ALGEBRA 1 - 20/01/2021

TEOREMA FONDAMENTALE DI OMOMORFISMO PER ANELLI

$\forall$ morfismo di anelli $\varphi : A \longrightarrow R$, il diagramma commutativo di funzioni tra insiemi

$$\begin{tikzcd}
A \arrow[rr, "\varphi"] \arrow[d, two heads, "\pi_\varphi"'] & & R \\
A/\rho_\varphi \arrow[rr, hook, two heads, "\cong", "\varphi_*"'] & & Im(\varphi) \arrow[u, hook, "j_\varphi"']
\end{tikzcd}$$

$$\begin{tikzcd}
a \arrow[rr, mapsto] \arrow[d, mapsto] & & \varphi(a) \\
{[a]_{\rho_\varphi} = a + Ker(\varphi)} \arrow[rr, mapsto] & & \varphi_*([a]_{\rho_\varphi}) \arrow[u, mapsto]
\end{tikzcd}$$

$[a]_{\rho_\varphi} = Ker(\varphi) + a$, $\quad \varphi_*([a]_{\rho_\varphi}) = \varphi(a)$, $\quad A/Ker(\varphi) = A/\rho_\varphi$

tutti gli insiemi sono anelli e tutte le funzioni sono morfismi. In particolare, π_φ è epimorfismo, j_φ è monomorfismo, e φ_* è isomorfismo, così $A/\rho_\varphi \cong Im(\varphi)$.

Dim.: Tutto segue dai fatti (già dimostrati):

1. A/ρ_φ è anello, con la struttura naturale di anello quoziente (perché ρ_φ è congruenza)

2. $Im(\varphi)$ è anello, in quanto sottoanello di R

3. Per il Teorema Fondamentale delle Applicazioni, le funzioni π_φ, φ_* e j_φ sono rispettivamente suriettiva, invertibile e iniettiva

4. Per il Teorema Fondamentale di Omomorfismo per semigruppi, le funzioni π_φ, φ_* e j_φ sono morfismi sia per la somma che per il prodotto

ALLORA 1 + 2 + 3 + 4 danno la tesi. $\square$

PROPOSIZIONE 1: $\boxed{Hp:}$ $\varphi : A \longrightarrow R$ morfismo di anelli

indichiamo con $\trianglelefteq_\bullet$ uno qualsiasi tra i simboli $\trianglelefteq_s$, $\trianglelefteq_D$ e $\trianglelefteq$

$\boxed{Th:}$ (a) $\quad B \leq A \implies \varphi(B) \leq \mathrm{Im}(\varphi) \leq R$

(b) $\quad S \leq R \implies A \geq \varphi^{-1}(S) \geq \mathrm{Ker}(\varphi)$

(c) $\quad B \leq A \implies \varphi^{-1}(\varphi(B)) = B + \mathrm{Ker}(\varphi) = \mathrm{Ker}(\varphi) + B$

(d) $\quad S \leq R \implies \varphi(\varphi^{-1}(S)) = S \cap \mathrm{Im}(\varphi)$

(e) $\quad I \trianglelefteq_\bullet A \implies \varphi(I) \trianglelefteq_\bullet \mathrm{Im}(\varphi)$

(f) $\quad J \trianglelefteq_\bullet R \implies \varphi^{-1}(J) \trianglelefteq_\bullet A$

(g) $\quad J \trianglelefteq_\bullet \mathrm{Im}(\varphi) \implies \varphi^{-1}(J) \trianglelefteq_\bullet A$

Dim.: $\boxed{1}$ Tutto ciò che riguarda gli aspetti relativi alla operazione di somma $+$ si ottiene applicando al gruppo (abeliano) $(A\,;+)$ l'analogo risultato relativo ai morfismi tra gruppi!

In particolare, le parti (b) e (c) sono già dimostrate...

$\boxed{2}$ Restano da verificare le proprietà relative al prodotto.

