

## XI Settimana

### 2. ELEMENTI BASILARI DELLA TEORIA DEGLI ANELLI (II PARTE)

• Dati due anelli  $(R, +, \cdot)$  e  $(R', +, \cdot)$ , un'applicazione  $f : R \rightarrow R'$  si dice un *omomorfismo di anelli* se:

$$f(x + y) = f(x) + f(y) \quad \text{e} \quad f(x \cdot y) = f(x) \cdot f(y), \quad \forall x, y \in R,$$

cioè, se il corrispondente della somma [ripettivamente, del prodotto] in  $R$  di due elementi in  $R$  coincide con la somma [ripettivamente, con il prodotto] in  $R'$  dei corrispondenti dei due elementi. In altre parole, un omomorfismo di anelli è un'applicazione che conserva le operazioni.

• Un omomorfismo di anelli, che è anche un'applicazione biettiva, viene chiamato un *isomorfismo di anelli*. Due anelli  $(R, +, \cdot)$  e  $(R', +, \cdot)$  sono detti *isomorfi*, se esiste un isomorfismo di anelli da  $(R, +, \cdot)$  a  $(R', +, \cdot)$ .

Dati due anelli  $(R, +, \cdot)$  e  $(R', +, \cdot)$ , denotiamo con  $0_R$  [rispettivamente,  $1_R$ ] l'elemento neutro rispetto alla somma + [ripettivamente, l'eventuale elemento neutro rispetto al prodotto  $\cdot$ ] di  $R$  e con  $0_{R'}$  [rispettivamente,  $1_{R'}$ ] l'elemento neutro rispetto alla somma + [ripettivamente, l'eventuale elemento neutro rispetto al prodotto  $\cdot$ ] di  $R'$ .

• Sia  $f : R \rightarrow R'$  un omomorfismo di anelli, poniamo:

$$\begin{aligned} \text{Ker}(f) &:= \{x \in R \mid f(x) = 0_{R'}\} = f^{-1}(0_{R'}) (\subseteq R), \\ \text{Im}(f) &:= \{x' \in R' \mid f(x) = x', \text{ per qualche } x \in R\} = f(R) (\subseteq R'). \end{aligned}$$

Il sottoinsieme  $\text{Ker}(f)$  di  $R$  è detto il *nucleo dell'omomorfismo*  $f$ . Il sottoinsieme  $\text{Im}(f)$  di  $R'$  è detto l'*immagine dell'omomorfismo*  $f$ .

**Proposizione 2.1.** *Dati due anelli  $(R, +, \cdot)$  e  $(R', +, \cdot)$  ed un omomorfismo di anelli  $f : R \rightarrow R'$ , allora:*

- (1)  $f(0_R) = 0_{R'}$  (l'immagine dello zero di  $R$  deve coincidere con lo zero di  $R'$ ).
- (2)  $f(-x) = -f(x)$  (l'immagine dell'opposto di un elemento  $x$  di  $R$  deve coincidere con l'opposto in  $R'$  dell'immagine in  $R'$  dell'elemento  $x$ ).
- (3)  $\text{Im}(f)$  è un sottoanello di  $(R', +, \cdot)$ .
- (4)  $\text{Ker}(f)$  è un sottoanello di  $(R, +, \cdot)$ .
- (5)  $f : R \rightarrow R'$  è un omomorfismo iniettivo se e soltanto se  $\text{Ker}(f) = \{0_R\}$ .

Inoltre, se supponiamo che gli anelli  $(R, +, \cdot)$  e  $(R', +, \cdot)$  siano unitari e che  $\text{Im}(f) = R'$ , allora:

- (6)  $f(1_R) = 1_{R'}$  (l'immagine dell'unità di  $R$  deve coincidere con l'unità di  $R'$ ).
- (7) Se  $x \in \mathbf{U}(R)$ , allora  $f(x) \in \mathbf{U}(R')$ , ed inoltre  $f(x^{-1}) = f(x)^{-1}$  (l'immagine dell'inverso di un elemento invertibile  $x$  di  $R$  deve coincidere con l'inverso in  $R'$  dell'immagine in  $R'$  dell'elemento  $x$ ). In particolare, l'omomorfismo di anelli  $f : R \rightarrow R'$  determina –per restrizione agli elementi invertibili– un omomorfismo di gruppi moltiplicativi (ancora denotato con  $f$ )  $f : \mathbf{U}(R) \rightarrow \mathbf{U}(R')$ .

