in A:\ a\cdot 1_A = 1_A \cdot a = a$*

Esempio 7.2. L'insieme dei numeri interi $\mathbb{Z}$ dotato delle operazioni $+$ e $\cdot$ è un anello commutativo con identità, con $0_{\mathbb{Z}} = 0$ e $1_{\mathbb{Z}} = 1$.

Esempio 7.3. L'insieme $\mathbb{Z}_n$ delle classi di resto modulo n (Capitolo 9) dotato delle operazioni $+$ e $\cdot$ è un anello commutativo con identità. In particolare:

i) $0_{\mathbb{Z}_n} = [0]$;

ii) $-[a] = [-a]$;

iii) $1_{\mathbb{Z}_n} = [1]$.

Molte proprietà dei numeri interi che usiamo abitualmente non sono caratteristiche dei numeri interi, ma dipendono soltanto dalla struttura di anello, ossia valgono per tutti gli anelli (oppure per tutti gli anelli commutativi con identità), incluso ad esempio $\mathbb{Z}_n$. L'enunciato seguente presenta alcune proprietà di questo tipo; alcune altre sono inserite tra gli esercizi.

Lemma 7.4. *Sia A un anello. Allora:*

i) *l'elemento neutro rispetto alla somma è unico;*

ii) *per ogni elemento $a \in A$ l'opposto è unico;*

iii) *vale la proprietà di cancellazione per la somma $a + c = b + c \Longrightarrow a = b$.*

iv) $\forall a \in A$, $0_A \cdot a = a \cdot 0_A = 0_A$*;*

Se inoltre A è un anello commutativo con identità 1_A, allora:

v) *l'identità rispetto al prodotto è unico;*

vi) *l'opposto $-a$ di un elemento $a \in A$ è $(-1_A) \cdot a$.*

Dimostrazione. Le proprietà i), ii), iii) derivano dal fatto che $(A, +)$ è un gruppo. iv) Sia a un qualsiasi elemento di A. Si hanno le uguaglianze: $0_A \cdot a = (0_A + 0_A) \cdot a = 0_A \cdot a + 0_A \cdot a$. Sommando ai due membri estremi dell'uguaglianza l'opposto di $(0_A \cdot a)$ troviamo da un lato $(0_A \cdot a) + (-(0_A \cdot a)) = 0_A$ e dall'altro $0_A \cdot a + 0_A \cdot a + (-(0_A \cdot a)) = 0_A \cdot a + 0_A = 0_A \cdot a$. Allora $0_A = 0_A \cdot a$, come volevasi. v) L'unicità dell'identità moltiplicativa si prova in modo del tutto analogo a quello seguito per l'identità additiva. vi) Basta provare che $(-1_A) \cdot a$ soddisfa la definizione di l'opposto di a, ossia che sommato con lui dà 0_A:

$$a + (-1_A) \cdot a = 1_A \cdot a + (-1_A) \cdot a = (1_A + (-1_A)) \cdot a = 0_A \cdot a = 0_A.$$

□

Definizione 7.5. *Siano A e B due anelli. Nel prodotto cartesiano $A \times B$ si possono introdurre due operazioni di somma e prodotto ponendo $\forall (a, b), (a', b') \in A \times B$*

$$(a, b) + (a', b') = (a + a', b + b'),$$
$$(a, b) \cdot (a', b') = (aa', bb').$$

Si verifica che con tali **operazioni componente per componente***, il prodotto cartesiano $A \times B$ è un anello, detto* ***anello prodotto*** *di A e B. Se inoltre A e B sono anelli commutativi con identità, anche $A \times B$ lo 'e . Se infine esistono le identità 1_A e 1_B, allora anche l'anello prodotto ha identità $1_{A \times B} = (1_A, 1_B)$.*

§ 7.2 Divisori dello zero e unità

In questa sezione consideriamo sempre un anello commutativo con identità A. Spesso sottointenderemo il simbolo $\cdot$ del prodotto, ossia scriveremo ab invece di $a \cdot b$, e useremo la notazione abbreviata $a - b$ al posto di $a + (-b)$.

