

ALGEBRA 1 - 13/01/2021

ANELLI

Def. 1: (a) Si dice anello un insieme A con due operazioni $+$ e $\cdot$ tali che

$\boxed{+}$ $(A; +)$ è gruppo abeliano (= commutativo)

cioè $+$ è associativa

$$\exists 0 \in A : a + 0 = a = 0 + a \quad \forall a \in A$$

$$\forall a \in A, \exists (-a) \in A : a + (-a) = 0 = (-a) + a$$

$+$ è commutativa

$\boxed{\cdot}$ $(A; \cdot)$ è semigrupp *cioè* $\cdot$ è associativa

$\boxed{\cdot / +}$ $\cdot$ è distributiva a destra & sinistra rispetto a $+$

(b) Un anello A si dice

— commutativo se $\cdot$ è commutativo

— unitario se $(A; \cdot)$ è monoidale

cioè se $\exists 1 \in A : a \cdot 1 = a = 1 \cdot a, \quad \forall a \in A$

Def. 2: Sia A un anello.

(1) Un $a \in A$ si dice divisore di zero se

$a \neq 0$ & $\exists a' \in A, a' \neq 0$ t.e. $a \cdot a' = 0$ o $a' \cdot a = 0$

(2) A si dice integro se è privo di divisori di zero

(3) A si dice un dominio se è commutativo & integro

(4) Se A è unitario, un $a \in A$ si dice invertibile se

a è invertibile in $(A; \cdot)$, cioè $\exists a^{-1} \in A : a \cdot a^{-1} = 1 = a^{-1} \cdot a$

$\leadsto U(A) := U(A; \cdot) = \{a \in A \mid \exists a^{-1} \in A\}$

(5) A si dice un corpo se è unitario & $U(A) = A \setminus \{0\}$ ($=: A^*$)

(6) A si dice un campo se è un corpo commutativo
cioè A è unitario & commutativo & $U(A) = A \setminus \{0\}$

N.B.: $(A; +, \cdot)$ è campo $\Leftrightarrow \begin{cases} (A; +) \text{ è gruppo abeliano} \\ (A^*; \cdot) \text{ è gruppo abeliano} \\ \text{vale la } \boxed{D \cdot / +} \end{cases}$

NOTA: molte delle "proprietà abituali" dei calcoli tra numeri valgono anche per i calcoli in un qualsiasi anello: il prossimo Esercizio ne elenca alcune.

Esercizio 3: Hp: $(A; +, \cdot)$ è anello

Th: (1) $a \cdot 0 = 0 = 0 \cdot a$, $\forall a \in A$

(2) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$, $\forall a, b \in A$

(3) ($\forall A$ unitario) $(-1) \cdot a = -a = a \cdot (-1)$, $\forall a \in A$

(4) ($\forall A$ unitario) $0 \in U(A) \iff A = \{0\}$

(5) ($\forall A$ unitario) $\forall a \in A$, $a \in U(A) \iff (-a) \in U(A)$
con $(-a)^{-1} = -(a^{-1})$

(6) A è corpo $\implies A \neq \{0\}$ & A è integro

(7) A è campo $\implies A \neq \{0\}$ & A è dominio

Def. 4: $\forall$ anello $(A; +, \cdot)$, si dice sottoanello di A ogni sottoinsieme A' in A tale che A' sia anello rispetto a $+|_{A' \times A'}$ e $\cdot|_{A' \times A'}$ o, si scrive allora $A' \leq A$

Lemma 5 (CRITERIO per SOTTOANELLI):

[Hp:] A è anello, $A' \subseteq A$

[Th:] (1) $A' \leq A \iff \begin{cases} (A'; +|_{A' \times A'}) \text{ è sottogruppo di } (A; +) \\ (A'; \cdot|_{A' \times A'}) \text{ è sottomonoidi di } (A; \cdot) \\ \text{cioè } A' \cdot A' \subseteq A' \end{cases}$

(2) $A' \leq A \iff \begin{cases} A' \neq \emptyset & (\text{e } 0 \in A') \\ \forall a', a'' \in A', (a' - a'') \in A' \\ \forall a', a'' \in A', a' \cdot a'' \in A' \end{cases} \iff A' \leq (A; +)$