**Esempio 2.2.** (0) Dati due anelli  $(R, +, \cdot)$  e  $(R', +, \cdot)$  l'applicazione costante sullo zero di  $R'$ , cioè l'applicazione  $\mathbf{0} : R \rightarrow R'$ ,  $x \mapsto 0_{R'}$ , è un omomorfismo di anelli, detto *omomorfismo banale*.

(1) Preso comunque un intero  $n \geq 2$ , l'applicazione:

$$\pi_n : \mathbb{Z} \rightarrow \frac{\mathbb{Z}}{\equiv_n} = \frac{\mathbb{Z}}{n\mathbb{Z}}, \quad k \mapsto [k]_n = k + n\mathbb{Z},$$

determina un omomorfismo dall'anello  $(\mathbb{Z}, +, \cdot)$  all'anello  $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot)$ .

Si verifica facilmente che:

$$\text{Ker}(\pi_n) = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}, \quad \text{Im}(\pi_n) = \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Si noti che  $\mathbf{U}(\mathbb{Z}) = \{-1, 1\}$  e che  $\pi_n(\mathbf{U}(\mathbb{Z})) = \{[1]_n, [n-1]_n\} (\subseteq \mathbf{U}(\frac{\mathbb{Z}}{n\mathbb{Z}}) = \{[k]_n \mid 1 \leq k \leq n, \text{MCD}(k, n) = 1\})$ .

(2) Sia  $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \frac{\mathbb{Z}}{p\mathbb{Z}}\}$ . Allora, l'applicazione:

$$\det : \mathbf{M}_{2,2}(K) \rightarrow K, \quad A \mapsto \det(A),$$

non definisce un omomorfismo dall'anello  $(\mathbf{M}_{2,2}(K), +, \cdot)$  all'anello  $(o, \text{ meglio, al campo}) (K, +, \cdot)$ . Infatti, in generale,  $\det(A+B) \neq \det(A) + \det(B)$ . Ad esempio:

$$\begin{aligned} \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right) &= \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 1 \\ \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) + \det\left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right) &= 0 + 0 = 0. \end{aligned}$$

Si noti anche che  $\mathbf{U}(\mathbf{M}_{2,2}(K)) = \text{GL}_2(K)$ , che  $\mathbf{U}(K) = K^*$  e che l'applicazione:

$$\det : \mathbf{U}(\mathbf{M}_{2,2}(K)) \rightarrow \mathbf{U}(K), \quad A \mapsto \det(A)$$

è un omomorfismo di gruppi moltiplicativi.

(3) L'applicazione  $f : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto 2x$ , non è un omomorfismo di anelli, perché conserva la somma ma non il prodotto.

(4) L'applicazione  $g : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto |x|$ , non è un omomorfismo di anelli, perché conserva il prodotto ma non la somma.

(5) Sia  $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \frac{\mathbb{Z}}{n\mathbb{Z}}\}$ . Allora, l'applicazione:

$$f : R \rightarrow \mathbf{M}_{2,2}(R), \quad x \mapsto \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix},$$

è un omomorfismo di anelli. Si noti però che, benché entrambi gli anelli siano unitari,  $f$  non conserva l'unità:

$$f(1_R) = \begin{pmatrix} 1_R & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1_R & 0 \\ 0 & 1_R \end{pmatrix} = 1_{\mathbf{M}_{2,2}(R)}.$$