Definizione 7.6. *Si dice che A è un* **dominio di integrità** *o semplicemente un* **dominio** *se in A vale la* **legge di annullamento del prodotto** *ossia se*

$$\forall\ a, b \in A: \quad ab = 0_A \Longrightarrow a = 0_A \text{ oppure } b = 0_A.$$

Lemma 7.7. *Se A è un dominio di integrità, allora in A vale la legge di cancellazione per il prodotto ossia $\forall\ a,\ b,\ c \in A$, se $c \neq 0_A$ allora $ac = bc \Longrightarrow a = b$.*

Dimostrazione. Sommando ai due membri di $ac = bc$ l'opposto di bc si ottiene $ac - bc = 0_A$ ossia $(a - b)c = 0_A$. Poiché vale la legge di annullamento del prodotto e $c \neq 0$, allora $a - b = 0$ ossia (sommando b ai due membri) $a = b$. □

Definizione 7.8. *Un elemento $a \in A$ si dice* **zero-divisore** *di A se esiste $b \in A$, $b \neq 0_A$, tale che $ab = 0_A$.*

Concretamente gli zero-divisori sono quegli elementi per cui non vale la legge di cancellazione del prodotto. Un anello commutativo con identità A è un dominio se e solo se l'unico zero-divisore è 0_A.

Esempio 7.9. In $\mathbb{Z}$ l'unico elemento per cui non vale la legge di cancellazione è 0 e quindi $\mathbb{Z}$ è un dominio di integrità.

Esempio 7.10. In $\mathbb{Z}_6$, l'anello delle classi di resto modulo 6 si ha $[2] \cdot [3] = [6] = [0]$, anche se $[2] \neq [0]$ e $[3] \neq [0]$. Quindi $\mathbb{Z}_6$ non è un dominio di integrit'a.

Esempio 7.11. L'anello prodotto $\mathbb{Z} \times \mathbb{Z}$ non è un dominio di integrit'a. Infatti $(1, 0) \neq 0_{\mathbb{Z}\times\mathbb{Z}} = (0, 0)$ e $(0, 1) \neq 0_{\mathbb{Z}\times\mathbb{Z}} = (0, 0)$, ma il loro prodotto è nullo:

$$(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0) = 0_{\mathbb{Z}\times\mathbb{Z}}.$$

Definizione 7.12. *Un elemento $u \in A$ si dice* **unità** *o anche* **elemento invertibile** *di A se esiste in A un suo* **inverso rispetto al prodotto**, *ossia un elemento v tale che $uv = vu = 1_A$. Di solito l'inverso di un elemento a (che, se esiste, è sempre unico) si indica con a^{-1}. Due elementi a, b di A si dicono* **associati** *l'uno all'altro se esiste una unità $u \in A$ tale che $a = ub$ (e quindi $b = u^{-1}a$).*

Esempio 7.13. In $\mathbb{Z}$ gli unici elementi invertibili sono 1 e -1. Due elementi sono allora associati se sono uguali oppure sono opposti.

Esempio 7.14. In $\mathbb{Z}_6$ gli unici elementi invertibili sono $[1]$ e $[5] = [-1] = -[1]$. Quindi in $\mathbb{Z}_6$, $[a]$ e $[b]$ sono associati se $[a] = [b]$ oppure se $[a] = [5][b] = [5b] = [-1][b] = [-b]$.

Esempio 7.15. Nell'anello prodotto $\mathbb{Q} \times \mathbb{Q}$ sono invertibili tutti gli elementi (a, b) tali che $a \neq 0$ e $b \neq 0$, mentre non lo sono tutti gli altri, ossia quelli in cui 0 compare al primo e/o al secondo posto.

Esempio 7.16. Le seguenti sono le tabelline del prodotto in $\mathbb{Z}_3$ e in $\mathbb{Z}_4$:

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Escludendo $[0]_3$ da $\mathbb{Z}_3$ otteniamo un gruppo col prodotto. Infatti i due elementi diversi da $[0]_3$ sono inversi di se stessi. Invece, nel caso $n = 4$ non otteniamo un gruppo neanche escludendo $[0]_4$, ossia neppure $(\mathbb{Z}_4 - \{[0]_4\}, \cdot)$ è un gruppo. Infatti anche $[2]_4$ non ha l'inverso.

Definizione 7.17. *Si dice che un anello commutativo con identità A è un* **campo** *se ogni elemento non nullo di A è una unità.*

Esempio 7.18. L'anello $\mathbb{Z}_3$ è un campo. Anche nell'anello $\mathbb{Z}_7$, tutti gli elementi tranne $[0]$ sono invertibili, quindi anche $\mathbb{Z}_7$ è un campo. Invece $\mathbb{Z}_4$ non è un campo.

