Istituzioni di A & G — ALGEBRA, lezione 19

07/11/22

Morfismi di anelli

Definizione 17. *Siano A e A' due anelli. Un'applicazione $\varphi : A \to A'$ è detta* ***omomorfismo (o morfismo di anelli)*** *se per ogni $a, b \in A$ si ha:*

$$\varphi(a+b) = \varphi(a) + \varphi(b), \qquad \varphi(ab) = \varphi(a)\varphi(b).$$

Se φ è iniettivo è detto ***monomorfismo****, se è suriettivo è detto* ***epimorfismo****, se è biettivo è detto* ***isomorfismo****.*

Osserviamo che, anche se i due anelli A e A' possiedono entrambi l'unità, non si ha automaticamente che $\varphi(1_A) = 1_{A'}$. Un controesempio è dato dalla mappa

$$\begin{aligned} \varphi : \mathbb{Z} &\to M(2, \mathbb{Z}) \\ n &\mapsto \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

Quindi ha senso dare la seguente definizione.

Definizione 18. *Siano A e A' due anelli con unità. Un'applicazione $\varphi : A \to A'$ è detta omo-mono-epi-isomorfismo se è un omo-mono-epi-isomorfismo di anelli e se inoltre soddisfa la condizione*

$$\varphi(1_A) = 1_{A'}.$$

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow M(2, \mathbb{Z}) \\ n &\longrightarrow \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

$\varphi(n+m) = \begin{pmatrix} n+m & 0 \\ 0 & 0 \end{pmatrix} = \varphi(n) + \varphi(m)$ $\qquad$ $\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_M$

$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

Esempi.

- Le inclusioni $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ sono monomorfismi.
- La proiezione $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_p$ è un epimorfismo.

Proposizione 19. *Valgono le seguenti proprietà:*

1. *L'applicazione identità* $id : A \to A$ *è un omomorfismo.*
2. *~~Il~~ prodotto di due omomorfismi è un omomorfismo.*
   La composizione
3. *Se* $\varphi : A \to A'$ *è un omomorfismo, allora per ogni* $a \in A$*, per ogni* $n \in \mathbb{Z}$*, per ogni* $k \in \mathbb{N}$ *si ha:*
   - $\varphi(0_A) = 0_{A'}$;
   - $\varphi(-a) = -\varphi(a)$;
   - $\varphi(na) = n\varphi(a)$;
   - $\varphi(a^k) = (\varphi(a))^k$.

Definizione 20. *Sia $\varphi : A \to A'$ un omomorfismo di anelli. Si dice* **nucleo** *di φ il nucleo di φ come omorfismo di gruppi additivi, cioè*

$$\mathrm{Ker}(\varphi) = \{a \in A \mid \varphi(a) = 0_{A'}\}.$$

Esempio. Se A è un anello con unità si definisce un omomorfismo (detto **omomorfismo unitario**) nel seguente modo:

$$\begin{aligned} \mu : \mathbb{Z} &\to A \\ n &\mapsto n1_A \end{aligned}$$

Esso è l'unico omomorfismo possibile dall'anello $\mathbb{Z}$ ad A.

dim: sia $f : \mathbb{Z} \to A$ omomorfismo di anelli qualsiasi.

Allora $f(1) = 1_A$. Sia $n \in \mathbb{Z}$,

$$f(n) = f(n \cdot 1) = f(1 + \overset{n}{\dots} + 1) \underset{\substack{\uparrow \\ f \text{ omom}}}{=} f(1) + \overset{n}{\dots} + f(1) = n1_A = \mu(n)$$

$\Rightarrow f = \mu$

Proposizione 21. *Se A è un anello con unità di caratteristica 0, il morfismo unitario è iniettivo.*

dim: $\mu: \mathbb{Z} \to A$ morfismo unitario.

$\ker \mu = \{ n \in \mathbb{Z} \mid \mu(n) = 0_A \} = \{ n \in \mathbb{Z} \mid n \cdot 1_A = 0_A \}$

Allora, μ iniettivo $\iff \ker \mu = \{0\} \iff n \cdot 1_A \neq 0_A \quad \forall n \neq 0$

$\iff \operatorname{char}(A) = 0$

Proposizione 22. *Se A è un anello con unità di caratteristica $m > 0$, allora il nucleo del morfismo unitario è $\operatorname{Ker}(\mu) = m\mathbb{Z}$ e μ induce un omomorfismo iniettivo $\bar{\mu} : \mathbb{Z}_m \to A$.*

di anelli

dim: sia $\operatorname{char}(A) = m$

Vediamo che $\ker(\mu) = m\mathbb{Z}$

$\supseteq$/ ovvio: $\mu(m) = m \cdot 1_A = 0_A \Rightarrow m \in \ker(\mu)$

$\subseteq$/ sia $n \in \ker(\mu)$, divisione euclidea:

$\exists\, q, r$ tale che $n = m \cdot q + r \qquad 0 \leq r < m$

Allora $0 = \mu(n) = n \cdot 1_A = (m \cdot q + r) 1_A = (m \cdot q) 1_A + r \cdot 1_A =$