(6) Sia  $X$  un insieme non vuoto ed  $(R, +, \cdot)$  un anello. Sia  $x_0$  un elemento fissato in  $X$ . L'applicazione  $ev_{x_0}$  (di "calcolo in  $x_0$ ") dall'anello  $(R^X, +, \cdot)$  (anello di tutte le applicazioni da  $X$  ad  $R$ ) all'anello  $(R, +, \cdot)$ , definita nella maniera seguente:

$$ev_{x_0} : R^X \rightarrow R, \quad f \mapsto f(x_0),$$

(il corrispondente  $ev_{x_0}(f)$  di una qualunque applicazione  $f \in R^X$  si ottiene "calcolando"  $f$  nell'elemento  $x_0$ ) è un omomorfismo di anelli.

• Un sottoanello  $S$  di un anello  $(R, +, \cdot)$  determina sempre una relazione di equivalenza (denotata " $\varepsilon_S$ ") su  $R$ , definita nella maniera seguente: presi  $x, y \in R$ , allora:

$$x \varepsilon_S y \quad :\Leftrightarrow \quad x - y \in S.$$

Non è difficile mostrare che:

$$\begin{aligned} [x]_{\varepsilon_S} &= x + S; \\ x \varepsilon_S y &\Leftrightarrow x + S = y + S. \end{aligned}$$

I sottoinsiemi di  $R$  del tipo  $x + S$ , che descrivono la partizione di  $R$  associata alla relazione di equivalenza  $\varepsilon_S$ , sono chiamati *classi laterali di  $R$  modulo il sottoanello  $S$* .

*Osservazione 2.3.* Si noti che, nel caso degli anelli, dato un sottoanello  $S$ , la relazione di equivalenza che si considera è unica (e ciò è in accordo anche con quanto descritto in teoria dei gruppi), in quanto  $S$ , in particolare, è un sottogruppo del gruppo abeliano (additivo)  $(R, +)$  (e, quindi, è banalmente un sottogruppo normale).

Si noti che, in accordo, con la situazione esaminata in teoria dei gruppi si ha:

**Lemma 2.4.** *Sia  $S$  un sottoanello di un anello  $(R, +, \cdot)$ . Allora, la relazione di equivalenza  $\varepsilon_S$ , definita su  $R$ , è compatibile con la somma, cioè:*

$$x \varepsilon_S y \quad e \quad x' \varepsilon_S y' \quad \Rightarrow \quad x + x' \varepsilon_S y + y'.$$

Per avere che la relazione di equivalenza  $\varepsilon_S$  sia compatibile anche con il prodotto è necessario assumere che  $S$  sia un sottoanello di “un tipo particolare”. (Ad esempio, se  $R := \mathbb{Q}$ , se  $S := \mathbb{Z}$ , se  $x := \frac{3}{2}$ ,  $y := \frac{1}{2}$ ,  $x' := \frac{4}{3}$  e  $y' := \frac{1}{3}$ , allora  $\frac{3}{2} - \frac{1}{2} \in \mathbb{Z}$  e  $\frac{4}{3} - \frac{1}{3} \in \mathbb{Z}$ , però  $\frac{3}{2} \cdot \frac{4}{3} - \frac{1}{2} \cdot \frac{1}{3} = \frac{12}{6} - \frac{1}{6} \notin \mathbb{Z}$ , pertanto in questo caso la relazione di equivalenza  $\varepsilon_{\mathbb{Z}}$ , definita su  $\mathbb{Q}$ , non è compatibile con il prodotto. Purtuttavia,  $\varepsilon_{\mathbb{Z}}$  è compatibile con la somma, in quanto  $\mathbb{Z}$  è un sottoanello di  $\mathbb{Q}$ .)

- Un sottoinsieme non vuoto  $I$  di un anello  $(R, +, \cdot)$  si dice *un ideale di  $R$*  se:

$$I - I \subseteq I \quad e \quad I \cdot R \subseteq I, \quad R \cdot I \subseteq I,$$

(cioè,  $x - y \in I$  e  $x \cdot r, r \cdot x \in I$ ,  $\forall x, y \in I, \forall r \in R$ ).

