X Settimana

1. Elementi basilari della teoria degli anelli (I parte)

• Un *anello* $(R, +, \cdot\,)$ è un insieme non vuoto R dotato di due operazioni (binarie), denotate per semplicità con i simboli "+" e "·"

$$+\ : R \times R \to R\,, \quad (x, y) \mapsto x + y\,, \qquad \cdot\ : R \times R \to R\,, \quad (x, y) \mapsto x \cdot y\,,$$

che prendono il nome di *somma* e *prodotto*, e che verificano le seguenti proprietà:

(An1) *$(R, +)$ è un gruppo abeliano;*

(An2) *l'operazione di prodotto è associativa:*

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z\,, \quad \forall x, y, z \in R\,;$$

(An3) *valgono le leggi distributive:*

$$\begin{aligned} x \cdot (y + z) = &\quad (x \cdot y) + (x \cdot z)\,, \quad \forall x, y, z \in R \text{ (\textit{legge distributiva destra})};\\ (x + y) \cdot z = &\quad (x \cdot z) + (y \cdot z)\,, \quad \forall x, y, z \in R \text{ (\textit{legge distributiva sinistra})}. \end{aligned}$$

Osservazione 1.1. **(1)** Dato un anello $(R, +, \cdot\,)$, dalla teoria dei gruppi (poiché $(R, +)$ è un gruppo) si ricava che l'elemento neutro rispetto alla somma in un anello, detto *lo zero* ovvero *l'elemento nullo* dell'anello, è univocamente determinato ed è denotato con 0_R (ovvero, con 0, qualora ciò non dìa adito ad ambiguità).
Si noti, poi, che – come accade in $\mathbb{Z}$ – lo zero di un anello, rispetto al prodotto, agisce come un "annullatore universale", cioè:

$$x \cdot 0_R = 0_R = 0_R \cdot x\,, \quad \forall x \in R\,.$$

[Infatti,

$$\begin{aligned} x \cdot 0_R &= x \cdot (0_R + 0_R) = x \cdot 0_R + x \cdot 0_R \ \Rightarrow\\ &\Rightarrow\ 0_R = x \cdot 0_R - x \cdot 0_R = (x \cdot 0_R + x \cdot 0_R) - x \cdot 0_R =\\ &\qquad = x \cdot 0_R + (x \cdot 0_R - x \cdot 0_R) = x \cdot 0_R + 0_R = x \cdot 0_R\,.] \end{aligned}$$

(2) Dato un anello $(R, +, \cdot\,)$, coerentemente con il simbolismo introdotto nella teoria dei gruppi (con notazione additiva), per ogni intero naturale $k > 0$, poniamo:

$$\begin{aligned} kx := &\quad \underbrace{x + x + \ldots + x}_{k \text{ volte}}\,.\\ -kx := &\quad \underbrace{(-x) + (-x) + \ldots + (-x)}_{k \text{ volte}}\,. \end{aligned}$$

Se $k = 0$, poniamo $0x := 0_R$.

Se, oltre alle proprietà di base (cioè, **(An1)** , **(An2)** e **(An3)**), un anello verifica ulteriori proprietà, esso assume denominazioni particolari:

• *Un anello* $(R, +, \cdot\,)$ si dice *unitario* se possiede un elemento neutro rispetto al prodotto o unità moltiplicativa (diverso dall'elemento neutro rispetto alla somma), cioè se esiste un elemento, denotato con 1_R $(\neq 0_R)$, tale che:

$$x \cdot 1_R = x = 1_R \cdot x\,, \quad \forall x \in R\,.$$

• *Un anello* $(R, +, \cdot\,)$ si dice *commutativo* se l'operazione di prodotto è commutativa, cioè:

$$x \cdot y = y \cdot x\,, \quad \forall x, y \in R\,.$$

• Un anello $(R, +, \cdot\,)$ si chiama *un campo* se $(R^*, \cdot\,)$ forma un gruppo abeliano, dove $R^* := R \setminus \{0\}$ è l'insieme degli elementi non nulli di R.

E' ovvio che un campo è sempre un anello commutativo unitario.