Ad esempio, verifichiamo:

$$(e)\quad I \trianglelefteq_{\bullet} A \quad \text{con} \quad \trianglelefteq_{\bullet} = \trianglelefteq_{s} \implies I \leq (A;+) \ \&\ A \cdot I \subseteq I \implies$$

$$\implies \varphi(I) \leq (\mathrm{Im}(\varphi);+) \text{ per il risultato relativo ai gruppi}$$

$$\& \quad \mathrm{Im}(\varphi)\cdot\varphi(I) = \varphi(A)\cdot\varphi(I) = \varphi(A\cdot I) \subseteq \varphi(I) \implies \text{OK}$$

... e analogamente per $\trianglelefteq_{\bullet} = \trianglelefteq_{D}$ e per $\trianglelefteq_{\bullet} = \trianglelefteq$

Tutte le altre parti dell'enunciato sono ESERCIZI. $\square$

COROLLARIO 2: $\boxed{\text{Hp:}}$ $\varphi : A \longrightarrow R$ è morfismo di anelli

$$\mathcal{S}_A := \{ S \mid S \leq A \}, \qquad \mathcal{S}_A^{\varphi} := \{ S \in \mathcal{S}_A \mid S \supseteq Ker(\varphi) \}$$

$$\mathcal{S}_R := \{ J \mid J \leq R \}, \qquad \mathcal{S}_{R,\varphi} := \{ J \in \mathcal{S}_R \mid J \subseteq Im(\varphi) \}$$

$$\mathcal{I}_A^{\bullet} := \{ I \mid I \trianglelefteq_{\bullet} A \}, \qquad \mathcal{I}_A^{\bullet\,\varphi} := \{ I \in \mathcal{I}_A^{\bullet} \mid I \supseteq Ker(\varphi) \}$$

$$\mathcal{I}_{R,\varphi}^{\bullet} := \{ J \mid J \trianglelefteq_{\bullet} Im(\varphi) \}$$

$\boxed{\text{Th:}}$ (a) $\exists$ ben definite funzioni

$$\mathcal{S}_A \xrightarrow{\sigma_\varphi} \mathcal{S}_R \quad (S \longmapsto \varphi(S)) \quad \text{t.c.} \quad Im(\sigma_\varphi) = \mathcal{S}_{R,\varphi}$$

$$\mathcal{S}_R \xrightarrow{\zeta_\varphi} \mathcal{S}_A \quad (J \longmapsto \varphi^{-1}(J)) \quad \text{t.c.} \quad Im(\zeta_\varphi) = \mathcal{S}_A^{\varphi}$$

(b) $\exists$ ben definite funzioni

$$\mathcal{J}^\bullet_A \xrightarrow{\nu^\bullet_\varphi} \mathcal{J}^\bullet_{R,\varphi} \quad (I \longmapsto \varphi(I)) \quad \text{t.c.} \quad \mathrm{Im}(\nu_\varphi) = \mathcal{J}^\bullet_{R,\varphi}$$

$$\mathcal{J}^\bullet_{R,\varphi} \xrightarrow{\mu^\bullet_\varphi} \mathcal{J}^\bullet_A \quad (J \longmapsto \varphi^{-1}(J)) \quad \text{t.c.} \quad \mathrm{Im}(\mu_\varphi) = \mathcal{J}^\bullet_A$$

(c) Le restrizioni di σ_φ e τ_φ danno biiezioni

$$\begin{tikzcd} \mathcal{S}^\varphi_A \arrow[r, bend left, "\sigma'_\varphi"] & \mathcal{S}_{R,\varphi} \arrow[l, bend left, "\tau'_\varphi"] \end{tikzcd}$$

inverse l'una dell'altra

(d) Le restrizioni di $\nu^\bullet_\varphi$ e $\mu^\bullet_\varphi$ danno biiezioni

$$\begin{tikzcd} \mathcal{J}^{\bullet\,\varphi}_A \arrow[r, bend left, "\hat{\nu}^\bullet_\varphi"] & \mathcal{J}^\bullet_{R,\varphi} \arrow[l, bend left, "\hat{\mu}^\bullet_\varphi"] \end{tikzcd}$$

inverse l'una dell'altra

$\boxed{\text{NOTE}}$ (1) Il Corollario 2 è l'analogo per gli anelli del risultato "parallelo" per i gruppi: come in quel caso, segue direttamente come conseguenza della Proposizione 1.