Def. 6: (a) $\forall$ anelli A, R si dice morfismo (di anelli)

da A ad R una funzione $\varphi: A \rightarrow R$ tale che
 $\varphi: (A; +) \rightarrow (R; +)$ e $\varphi: (A; \cdot) \rightarrow (R; \cdot)$ sono
morfismi (di gruppi / di semigrupp.)

$$\begin{aligned} \text{cioè } \varphi(a_1 + a_2) &= \varphi(a_1) + \varphi(a_2) & \forall a_1, a_2 \in A \\ \varphi(a_1 \cdot a_2) &= \varphi(a_1) \cdot \varphi(a_2) & \forall a_1, a_2 \in A \end{aligned}$$

(b) $\forall$ morfismo $\varphi: A \rightarrow R$ di anelli

IMMAGINE di $\varphi := \varphi(A) =: \text{Im}(\varphi) \quad (\subseteq R)$

NUCLEO di $\varphi := \varphi^{-1}(\mathcal{O}_R) =: \text{Ker}(\varphi) \quad (\subseteq A)$

(c) Uniamo le parole monomorfismo, epimorfismo e isomorfismo
di anelli in modo analogo a quanto si fa per i gruppi:

"epi-" := suriettivo, "mono-" := iniettivo, "iso-" := invertibile.

PROPOSIZIONE 7: $\boxed{\text{Hp:}}$ $\varphi: A \longrightarrow R$ è morfismo di anelli

$\boxed{\text{Th:}}$ (a) $\text{Im}(\varphi) = \{0_R\} \iff \varphi \text{ è banale (= costante)}$
 $\text{Ker}(\varphi) = A \iff (\text{cioè } \varphi(a) = 0_R, \forall a \in A)$

(b) $\text{Im}(\varphi) = R \iff \varphi \text{ è suriettivo}$

(c) $\text{Ker}(\varphi) = \{0_A\} \iff \varphi \text{ è iniettivo}$

Dim.: Segue dall'omologo risultato per il morfismo di gruppi $\varphi: (A; +) \longrightarrow (R; +)$

(cf. lezione del 16/12/2020).

□

Lemma 8: $\forall$ anello A , $\forall$ famiglia $\{A_i\}_{i \in I}$ di
 sottoanelli di A si ha $\bigcap_{i \in I} A_i \leq A$
 cioè l'intersezione di sottoanelli è un sottoanello.

Dim.: $A_i \leq A \Rightarrow (A_i; +) \leq (A; +) \Rightarrow$

$$\Rightarrow \left(\bigcap_{i \in I} A_i; + \right) \leq (A; +) \quad \text{ok per } +$$

INOLTRE $\left(\bigcap_{i \in I} A_i \right) \cdot \left(\bigcap_{i \in I} A_i \right) \stackrel{\text{ok}}{\subseteq} \bigcap_{i \in I} A_i$ ok per $\cdot$

$\cup$
 $a' \cdot a''$

$a' \cdot a'' \in \bigcap_{i \in I} A_i$
 $\uparrow$

con $a', a'' \in \bigcap_{i \in I} A_i \Rightarrow a', a'' \in A_i \Rightarrow a' \cdot a'' \in A_i$
 $\forall i \in I \quad \forall i \in I$ □

Def. 9: $\forall$ anello A , $\forall S \subseteq A$, si dice
 sottoanello di A generato da S il minimo (rip. a $\subseteq$)
 sottoanello di A contenente S .
Se $\exists$, tale minimo sottoanello è unico, indicato con $\langle S \rangle$.

Lemma 10: $\forall$ anello, $\forall S \subseteq A$,

$\exists \langle S \rangle$, dato da

$$(1) \quad \langle S \rangle = \bigcap_{\substack{A' \leq A \\ A' \supseteq S}} A' =: A_S$$

$$\begin{aligned} (1) + (2) \cdot (1_3 1_5 - 1_1) &= \\ &= 1_1 1_3 1_5 + (-1_1 1_1) + \\ &+ 1_2 1_3 1_5 + (-1_2 1_1) \end{aligned}$$

$$(2) \quad \langle S \rangle = \left\{ a \in A \mid \exists 1_j^{(i)} \in S : a = \sum_i \underbrace{\pm (1_{j_1}^{(i)} \cdots 1_{j_k}^{(i)})}_{(+1_{j_1}^{(i)}) \cdots (-1_{j_k}^{(i)})} \right\} =: A_{(S)}$$