• In un anello unitario $(R, +, \cdot\,)$ un elemento non nullo $x \in R$ si dice *invertibile (in R)* se esiste un elemento $x' \in R$, detto *inverso (moltiplicativo) di x,* in modo tale che:

$$x \cdot x' = 1_R = x' \cdot x\,.$$

Proposizione 1.2. *Sia $(R, +, \cdot\,)$ un anello unitario.*

(1) *L'unità di R è unica.*

(2) *Se un elemento $x \in R$ è invertibile allora l'inverso di x è univocamente determinato.*

Dimostrazione. **(1)** Se $1'_R, 1''_R$ sono entrambi unità di R, allora:

$$1'_R = 1'_R \cdot 1''_R = 1''_R\,.$$

(2) Se x', x'' sono entrambi inversi di x in R, allora:

$$x' = x' \cdot 1_R = x' \cdot (x \cdot x'') = (x' \cdot x) \cdot x'' = 1_R \cdot x'' = x''\,.$$

Osservazione 1.3. Conformemente a quanto fatto nel caso dei gruppi moltiplicativi, se $(R, +, \cdot\,)$ è un anello unitario allora, per ogni intero naturale $k > 0$ e per ogni $x \in R$, poniamo:

$$x^k := \underbrace{x \cdot x \cdot \ldots \cdot x}_{k \text{ volte}}\,.$$

Se, poi x è invertibile in R, allora:

$$x^{-k} := \underbrace{x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1}}_{k \text{ volte}}\,.$$

Se $k = 0$, poniamo $x^0 := 1_R$.

Esempio 1.4. **(0)** $(\{0\}, +, \cdot\,)$ è un anello, detto *anello zero* o *anello banale.*

(1) $(\mathbb{Z}, +, \cdot\,)$ e $(\mathbb{Z}[i], +, \cdot\,)$ sono anelli commutativi unitari (dove $\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$ ($\subsetneq \mathbb{C}$) è chiamato *l'anello degli interi di Gauss*).
$(\mathbb{Q}, +, \cdot\,)$, $(\mathbb{R}, +, \cdot\,)$, $(\mathbb{C}, +, \cdot\,)$ sono dei campi.

(2) $(\mathbb{N}, +, \cdot\,)$ *non* è un anello (infatti, $(\mathbb{N}, +)$ non è neanche un gruppo).

(3) Per ogni intero $n \geq 2$, consideriamo l'insieme-quoziente di $\mathbb{Z}$ rispetto alla relazione di equivalenza $\equiv_n$ (congruenza modulo n):

$$\frac{\mathbb{Z}}{\equiv_n} := \{[k]_n \mid k \in \mathbb{Z}\} = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}\,.$$

Allora, $(\mathbb{Z}/\equiv_n, +, \cdot\,)$ è un anello commutativo unitario (dove, $[x]_n + [y]_n := [x + y]_n$, $[x]_n \cdot [y]_n := [x \cdot y]_n$, $\forall x, y \in \mathbb{Z}$).
Ricordiamo che, come già osservato nell'ambito della teoria dei gruppi:

$$[k]_n = k + n\mathbb{Z} := \{k + nt \mid t \in \mathbb{Z}\}\,, \quad \forall k \in \mathbb{Z}\,.$$

Quindi, come abbiamo già visto:

$$\frac{\mathbb{Z}}{\equiv_n} = \frac{\mathbb{Z}}{n\mathbb{Z}} := \{k + n\mathbb{Z} \mid k \in \mathbb{Z}\} = \{n\mathbb{Z},\ 1 + n\mathbb{Z},\ 2 + n\mathbb{Z},\ \ldots,\ n - 1 + n\mathbb{Z}\}\,.$$

Si noti che, se n non è un numero primo (e soltanto in questo caso), nell'anello $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot\ )$ esistono elementi non nulli tali che il loro prodotto è uguale all'elemento nullo dell'anello. Precisamente, se $n = a \cdot b$, con $1 < a, b < n$, allora:

$$[a]_n \cdot [b]_n = [a \cdot b]_n = [a \cdot b]_n = [n]_n = [0]_n \,, \quad (\text{con} \quad [a]_n \neq [0]_n \,,\ [b]_n \neq [0]_n\,)\,.$$

In generale, in un anello $(R, +, \cdot\ )$, due elementi $a, b \in R$, tali che $a \neq 0$, $b \neq 0$ e $a \cdot b = 0$ si dicono *divisori dello zero nell'anello* $(R, +, \cdot\ )$.