§ 7.3 Omomorfismi di anelli

Definizione 7.19. *Siano A e B due anelli. Una funzione $f\colon A \to B$ si dice* **omomorfismo di anelli** *se*

i) f è un omomorfismo dei gruppi additivi $(A, +)$ e $(B, +)$ (ossia rispetta la somma):

$$\forall a, a' \in A\colon \quad f(a + a') = f(a) + f(a')$$

ii) f è un omomorfismo dei semigruppi moltiplicativi $(A, \cdot)$ e $(B, \cdot)$ (ossia rispetta il prodotto):

$$\forall a, a' \in A\colon \quad f(a \cdot a') = f(a) \cdot f(a').$$

Se inoltre A e B hanno identit'a , si richiede che valga anche: $f(1_A) = 1_B$.

Definizione 7.20. *Un omomorfismo di anelli si dice:*

- **epimorfismo** *se è suriettivo*
- **monomorfismo** *se è iniettivo*
- **isomorfismo** *se è biunivoco.*

Possiamo caratterizzare la suriettività e l'iniettività di un omomorfismo di anelli mediante l'immagine e il nucleo, esattamente come abbiamo visto nel caso degli omomorfismi di gruppi.

Definizione 7.21. *L'immagine di un omomorfismo di anelli* $f\colon (A,+,\cdot) \to (B,+,\cdot)$ *è* $Im(f) := \{b \in B \mid \exists a \in A :\ f(a) = b\}$. *Il nucleo di* f *è* $Ker(f) := \{a \in A \mid f(a) = 0_B\}$.

Le definizioni date di nucleo e di immagine si riferiscono semlicemente alla struttura additiva degli anelli A e B. Ricordando che ogni omomorfismo di anelli è anche, per definizione, un omomorfismo di gruppi additivi, otteniamo il risultato seguente:

Proposizione 7.22. *Sia* $f\colon (A,+,\cdot) \to (B,+,\cdot)$ *un omomorfismo di anelli. Allora*

- f *è un epimorfismo di anelli, ossia è suriettivo* $\iff Im(f) = B$
- f *è un monomorfismo di anelli, ossia è iniettivo* $\iff Ker(f) = \{0_A\}$.

§ 7.4 Costruzione di $\mathbb{Z}$ (Facoltativa)

Consideriamo il prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ dell'insieme dei numeri naturali per sè ed in esso la relazione:

$$(n,m)\ \rho\ (n',m') \iff n + m' = n' + m.$$

Si può facilmente verificare che ρ è una relazione di equivalenza. Osserviamo che sono in relazione con la coppia $(0,0)$ tutte e sole le coppie del tipo (n,n). Inoltre, in ogni altra classe di equivalenza vi è una (e soltanto una) coppia in cui uno dei due elementi è lo 0. Se infatti $n > m$, ossia se $n = m + p$, allora $(n,m)\rho(p,0)$ e, analogamente, se $n < m$, ossia se $m = n + q$, allora $(n,m)\rho(0,q)$.

Definizione 7.23. *Si dice insieme dei numeri interi relativi* $\mathbb{Z}$ *l'insieme quoziente* $(\mathbb{N}\times\mathbb{N})/\rho$. *Ogni classe di equivalenza* $[(n,m)]$ *si dice* **numero intero relativo**. *La classe di* $(0,0)$ *si dice* **zero di** $\mathbb{Z}$ *e si indica con* 0*; la classe di* $(p,0)$ *(dove* $p \in \mathbb{N}$*) si indica con* $+p$ *o semplicemente con* p *e si dice* **numero intero positivo**, *la classe di* $(0,q)$ *(dove* $q \in \mathbb{N}$*) si indica con* $-q$ *e si dice* **numero intero negativo**.

Possiamo definire le operazioni somma e prodotto in $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\rho$ a partire dalle operazioni di $\mathbb{N}$, nel modo seguente:

$$[(n, m)] + [(n', m')] = [(n + n', m + m')]$$

e

$$[(n, m)] \cdot [(n', m')] = [(nn' + mm', nm' + n'm)]$$

Possiamo inoltre definire in $\mathbb{Z}$ un ordine totale nel modo seguente:

$$[(n, m)] \leq [(n', m')] \text{se in} \mathbb{N} \text{vale la disuguaglianza} n + m' \leq n' + m.$$

Lasciamo per esercizio al lettore la verifica che queste operazioni sono **ben poste** (ossia che il risultato non dipende dai rappresentanti) e la dimostrazione del seguente risultato.