Ovviamente, un ideale è un sottoanello particolare, in quanto un sottoanello  $S$ , per essere tale, verifica le condizioni:

$$S - S \subseteq S \quad e \quad S \cdot S \subseteq S,$$

dove la seconda condizione (chiusura rispetto alla moltiplicazione) è più debole delle “condizioni moltiplicative” richieste per un ideale (chiusura sia rispetto alla moltiplicazione a destra sia rispetto alla moltiplicazione a sinistra con elementi arbitrari dell’anello).

**Esempio 2.5. (0)** Se  $(R, +, \cdot)$  è un anello, allora  $\{0\}$  e  $R$  sono ideali di  $(R, +, \cdot)$ , detti *ideali banali di  $R$* .

(1) Preso comunque  $n \geq 2$ ,  $n\mathbb{Z}$  è un ideale proprio di  $(\mathbb{Z}, +, \cdot)$  (ed ogni ideale proprio di  $(\mathbb{Z}, +, \cdot)$  è di questo tipo; vedi quanto già osservato per i sottoanelli di  $(\mathbb{Z}, +, \cdot)$ ).

(2)  $\mathbb{Z}$  (è un sottoanello, ma) *non* è un ideale di  $(\mathbb{Q}, +, \cdot)$ .

(3) Sia  $(R, +, \cdot)$  un anello assegnato (ad esempio, sia  $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \frac{\mathbb{Z}}{n\mathbb{Z}}\}$ ). Sia  $\mathbf{S}_{2,2}(R) := \{A \in \mathbf{M}_{2,2}(R) \mid \det(A) = 0\}$  (tale insieme è chiamato insieme delle *matrici singolari di  $\mathbf{M}_{2,2}(R)$* ). Allora, è facile verificare che  $\mathbf{S}_{2,2}(R)$  *non* è un ideale di  $(\mathbf{M}_{2,2}(R), +, \cdot)$ , perchè  $(\mathbf{S}_{2,2}(R), +)$  non è un sottogruppo di  $(\mathbf{M}_{2,2}(R), +)$  (non

è detto che la somma o la differenza di matrici singolari sia ancora singolare, ad esempio:

$$\det\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right) = \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 1$$

$$\det\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) = 0, \quad \det\left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right) = 0.$$

Si noti però che:

$$\mathbf{S}_{2,2}(R) \cdot \mathbf{M}_{2,2}(R) \subseteq \mathbf{S}_{2,2}(R), \quad \mathbf{M}_{2,2}(R) \cdot \mathbf{S}_{2,2}(R) \subseteq \mathbf{S}_{2,2}(R),$$

(basta utilizzare la ben nota proprietà del determinante:  $\det(A \cdot B) = \det(A) \cdot \det(B)$ ).

(4) Sia  $S$  un insieme non vuoto. Nell'anello commutativo unitario  $(\mathbf{P}(S), +, \cdot)$  [dove  $+$  :=  $\Delta$  (differenza simmetrica),  $\cdot$  :=  $\cap$  (intersezione)], il sottoinsieme  $\mathbf{P}_f(S) := \{X \in \mathbf{P}(S) \mid \text{Card}(X) < \infty\}$  forma un ideale dell'anello  $(\mathbf{P}(S), +, \cdot)$ .

(5) Sia  $S$  un insieme non vuoto e  $T$  un sottoinsieme non vuoto di  $S$ . Nell'anello commutativo unitario  $(\mathbf{P}(S), +, \cdot)$  [dove  $+$  :=  $\Delta$  (differenza simmetrica),  $\cdot$  :=  $\cap$  (intersezione)], il sottoinsieme  $\mathbf{P}(T)$  costituisce un ideale di  $(\mathbf{P}(S), +, \cdot)$ .