(4) Sia $r \geq 2$ e sia $(R, +, \cdot\ )$ un anello (ad esempio, $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[i], \frac{\mathbb{Z}}{n\mathbb{Z}}\}$). L'insieme $\boldsymbol{M}_{r,r}(R)$ delle matrici quadrate ad r righe ed r colonne ad entrate in R, dotato delle operazioni di

(+) *somma*:

$$(a_{i,j}) + (b_{i,j}) := (a_{i,j} + b_{i,j})\,, \quad \forall (a_{i,j}), (b_{i,j}) \in \boldsymbol{M}_{r,r}(R)\,;$$

(·) *prodotto (righe × colonne)*:

$$(a_{i,j}) \cdot (b_{i,j}) := \left(\sum_{h=1}^{r} a_{i,h} \cdot b_{h,j} \right)\,, \quad \forall (a_{i,j}), (b_{i,j}) \in \boldsymbol{M}_{r,r}(R)\,;$$

costituisce un anello *non* commutativo (anche se $(R, +, \cdot\ )$ è un anello commutativo). Si noti che in tale anello sono presenti divisori dello zero (anche se R è privo di divisori dello zero).
Ad esempio, se $r := 2$ ed $R := \mathbb{Z}$, allora:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\,.$$

Si noti, tuttavia, che se $(R, +, \cdot\ )$ è un anello unitario, allora anche $(\boldsymbol{M}_{r,r}(R), +, \cdot\ )$ è un anello unitario, con unità (moltiplicativa) data dalla matrice:

$$I := (\delta_{i,j})\,, \quad \text{dove} \ \ \delta_{i,j} := 0_R\,, \ \ \text{se } i \neq j\,, \quad \text{e} \quad \delta_{i,i} := 1_R\,, \ \forall i\,, 1 \leq i \leq r\,.$$

Nel caso $r := 2$ la matrice unità dell'anello $(\boldsymbol{M}_{2,2}(R), +, \cdot\ )$ è data da:

$$I := \begin{pmatrix} 1_R & 0_R \\ 0_R & 1_R \end{pmatrix}\,.$$

(5) Sia S un insieme non vuoto. Allora $(\boldsymbol{P}(S), +, \cdot\ )$, dove:

$$X + Y := X \vartriangle Y := (X \cup Y) \setminus X \cap Y)\,, \ \ X \cdot Y := X \cap Y\,, \ \ \forall X, Y \in \boldsymbol{P}(S)\,,$$

è un anello commutativo unitario (dove $1_{\boldsymbol{P}(S)} := S$ e $0_{\boldsymbol{P}(S)} := \emptyset$).
Si noti che, in tale anello, ogni elemento ha come opposto se stesso:

$$2X := X + X = \emptyset = 0_{\boldsymbol{P}(S)} \quad \Rightarrow \quad -X = X\,, \quad \forall X \in \boldsymbol{P}(S)\,.$$

Si noti inoltre che, in tale anello, ogni elemento è *idempotente,* cioè:

$$X^2 := X \cdot X = X \cup X = X\,, \quad \forall X \in \boldsymbol{P}(S)\,.$$

(6) Sia X un insieme non vuoto ed $(R, +, \cdot\ )$ un anello (ad esempio, $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[i], \frac{\mathbb{Z}}{n\mathbb{Z}}\}$).
L'insieme $R^X := \{f : X \to R \mid f$ è un'applicazione$\}$, dotato delle *operazioni di somma e prodotto "definite puntualmente"*, precisamente date comunque due applicazioni $f, g \in R^X$:

(+) *la somma* $f + g$ è l'applicazione da X ad R definita nella maniera seguente:

$$(f + g)(x) := f(x) + g(x)\,, \quad \forall x \in X\,;$$

(·) *il prodotto* $f \cdot g$ è l'applicazione da X ad R definita nella maniera seguente:

$$(f \cdot g)(x) := f(x) \cdot g(x)\,, \quad \forall x \in X\,;$$

(dove la somma $f(x)+g(x)$ ed il prodotto $f(x)\cdot g(x)$, a secondo membro delle precedenti definizioni, sono operazioni effettuate nell'anello R) forma un anello (lo zero di tale anello è l'applicazione costante $\mathbf{0} : X \to R\,,\ x \mapsto 0_{R}\,,\ \ \forall x \in X\,,$ cioè $0_{R^X} := \mathbf{0}$).
Si noti che se $(R,+,\cdot\ )$ è un anello commutativo, allora $(R^X,+,\cdot\ )$ è anch'esso un anello commutativo.
Se $(R,+,\cdot\ )$ è un anello unitario, allora anche $(R^X,+,\cdot\ )$ è un anello unitario, con unità uguale all'applicazione costante $\mathbf{1} : X \to R\,,\ x \mapsto 1_{R}\,,\ \ \forall x \in X\,,$ cioè $1_{R^X} := \mathbf{1}$.
Si noti che, nel caso in cui X possieda almeno due elementi, $(R^X,+,\cdot\ )$ può avere divisori dello zero (anche se $(R,+,\cdot\ )$ non possiede divisori dello zero).
Ad esempio, se $R := \mathbb{Z}$, $X := \{a,b\}$ e se

$$\begin{array}{ll} f: & X \to \mathbb{Z}\,,\ a \mapsto 0\,,\ \ b \mapsto 1\,, \\ g: & X \to \mathbb{Z}\,,\ a \mapsto 1\,,\ \ b \mapsto 0\,, \end{array}$$

allora $f\cdot g = \mathbf{0}$, in quanto:

$$f\cdot g : X \to \mathbb{Z}\,,\ a \mapsto f(a)\cdot g(a) = 0\cdot 1 = 0\,,\quad b \mapsto f(b)\cdot g(b) = 1\cdot 0 = 0\,.$$

Quindi $f,g \in \mathbb{Z}^X$, $f \neq \mathbf{0}$, $g \neq \mathbf{0}$, però $f\cdot g = \mathbf{0}$.

(7) Siano $(R_1,+,\cdot\ )$ e $(R_2,+,\cdot\ )$ due anelli. Nell'insieme prodotto cartesiano $R_1 \times R_2$ possiamo definire, *componente per componente*, le operazioni di

(+) *somma*:

$(x_1,x_2)+(y_1,y_2) := (x_1+y_1, x_2+y_2)\,,\quad \forall (x_1,x_2),(y_1,y_2) \in R_1\times R_2\,;$

(·) *prodotto*:

$(x_1,x_2)\cdot(y_1,y_2) := (x_1\cdot y_1, x_2\cdot y_2)\,,\quad \forall (x_1,x_2),(y_1,y_2) \in R_1\times R_2\,.$

Con tali operazioni, l'insieme $R_1\times R_2$ acquista una struttura di anello $(R_1 \times R_2,+,\cdot\ )$, detto *anello prodotto diretto di* $(R_1,+,\cdot\ )$ *e* $(R_2,+,\cdot\ )$. Si noti ad esempio che lo zero di tale anello è dato da $0_{R_1\times R_2} := (0_{R_1}, 0_{R_2})$.
Si noti poi che, se $(R_1,+,\cdot\ )$ e $(R_2,+,\cdot\ )$ sono anelli commutativi allora $(R_1 \times R_2,+,\cdot\ )$ è anch'esso commutativo.
Si noti anche che, se $(R_1,+,\cdot\ )$ e $(R_2,+,\cdot\ )$ sono anelli unitari allora $(R_1\times R_2,+,\cdot\ )$ è anch'esso unitario (con $1_{R_1\times R_2} := (1_{R_1}, 1_{R_2})$).
Si noti infine che, se $(R_1,+,\cdot\ )$ e $(R_2,+,\cdot\ )$ sono non banali, allora $(R_1\times R_2,+,\cdot\ )$ possiede sempre divisori dello zero. Infatti , se $x \in R_1$, $x \neq 0$, e se $y \in R_2$, $y \neq 0$, allora $(x, 0_{R_2})\cdot(0_{R_1}, y) = (0_{R_1}, 0_{R_2})$.

• Un anello commutativo unitario privo di divisori dello zero viene chiamato *un dominio* (oppure, *un dominio di integrità*).