Proposizione 7.24. *L'applicazione* $i \colon \mathbb{N} \longrightarrow \mathbb{Z}$ *data da* $i(p) = [(p, 0)]$ *è iniettiva e rispetta le operazioni e l'ordinamento ossia:*

$$i(p + q) = i(p) + i(q), i(pq) = i(p) \cdot i(q), p \leq q in \mathbb{N} se\ e\ solo\ se i(p) \leq i(q) in \mathbb{Z}.$$

Mediante i ossiamo identificare i numeri naturali con i numeri interi positivi e considerare $\mathbb{N}$ come un sottoinsieme di $\mathbb{Z}$.

§ 7.5 Esercizi

7.1 Siano A e B due anelli (oppure anelli commutativi con identità). Verificare che le operazioni definite componente per componente nel prodotto $A \times B$ soddisfano le proprietà di anello (rispettivamente: di anello commutativo con identità). **7.2** Si consideri l'anello $\mathbb{Z}_8$ con la somma e il prodotto usuali

a. Stabilire quali sono gli elementi invertibili di $\mathbb{Z}_8$.

b. Determinare gli eventuali zero-divisori di $\mathbb{Z}_8$.

c. è vero che $\mathbb{Z}_8$ è un dominio? è vero che $\mathbb{Z}_8$ è un campo?

7.3 Si consideri l'anello $\mathbb{Z}_{11}$ con la somma e il prodotto usuali

a. Stabilire quali sono gli elementi invertibili di $\mathbb{Z}_{11}$.

b. Determinare gli eventuali zero-divisori.

c. è vero che $\mathbb{Z}_{11}$ è un dominio? è vero che $\mathbb{Z}_{11}$ è un campo?

7.4 Si consideri l'anello $\mathbb{Z}$ con le operazioni usuali e l'anello prodotto $\mathbb{Z} \times \mathbb{Z}$.

a. Stabilire se la funzione $g \colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ data da $g(x) = (x, -x)$ è un omomorfismo di anelli.

b. La funzione g è iniettiva? è suriettiva?

7.5 Si considerino gli anelli $\mathbb{Z}$ e $\mathbb{Z}_6$ con le operazioni usuali e l'anello prodotto $\mathbb{Z} \times \mathbb{Z}_6$.

a. Provare che la funzione $h\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_6$ data da $h(x) = (x, [3x])$ è un omomorfismo di anelli.

b. Determinare nucleo e immagine di h.

c. h è un monomorfismo di anelli? è un epimorfismo di anelli?

7.6 Stablire se la funzione $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ data da $\varphi(x) = \frac{x}{2}$ è un omomorfismo di anelli. è anche un omorfismo di anelli commutativi con identità ?

7.7 Stablire se la funzione $\psi\colon \mathbb{Z} \to \mathbb{Q}$ data da $\psi(x) = \frac{1}{x}$ è un omomorfismo di anelli.

7.8 Determinare il nucleo e l'immagine dell'omomorfismo $f\colon \mathbb{Z} \to \mathbb{Z}_6 \times \mathbb{Z}_4$ data da $f(x) = ([x]_6, [x]_4)$.

7.9 Determinare il nucleo e l'immagine dell'applicazione $g\colon \mathbb{Z} \to \mathbb{Z}_3 \times \mathbb{Z}_8$ data da $f(x) = ([x]_3, [x]_8)$.

7.10 Sia A un anello commutativo con identità. Provare che l'inverso di un elemento $a \in A$, se esiste, è unico.

7.11 Sia A un anello commutativo con identità e siano u e v elementi invertibiie di A.

a. Provare che u è cancellabile ossia che $\forall a, b \in A : au = bu \Rightarrow a = b$.

b. Provare che uv è invertibile.

c. Provare per induzione che v^n è invertibile , per ogni $n \in \mathbb{Z}$.

7.12 Sia A un anello commutativo con identità. Provare l'equivalenza:

$$c \text{ è uno zero-divisore} \Leftrightarrow c \text{ non è cancellabile.}$$

7.13 Sia A un anello commutativo con identità 1_A. Provare per ogni $a, b \in A$ le seguenti relazioni (tra le quali la regoletta del "$- \times - = +$"):

a. $-(ab) = (-a)b = a(-b), \quad (-1_A)^2 = 1_A, \quad (-a)^2 = a^2, \quad (-a)(-b) = ab,$

b. $-(a - b) = -a + b\ , \qquad -(-a) = a,$

c. $(-1_A)^n = 1_A$ se n è un intero pari e $(-1_A)^n = -1_A$ se n è un intero dispari.