Lemma 8

Dim.:

$$(1) \quad \boxed{1} \quad A_S := \bigcap_{\substack{A' \leq A \\ A' \geq S}} A' \leq A \quad \& \quad \underbrace{\forall A' \leq A : A' \geq S}_{\Downarrow} \quad \boxed{3} \quad A_S \subseteq A'$$

$$\boxed{2} \quad A_S \geq S$$

QUINDI: $\boxed{1}$ A_S è sottoretello di A , $\boxed{2}$ $A_S \geq S$

$$\boxed{3} \quad A_S \subseteq A', \quad \forall A' \leq A : A' \geq S$$

PERCIO' A_S ha le proprietà che definiscono $\langle S \rangle$,

precisamente $A_S = \min_{\subseteq} \{A' \mid A' \leq A, A' \geq S\}$

con $\min_{\subseteq} \{A' \mid A' \leq A, A' \geq S\} =: \langle S \rangle$

$$\langle S \rangle = A_S$$

□

$$(3) \quad \forall A' \leq A : A' \geq S \Rightarrow \underbrace{A' \geq S = \{\lambda \mid \lambda \in S\}}$$

&

$$A' \leq A \Rightarrow A' \cdot A' \leq A \Rightarrow \underbrace{A' \geq \{\lambda_1 \cdot \lambda_2 \cdots \lambda_k \mid \lambda_i \in S, \forall i\}}$$

&

$$A' \leq A \quad -A' \leq A' \Rightarrow \underbrace{A' \geq \{\pm(\lambda_1 \cdot \lambda_2 \cdots \lambda_k) \mid \lambda_j \in S, \forall j\}}$$

$$(A'; +) \leq (A; +)$$

$$A' \geq \underbrace{\left\{ \sum_{(i)} \pm (\lambda_1^{(i)} \lambda_2^{(i)} \cdots \lambda_{k_i}^{(i)}) \mid \lambda_j^{(i)} \in S, \forall j, i \right\}}_{=: A_{(S)}}$$

$$A' + A' \leq A'$$

QUINDI

$$\forall A' \leq A : A' \geq S \text{ si ha } \boxed{A_{(S)} \subseteq A'}$$

INFINE

*

$$\underline{A_{(S)} \leq A}$$

$\Rightarrow$

$$\boxed{A_{(S)}} = \min_{\subseteq} \{A'\}_{A' \geq S}^{A' \leq A} =: \boxed{\langle S \rangle}$$

OK

Infatti, la $*$ è vera perché

① $\emptyset \in A_{(S)}$, perché $\emptyset = \sum \text{di } \emptyset \text{ addendi}$

② $\forall \sum_{(i)} \pm (\tilde{\lambda}_1^{(i)} \dots \tilde{\lambda}_k^{(i)}), \sum_{(j)} \pm (\tilde{\lambda}_1^{(j)} \dots \tilde{\lambda}_h^{(j)}) \in A_{(S)}$

si ha
$$\left(\sum_{(i)} \pm (\tilde{\lambda}_1^{(i)} \dots \tilde{\lambda}_k^{(i)}) \right) - \left(\sum_{(j)} \pm (\tilde{\lambda}_1^{(j)} \dots \tilde{\lambda}_h^{(j)}) \right) =$$

$$= \left(\sum_{(i)} \pm (\tilde{\lambda}_1^{(i)} \dots \tilde{\lambda}_k^{(i)}) \right) + \left(\sum_{(j)} \mp (\tilde{\lambda}_1^{(j)} \dots \tilde{\lambda}_h^{(j)}) \right) \in A_{(S)}$$

③ $\forall \sum_{(i)} \pm (\tilde{\lambda}_1^{(i)} \dots \tilde{\lambda}_k^{(i)}), \sum_{(j)} \pm (\tilde{\lambda}_1^{(j)} \dots \tilde{\lambda}_h^{(j)}) \in A_{(S)}$

si ha
$$\left(\sum_{(i)} \pm (\tilde{\lambda}_1^{(i)} \dots \tilde{\lambda}_k^{(i)}) \right) \cdot \left(\sum_{(j)} \pm (\tilde{\lambda}_1^{(j)} \dots \tilde{\lambda}_h^{(j)}) \right) =$$

$$= \sum_{(i), (j)} \pm (\tilde{\lambda}_1^{(i)} \dots \tilde{\lambda}_k^{(i)} \cdot \tilde{\lambda}_1^{(j)} \dots \tilde{\lambda}_h^{(j)}) \in A_{(S)}$$