Si noti che:

$$\text{campo} \quad \Rightarrow \quad \text{dominio}$$

(infatti se, per assurdo, in un campo $a\cdot b = 0$ con $a \neq 0$ e $b \neq 0$, allora moltiplicando a sinistra per l'inverso a^{-1} di a, si ottiene $b = 1\cdot b = a^{-1}\cdot a\cdot b = a^{-1}\cdot 0 = 0$: contraddizione).
Non è vero il viceversa. Ad esempio,
– $(\mathbb{Z},+,\cdot\ )$, $(\mathbb{Z}[i],+,\cdot\ )$ sono domini, ma *non* sono campi.

Si osservi poi che:
– $(\mathbb{Q},+,\cdot\ )$, $(\mathbb{R},+,\cdot\ )$ e $(\mathbb{C},+,\cdot\ )$ sono campi.

– $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot\,\right)$ è un anello commutativo unitario, ma *non* è un dominio, se n non è un intero primo.

– $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}, +, \cdot\,\right)$ è un campo, se p è un intero primo.

Se $(R, +, \cdot\,)$ è un anello unitario arbitrario, non è detto che l'insieme degli elementi non nulli di R rispetto al prodotto, $(R^*, \cdot\,)$, costituisca un gruppo. Tuttavia, ad ogni anello unitario, può essere comunque associato un gruppo moltiplicativo (eventualmente banale), considerando l'insieme degli elementi invertibili di R: $(\mathbf{U}(R), \cdot\,)$. (Si noti che, comunque, $1_R \in \mathbf{U}(R)$.)
E' subito visto che $(R, +, \cdot\,)$ è un campo se e soltanto se $\mathbf{U}(R) = R^*$ e $(\mathbf{U}(R), \cdot\,)$ è un gruppo abeliano.

Esempio 1.5. **(1)** $(\mathbf{U}(\mathbb{Z}), \cdot\,) = (\{1, -1\}, \cdot\,)$ è un gruppo abeliano (mentre $(\mathbb{Z}^*, \cdot\,)$ non è un gruppo).

(2) $(\mathbf{U}(\mathbb{Z}[i]), \cdot\,) = (\{1, -1, i, -i\}, \cdot\,)$ è un gruppo abeliano (mentre $(\mathbb{Z}[i]^*, \cdot\,)$ non è un gruppo). (Si noti che $z := a + bi \in \mathbf{U}(\mathbb{Z}[i])$ se e soltanto se $1 = \mathrm{N}(z) = a^2 + b^2$, ovvero se e soltanto se $a = \pm 1$ e $b = 0$ oppure $a = 0$ e $b = \pm 1$.)

(3) Per ogni intero $n \geq 2$, l'insieme:

$$\mathbf{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) := \{[x]_n \mid \mathrm{MCD}(x, n) = 1\ ,\ 1 \leq x \leq n-1\}$$

(avente $\varphi(n)$ elementi) è un sottoinsieme dell'insieme-quoziente $\mathbb{Z}/n\mathbb{Z}$ (avente n elementi) e $\left(\mathbf{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right), \cdot\,\right)$ è un gruppo abeliano.
Ad esempio, se $n = 8$, allora $\mathbf{U}\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right) = \{[1]_8,\ [3]_8,\ [5]_8,\ [7]_8\} \subsetneq \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^*$. Mentre, se $n = 7$, allora $\mathbf{U}\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right) = \{[1]_7,\ [2]_7,\ [3]_7,\ [4]_7,\ [5]_7,\ [6]_7\} = \left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^*$.

(4) Sia K un campo $\left(\text{ad esempio } K \in \left\{\mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \frac{\mathbb{Z}}{p\mathbb{Z}}\right\}\right)$ e sia $(\boldsymbol{M}_{2,2}(K), +, \cdot\,)$ l'anello delle matrici quadrate con 2 righe e 2 colonne ad entrate nel campo K. Allora, $(\mathbf{U}(\boldsymbol{M}_{2,2}(K)), \cdot\,) = (\mathrm{GL}_2(K), \cdot\,)$ è il gruppo (non abeliano) delle matrici non singolari con 2 righe e 2 colonne ad entrate nel campo K

- Dato un sottoinsieme non vuoto S di un anello $(R, +, \cdot\,)$ è *un sottoanello di* $(R, +, \cdot\,)$ se S con le operazioni di R, ristrette agli elementi di S è un anello.