(6) Sia  $(R, +, \cdot)$  un anello. Allora il seguente sottoinsieme (non vuoto) di  $R$ , detto *centro dell'anello*  $(R, +, \cdot)$ :

$$\mathbf{Z}(R) := \{z \in R \mid z \cdot r = r \cdot z, \forall r \in R\} \quad (\text{si noti che } 0 \in \mathbf{Z}(R))$$

è un sottoanello, ma *non* è un ideale di  $(R, +, \cdot)$ .

Ad esempio, se  $(R, +, \cdot)$  è un anello, allora il centro  $(\mathbf{M}_{2,2}(R), +, \cdot)$  dell'anello delle matrici quadrate a 2 righe e 2 colonne ad entrate in  $R$  è dato da

$$\mathbf{Z}(\mathbf{M}_{2,2}(R)) := \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in R \right\}.$$

(Si noti che:

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} ax & ay \\ az & aw \end{pmatrix} \notin \mathbf{Z}(\mathbf{M}_{2,2}(R)).)$$

(7) Sia  $(R, +, \cdot)$  un anello,  $S$  un sottoanello di  $(R, +, \cdot)$  e  $X$  un insieme non vuoto. Allora  $S^X$  è un sottoanello ma *non* un ideale dell'anello delle applicazioni  $(R^X, +, \cdot)$ . [Ogni elemento  $g : X \rightarrow S$  di  $S^X$  viene identificato con l'elemento  $g : X \rightarrow S \subseteq R$  di  $R^X$ .]

Si osservi, però, che se  $I$  è un ideale di  $(R, +, \cdot)$  allora  $I^X$  è un ideale dell'anello delle applicazioni  $(R^X, +, \cdot)$ .

(8) Siano  $(R_1, +, \cdot)$  e  $(R_2, +, \cdot)$  due anelli e sia  $(R_1 \times R_2, +, \cdot)$  l'anello prodotto diretto. Allora  $R_1 \times \{0\}$  e  $\{0\} \times R_2$  sono ideali di  $(R_1 \times R_2, +, \cdot)$ .

*Osservazione 2.6.* (1) Si noti che se  $I$  è un ideale in un anello unitario  $(R, +, \cdot)$  e se  $1_R \in I$  allora necessariamente  $I = R$  (infatti  $R = 1_R \cdot R \subseteq I \cdot R \subseteq I \subseteq R$ ).

(2) Un campo  $(K, +, \cdot)$  non possiede ideali propri (cioè i suoi soli ideali sono quelli banali).

- Se  $I$  è di un anello  $(R, +, \cdot)$ , allora nell'insieme-quotiente:

$$\frac{R}{I} := \frac{R}{\varepsilon_I} = \{x + I \mid x \in R\}$$

si possono (ben) definire un'operazione di somma  $+$  ed un'operazione di prodotto  $\cdot$ , dedotte canonicamente dalle omonime operazioni di  $R$ , nella maniera seguente:

$$(x + I) + (y + I) := x + y + I, \quad (x + I) \cdot (y + I) := x \cdot y + I, \quad \forall x, y \in R.$$

Ebbene:

**Proposizione 2.7.** *Sia  $I$  un ideale di un anello  $(R, +, \cdot)$ , allora:*

- (1) *La relazione di equivalenza  $\varepsilon_I$ , definita su  $R$ , è compatibile con la somma, cioè:*

$$x \varepsilon_I y \text{ e } x' \varepsilon_I y' \Rightarrow x + x' \varepsilon_I y + y'.$$

*Quindi, l'operazione di somma tra classi:*

$$(x + I) + (y + I) := x + y + I, \quad \forall x, y \in R$$

*è ben definita.*

*[Si noti che, questa parte dell'enunciato, vale sotto la ipotesi più debole che  $I$  sia un sottoanello di  $(R, +, \cdot)$ .]*