QUINDI ① + ② + ③ $\Rightarrow A_{(S)} \leq A$, q.e.d. $\square$

ESEMPLI & CONTROESEMPLI:

(1) $(\mathbb{N}; \max, \min)$ NON è anello

(2) $(\mathbb{Z}; \max, \min)$ NON è anello

(3) $(\mathbb{N}; +, \cdot)$ NON è anello

(4) $(\mathbb{Z}; +, \cdot)$ è anello $\begin{cases} \text{commutativo} \\ \text{unitario} \\ \text{integro} \end{cases}$ NON è campo

ma NON è corpo (campo)

(5) $(k \cdot \mathbb{Z}; +, \cdot)$ è sottanello di $\mathbb{Z}$

che è unitario $\Leftrightarrow k \in \{+1, -1\} \Leftrightarrow k\mathbb{Z} = \mathbb{Z}$

(6) $(\mathbb{Z}_n; +, \cdot)$ è anello $\begin{cases} \text{commutativo} \\ \text{unitario} \end{cases}$

MA $\mathbb{Z}_n$ è $\begin{cases} \text{integro (dominio)} \\ \text{campo} \end{cases} \iff n \text{ è primo}$

(7) $(\mathbb{Q}; +, \cdot)$ e $(\mathbb{R}; +, \cdot)$ sono CAMPI

(8) $(\mathcal{P}(E); \cup, \cap)$ NON è anello

(9) $(\mathcal{P}(E); \Delta, \cap)$ è anello $\begin{cases} \text{commutativo} \\ \text{unitario} \end{cases}$

ma NON è integro $\left(\begin{array}{l} \exists A, B \in \mathcal{P}(E) : A \neq \emptyset \neq B \\ \text{ma } A \cap B = \emptyset \\ \forall E : |E| \geq 2 \end{array} \right)$

(10) $\forall$ gruppo abeliano $(\Gamma; +)$,

$$\text{End}_g(\Gamma; +) = \{ \text{endomorfismi di } (\Gamma; +) \}$$

è anello unitario per $\oplus$ e $\circ$

$$\forall \varphi, \psi \in \text{End}(\Gamma), \quad (\varphi \oplus \psi)(\gamma) := \varphi(\gamma) + \psi(\gamma), \quad \forall \gamma \in \Gamma$$
$$(\varphi \circ \psi)(\gamma) := \varphi(\psi(\gamma)), \quad \forall \gamma \in \Gamma$$

(11) $\forall A_1, \dots, A_n$ anelli,

$\exists$ quello prodotto diretto $A_1 \times \dots \times A_n$ con

$$(a'_1, \dots, a'_n) + (a''_1, \dots, a''_n) := (a'_1 + a''_1, \dots, a'_n + a''_n)$$

$$(a'_1, \dots, a'_n) \cdot (a''_1, \dots, a''_n) := (a'_1 \cdot a''_1, \dots, a'_n \cdot a''_n)$$

$A_1 \times A_2 \times \dots \times A_n$ è $\begin{cases} \text{commutativo} \\ \text{unitario} \end{cases}$ se ogni A_i è $\begin{cases} \text{commutativo} \\ \text{unitario} \end{cases}$

(12) $\forall$ insieme E , $\forall$ anello A

$A^E := \{ f: E \rightarrow A \}$ è anello per

$$\forall h, k \in A^E, \quad \begin{aligned} (h+k)(e) &:= h(e) + k(e) & \forall e \in E \\ (h \cdot k)(e) &:= h(e) \cdot k(e) & \forall e \in E \end{aligned}$$

A^E è ~~commutativo~~ se A è ~~commutativo~~
unitario

(13) $\forall$ insieme E , sia $\underline{2} = \{0, 1\} = \mathbb{Z}_2$ (con + e ·)

$\Rightarrow \exists$ anelli $\mathbb{Z}_2^E = \underline{2}^E$ e $(\mathcal{P}(E); \Delta, \cap)$

ALLORA $\exists \phi: \mathcal{P}(E) \xrightarrow{\quad} \underline{2}^E = \mathbb{Z}_2^E$
 $F \mapsto \phi(F) := \chi_F \left(e \mapsto \begin{cases} \bar{1}, & \forall e \in F \\ \bar{0}, & \forall e \in E \setminus F \end{cases} \right)$

e tale ϕ è un isomorfismo di anelli !!!