E' subito visto che S è un sottoanello di $(R, +, \cdot\,)$ se e soltanto se:

(S-An1) $\quad S - S \subseteq S \quad$ (cioè, $x - y \in S\ ,\ \ \forall x, y \in S$);

(S-An2) $\quad S \cdot S \subseteq S \quad$ (cioè , $x \cdot y \in S\ ,\ \ \forall x, y \in S$).

La prima condizione assicura che $(S, +)$ è un sottogruppo di $(R, +)$. La seconda condizione esprime il fatto che S è chiuso rispetto al prodotto di R, ciò basta affinché la proprietà associativa del prodotto (valendo in R) valga anche in S e le proprietà distributive del prodotto rispetto alla somma (valendo in R) valgano anche in S.

Si noti che un sottoanello di un anello commutativo [rispettivamente, privo di divisori dello zero] è ancora commutativo [rispettivamente, privo di divisori dello zero].

Un sottoanello di un anello unitario può anche non essere unitario, oppure se è unitario, può avere unità differente da quella dell'anello dato (vedi gli esempi sottostanti).

Un sottoanello di un campo non è detto che sia un campo.

Tutte le eventualità sopra prospettate sono illustrate negli esempi seguenti.

Esempio 1.6. **(0)** Dato un anello $(R,+,\cdot\,)$, allora $(\{0\},,+,\cdot\,)$ e $(R,+,\cdot\,)$ sono sottoanelli di $(R,+,\cdot\,)$ detti *sottoanelli banali.*

(1) Per ogni intero $n \geq 2$, $n\mathbb{Z}$ è un sottoanello (non unitario) di $(\mathbb{Z},+,\cdot\,)$, che è un anello unitario.
Si noti che un qualunque sottoanello non banale S di $(\mathbb{Z},+,\cdot\,)$ è di questo tipo e coincide, precisamente, con $s_0\mathbb{Z}$, dove s_0 è il più piccolo intero positivo appartenente ad S (la dimostrazione si basa sulla possibilità di effettuare una divisione con il resto in $\mathbb{Z}$).

(2) $\mathbb{Z}$ è un sottoanello unitario (non un campo) del campo $(\mathbb{Q},+,\cdot\,)$ (e l'unità del sottoanello coincide con quella dell'anello).
$\mathbb{Q}$ è un sottoanello unitario (che è un campo) del campo $(\mathbb{R},+,\cdot\,)$ (e l'unità del sottoanello coincide con quella dell'anello).
$\mathbb{R}$ è un sottoanello unitario (che è un campo) del campo $(\mathbb{C},+,\cdot\,)$ (e l'unità del sottoanello coincide con quella dell'anello).
$\mathbb{Z}[i]$ è un sottoanello (non un campo) del campo $(\mathbb{C},+,\cdot\,)$ (e l'unità del sottoanello coincide con quella dell'anello).

(3) Se S è un sottoanello di un anello $(R,+,\cdot\,)$, allora l'insieme $\boldsymbol{M}_{r,r}(S)$ delle matrici quadrate ad r righe ed r colonne ad entrate in S è un sottoanello dell'anello $(\boldsymbol{M}_{r,r}(R),+,\cdot\,)$.

(4) Sia S un insieme non vuoto e T un sottoinsieme non vuoto di S. Allora $\boldsymbol{P}(T)$ $(\subseteq \boldsymbol{P}(S)\,)$ è un sottoanello unitario dell'anello unitario $(\boldsymbol{P}(S),+,\cdot\,)$, però $1_{\boldsymbol{P}(T)} = T \neq 1_{\boldsymbol{P}(S)} = S$.

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

(6) 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 sottoanelli di $(R_1 \times R_2,+,\cdot\,)$. Si noti che, se $(R_1,+,\cdot\,)$ e $(R_2,+,\cdot\,)$ sono unitari, allora $R_1 \times \{0\}$ e $\{0\} \times R_2$ sono sottoanelli unitari dell'anello unitario $(R_1 \times R_2,+,\cdot\,)$, però $1_{R_1 \times \{0\}} := (1_{R_1}, 0_{R_2}) \neq (1_{R_1}, 1_{R_2}) =: 1_{R_1 \times R_2}$ e $1_{\{0\} \times R_2} := (0_{R_1}, 1_{R_2}) \neq (1_{R_1}, 1_{R_2}) =: 1_{R_1 \times R_2}$.

* * *

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.

* * *