- (2) *La relazione di equivalenza  $\varepsilon_I$ , definita su  $R$ , è compatibile con il prodotto, cioè:*

$$x \varepsilon_I y \text{ e } x' \varepsilon_I y' \Rightarrow x \cdot x' \varepsilon_I y \cdot y'.$$

*Quindi, l'operazione di prodotto tra classi:*

$$(x + I) \cdot (y + I) := x \cdot y + I, \quad \forall x, y \in R$$

*è ben definita.*

- (3)  *$(\frac{R}{I}, +, \cdot)$  è un anello, chiamato l'anello-quotiente di  $R$  rispetto all'ideale  $I$ .*

*Osservazione 2.8.* Sia  $I$  un ideale di un anello  $(R, +, \cdot)$ . Si noti che:

- se  $(R, +, \cdot)$  è un anello commutativo, allora l'anello-quotiente  $(\frac{R}{I}, +, \cdot)$  è anch'esso commutativo;

- se  $(R, +, \cdot)$  è un anello unitario, allora l'anello-quotiente  $(\frac{R}{I}, +, \cdot)$  è anch'esso unitario (avente come unità la classe  $1_R + I$ );

- l'anello-quotiente  $(\frac{R}{I}, +, \cdot)$  può avere divisori dello zero anche se  $(R, +, \cdot)$  è privo di divisori dello zero (ad esempio,  $\frac{\mathbb{Z}}{n\mathbb{Z}}$  ha divisori dello zero, se  $n$  non è primo, mentre  $(\mathbb{Z}, +, \cdot)$  non ha divisori dello zero).

- l'anello-quotiente  $(\frac{R}{I}, +, \cdot)$  può essere privo di divisori dello zero anche se  $(R, +, \cdot)$  possiede divisori dello zero (ad esempio,  $\frac{\mathbb{Z}}{4\mathbb{Z}}$  ha divisori dello zero,  $\frac{2\mathbb{Z}}{4\mathbb{Z}}$  è un ideale di  $\frac{\mathbb{Z}}{4\mathbb{Z}}$ , l'anello quoziente:

$$\frac{\frac{\mathbb{Z}}{4\mathbb{Z}}}{\frac{2\mathbb{Z}}{4\mathbb{Z}}} = \left\{ [0]_4 + \frac{2\mathbb{Z}}{4\mathbb{Z}}, [1]_4 + \frac{2\mathbb{Z}}{4\mathbb{Z}} \right\}$$

è un campo).

- un campo  $(K, +, \cdot)$ , possedendo soltanto gli ideali banali  $\{0\}$  e  $K$ , possiede soltanto anelli-quotiente banali ( $\frac{K}{\{0\}}$  è isomorfo a  $K$ ;  $\frac{K}{K}$  è isomorfo all'anello zero).

**Proposizione 2.9.** *Dati due anelli  $(R, +, \cdot)$  e  $(R', +, \cdot)$  ed un omomorfismo di anelli  $f : R \rightarrow R'$ , allora  $\text{Ker}(f)$  è un ideale di  $(R, +, \cdot)$ .*

*Osservazione 2.10.* Si noti che la relazione di equivalenza  $\varepsilon_{\text{Ker}(f)}$  definita su  $R$  (associata all'ideale  $\text{Ker}(f)$ ) coincide con la relazione di equivalenza  $\kappa_f$  “nucleo dell'applicazione”  $f$ , definita nell'ambito della teoria delle applicazioni tra insiemi. Infatti, presi  $x, y \in R$ , allora:

$$\begin{aligned} x \varepsilon_{\text{Ker}(f)} y & :\Leftrightarrow x - y \in \text{Ker}(f) \Leftrightarrow f(x - y) = 0_{R'} \Leftrightarrow \\ & \Leftrightarrow f(x) = f(y) \Leftrightarrow: x \kappa_f y . \end{aligned}$$

Pertanto,  $[x]_{\kappa_f} = x + \text{Ker}(f) = [x]_{\varepsilon_{\text{Ker}(f)}}$  e quindi (come insiemi) si ha che:

$$\frac{R}{\text{Ker}(f)} = \frac{R}{\kappa_f} = \{x + \text{Ker}(f) \mid x \in R\} .$$