$= r \cdot 1_A \Rightarrow r = 0 \Rightarrow n \in m\mathbb{Z}$

A Anelli di gruppi abeliani, possiamo usare il I Teorema di isomorfismo:

Esiste $\bar{\mu}: \mathbb{Z}_m \to A$ omomorfismo iniettivo di <u>gruppi</u>

tale che

$$\begin{tikzcd} \mu : \mathbb{Z} \arrow[r] \arrow[d, "\pi"'] & A \\ \mathbb{Z}_m \arrow[ur, "\bar{\mu}"'] & \end{tikzcd}$$

Manca vedere che è un morfismo di anelli:

- $\bar{\mu}(\bar{1}) = \mu(1) = 1_A$.
- $\bar{\mu}(\bar{h} \cdot \bar{k}) = \bar{\mu}(\overline{h \cdot k}) = \mu(h \cdot k) = (h \cdot k) \cdot 1_A = (h \cdot 1_A) \cdot (k \cdot 1_A)$

$= \bar{\mu}(\bar{h}) \cdot \bar{\mu}(\bar{k})$.

Sottoanelli e ideali

Definizione 23. *Un sottoinsieme non vuoto S di un anello (risp. campo) A è detto* ***sottoanello*** *(risp.* ***sottocampo****) di A se è un anello (risp. campo) rispetto alla restrizione ad S delle operazioni di A.*

Criterio per sottoanelli. *Un sottoinsieme non vuoto S di un anello A è un suo sottoanello se e solo se valgono le seguenti condizioni:*

$$\forall\, x, y \in S : \underbrace{x - y \in S}_{\text{criterio di sottogruppo additivo}} \quad \text{e} \quad \underbrace{xy \in S}_{\text{stabile rispetto al prodotto}}.$$

Esempi.

i) • $n\mathbb{Z}$ è sottoanello di $\mathbb{Z}$ per ogni n;

ii) • l'**anello degli interi di Gauss** $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ è sottoanello di $\mathbb{C}$;

iii) • $\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b \in \mathbb{R} \mid a, b \in \mathbb{Z}\}$ è sottoanello di $\mathbb{R}$;

iv) • $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$ è sottocampo di $\mathbb{R}$;

i) osserv: tutti i sottoanelli di $\mathbb{Z}$ sono di questa forma

ii) $(a+ib), (c+id) \in \mathbb{Z}[i]$

1) $(a+bi) - (c+id) = \underbrace{(a-c)}_{\in \mathbb{Z}} + i\,(\underbrace{b-d}_{\in \mathbb{Z}}) \in \mathbb{Z}[i]$

2) $(a+bi)(c+di) = \underbrace{(ac-bd)}_{\in \mathbb{Z}} + i\,\underbrace{(ad+bc)}_{\in \mathbb{Z}} \in \mathbb{Z}[i]$

Proposizione 24. *Se* $\varphi : A \to A'$ *è un omomorfismo di anelli,* $\mathrm{Im}(\varphi)$ *è un sottoanello di* A'.

dim: sappiamo già che $\mathrm{Im}(\varphi)$ è sottogruppo additivo

Manca vedere: $x', y' \in \mathrm{Im}(\varphi) \Rightarrow \exists\, x, y \in A$ tale che

$\varphi(x) = x'$, $\varphi(y) = y'$. Dunque

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = x' \cdot y' \Rightarrow x' \cdot y' \in \mathrm{Im}(\varphi)$$

$\square$

Osserviamo che grazie al morfismo unitario μ dunque ogni anello con unità di caratteristica 0 contiene un sottoanello isomorfo a $\mathbb{Z}$, e ogni campo di caratteristica zero contiene un sottocampo isomorfo a $\mathbb{Q}$. Ogni campo di caratteristica p contiene un sottocampo isomorfo a $\mathbb{Z}_p$.

Il concetto di sottoanello non è sufficiente per generalizzare al caso degli anelli le costruzioni viste per i gruppi; per questo introduciamo dei nuovi oggetti.

Definizione 9. *Un sottoinsieme non vuoto I di un anello A si dice* ***ideale (o ideale bilatero)*** *di A se valgono le seguenti proprietà:*

1. *per ogni $x, y \in I$: $x - y \in I$;*
2. *per ogni $x \in$ e per ogni $a \in A$: $ax \in I$ e $xa \in I$.*

Osservazioni/esempi.

- Un ideale è in particolare un sottoanello.
- A e $\{0_A\}$ sono ideali detti impropri.
- $\mathbb{Z}$ è un sottoanello di $\mathbb{Q}$, ma non un suo ideale.
- Per ogni intero n, $n\mathbb{Z}$ è un ideale di $\mathbb{Z}$.
- Se un ideale I di A contiene 1_A, allora $I = A$.

Esempio. Nell'anello $\mathbb{R}[x]$ dei polinomi a coefficienti reali nell'indeterminata x, dimostriamo che l'insieme

$$\left\{p(x) = \textstyle\sum_{i\in\mathbb{N}_0} a_i x^i \in \mathbb{R}[x] \mid a_0 = 0\right\}$$

è un ideale.