**Teorema 2.11. (Teorema Fondamentale dell'Omomorfismo tra anelli)** *Da-  
ti due anelli  $(R, +, \cdot)$  e  $(R', +, \cdot)$  ed un omomorfismo di anelli  $f : R \rightarrow R'$ , allora  
esiste un isomorfismo di anelli, che denotiamo con  $f^\#$ , canonicamente associato ad  
 $f$ , da  $(\frac{R}{\text{Ker}(f)}, +, \cdot)$  a  $(\text{Im}(f), +, \cdot)$ , (ben) definito nella maniera seguente:*

$$f^\#(x + \text{Ker}(f)) := f(x), \quad \forall x \in R .$$

*Più precisamente, un qualunque omomorfismo  $f : R \rightarrow R'$  di anelli si può fattoriz-  
zare nel prodotto operatorio di un omomorfismo suriettivo di anelli:*

$$\pi_f : R \twoheadrightarrow \frac{R}{\text{Ker}(f)}, \quad x \mapsto x + \text{Ker}(f) ,$$

*un isomorfismo di anelli:*

$$f^\# : \frac{R}{\text{Ker}(f)} \xrightarrow{\sim} \text{Im}(f), \quad x + \text{Ker}(f) \mapsto f(x) ,$$

*ed un omomorfismo iniettivo di anelli:*

$$j_f : \text{Im}(f) \hookrightarrow R', \quad y \mapsto y ,$$

*cioè,  $f = j_f \circ f^\# \circ \pi_f$ . In altre parole, il seguente diagramma è commutativo:*

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \downarrow \pi_f & & \uparrow j_f \\ \frac{R}{\text{Ker}(f)} & \xrightarrow{f^\#} & \text{Im}(f) \end{array}$$

**Esempio 2.12. (1)** Sia  $x_0$  un elemento fissato in un insieme non vuoto  $X$  e sia  $(R, +, \cdot)$  un anello. Per l'omomorfismo  $\text{ev}_{x_0} : R^X \rightarrow R$ , definito ponendo  $\text{ev}_{x_0}(f) := f(x_0)$ , si ha che:

$$\text{Im}(\text{ev}_{x_0}) = R, \quad \text{Ker}(\text{ev}_{x_0}) = \{f \in R^X \mid f(x_0) = 0_R\} ,$$

$$\frac{R^X}{\text{Ker}(\text{ev}_{x_0})} \text{ è isomorfo a } R .$$

**(2)** Siano  $(R_1, +, \cdot)$  e  $(R_2, +, \cdot)$  due anelli e sia  $(R_1 \times R_2, +, \cdot)$  l'anello prodotto diretto. Possiamo definire in modo naturale un omomorfismo:

$$\text{pr}_1 : R_1 \times R_2, \quad (x_1, x_2) \mapsto x_1 ,$$

detta *prima proiezione*, ed anche

$$\text{pr}_2 : R_1 \times R_2, \quad (x_1, x_2) \mapsto x_2 ,$$

detta *seconda proiezione*.

E' facile mostrare che:

$$\begin{aligned} \text{Im}(pr_1) &= R_1, \quad \text{Ker}(pr_1) = \{0\} \times R_2, \\ \text{Im}(pr_2) &= R_2, \quad \text{Ker}(pr_2) = R_1 \times \{0\}. \end{aligned}$$

pertanto, per il Teorema Fondamentale dell'Omomorfismo di anelli, si ha:

$$\frac{R_1 \times R_2}{\{0\} \times R_2} \xrightarrow{\sim} R_1, \quad \frac{R_1 \times R_2}{R_1 \times \{0\}} \xrightarrow{\sim} R_2.$$

• Sia  $(R, +, \cdot)$  un anello unitario, allora esiste sempre un omomorfismo canonico dall'anello degli interi  $\mathbb{Z}$  ad  $R$ , che conserva l'unità, definito nella maniera seguente:

$$\chi: \mathbb{Z} \rightarrow R, \quad k \mapsto k \cdot 1_R := \underbrace{1_R + 1_R + \dots + 1_R}_{k \text{ volte}},$$

(con  $\chi(1) = 1 \cdot 1_R = 1_R$ ). Se esiste un più piccolo intero positivo  $n$  tale che  $n \cdot 1_R = 0_R$ , allora diremo che *la caratteristica dell'anello  $R$  è uguale ad  $n$*  (in simboli,  $\text{ch}(R) := n$ ); se, invece, per ogni  $k > 0$  si ha che  $k \cdot 1_R \neq 0_R$ , allora diremo che *la caratteristica dell'anello  $R$  è uguale a 0* (in simboli,  $\text{ch}(R) := 0$ ).

**Proposizione 2.13.** *Sia  $(R, +, \cdot)$  un anello unitario. Allora:*

$$\begin{aligned} \text{ch}(R) = n &\Leftrightarrow \text{Ker}(\chi) = n\mathbb{Z}. \\ \text{ch}(R) = 0 &\Leftrightarrow \text{Ker}(\chi) = \{0\}, \quad \text{cioè } \chi \text{ è un omomorfismo iniettivo.} \end{aligned}$$

*Osservazione 2.14. (1)* Si noti che un dominio  $(D, +, \cdot)$  (cioè un anello commutativo unitario privo di divisori dello zero) può avere caratteristica 0 oppure un numero primo  $p$ . [Non può avere caratteristica  $n = a \cdot b$  (numero intero composto ovvero non primo) con  $1 < a, b < n$ , perché altrimenti  $a \cdot 1_D, b \cdot 1_D \in D$  sarebbero divisori dello zero in  $D$ ].

*(2)* Si noti che, come conseguenza del Teorema Fondamentale di Omomorfismo per gli anelli, se un anello  $(R, +, \cdot)$  ha caratteristica zero, allora  $R$  contiene un sottoanello (precisamente,  $\text{Im}(\chi)$ ) isomorfo a  $\mathbb{Z}$ . Mentre, se  $(R, +, \cdot)$  ha caratteristica positiva  $n$ , allora  $R$  contiene un sottoanello (precisamente,  $\text{Im}(\chi)$ ) isomorfo a  $\frac{\mathbb{Z}}{n\mathbb{Z}}$ .

**Esempio 2.15. (1)**  $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot)$  ha caratteristica  $n$ .

**(2)** Se  $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ , allora l'anello  $(R, +, \cdot)$  ha caratteristica 0.

**(3)** Sia  $S$  un insieme non vuoto. Allora  $(P(S), +, \cdot)$  ha caratteristica uguale a 2 (infatti, per ogni  $X \in P(S)$ ,  $X + X := X \Delta X = \emptyset$ ).

**(4)** Siano  $(R_1, +, \cdot)$  e  $(R_2, +, \cdot)$  due anelli unitari e sia  $(R_1 \times R_2, +, \cdot)$  l'anello prodotto diretto. Se uno dei due anelli ha caratteristica zero, allora anche  $(R_1 \times R_2, +, \cdot)$  ha caratteristica zero. Se invece entrambi gli anelli hanno caratteristica positiva, allora:

$$\text{ch}(R_1 \times R_2) = \text{mcm}(\text{ch}(R_1), \text{ch}(R_2)).$$

Ad esempio,

$$\text{ch}\left(\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}\right) = \text{mcm}\left(\text{ch}\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right), \text{ch}\left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right)\right) = 6.$$

\* \* \*

Tali argomenti (e le dimostrazioni dei risultati enunciati) si possono trovare nel Capitolo 4 di [PC].

[PC] Giulia Maria Piacentini Cattaneo, *Algebra. Un approccio algoritmico*. Decibel-Zanichelli, 1996.

\* \* \*