(2) Nel caso di un **epimorfismo** $\varphi : A \twoheadrightarrow R$ si ha $\mathcal{S}_{R,\varphi} = \mathcal{S}_R$ e $\mathcal{I}^\bullet_{R,\varphi} = \mathcal{I}^\bullet_R$ quindi il Corollario 2 si semplifica. In particolare, per gli anelli quoziente e per la proiezione $\varphi := \pi_I : A \twoheadrightarrow A/I$ con $I \trianglelefteq A$ si ha

COROLLARIO 3: Per ogni anello quoziente A/I $(I \trianglelefteq A)$, $\exists$ biiezione tra sottoanelli / ideali sinistri / ideali destri / ideali (bilateri) di A/I e sottoanelli / ideali sinistri / ideali destri / ideali (bilateri) di A che contengono I data da

$$\begin{pmatrix} A \supseteq \\ I \subseteq \end{pmatrix} \qquad \begin{array}{ccc} S & \longmapsto & \pi_I(S) = \{s+I \mid s \in S\} \\ \pi^{-1}(J) & \longleftarrow\!\shortmid & J \end{array} \qquad \left(\subseteq A/I \right)$$

CAMPO dei QUOZIENTI di un DOMINIO

OBIETTIVO dato un anello D, trovare un campo $Q(D)$ tale che

① $D \leq Q(D)$ ② $Q(D)$ è il minimo campo contenente D

N.B.: [$Q(D)$ è campo $\Rightarrow$ è dominio] & ① $\Rightarrow$ D deve essere dominio

IDEA generalizzare la costruzione $(\mathbb{Z}; +, \cdot) \rightsquigarrow (\mathbb{Q}; +, \cdot)$

STRATEGIA $\forall\, \delta \in D^* := D \setminus \{0\}$ $\rightsquigarrow$ "aggiungiamo" δ^{-1} in $Q(D)$

poi tutti i prodotti $d \cdot \delta^{-1}$, poi le somme ecc.

TECNICA $(D^*; \cdot)$ è semigruppo commutativo cancellativo

$\rightsquigarrow$ $\exists$ $G(D^*) :=$ gruppo "delle frazioni" di D^*

dato da $G(D^*) := D^* \times D^* / \eta = \{ d/\delta := [(d,\delta)]_\eta \mid (d,\delta) \in D^* \times D^* \}$

(vedasi lezione del 2/12/2020), secondo la ricetta che dà, ad esempio, $(\mathbb{Z}_1;+) = G(\mathbb{N}_+;+)$ $(\mathbb{Q}^*_+;\cdot) = G(\mathbb{N}_+;\cdot)$

<u>ALLORA</u> si deve ancora:

(1) <u>adattare</u> la costruzione $(D^*;\cdot) \rightsquigarrow (G(D^*);\cdot)$ includendo 0_D

(2) introdurre una "somma" tra frazioni

$\boxed{\text{TEOREMA 4}}$ $\forall$ dominio D, $\exists$ un campo $Q(D)$ e $\exists$ un monomorfismo di anelli $D \xhookrightarrow{j_D} Q(D)$ t.c. $\forall\, q \in Q(D)$, $\exists\, (d,\delta) \in D \times D^*$: $q = j_D(d) \cdot j_D(\delta)^{-1}$ in $Q(D)$

Dim.: Procediamo per passi, ciascuno di per sé elementare.

$\boxed{1}$ Definiamo in $D \times D^*$ le due operazioni

$$\left.\begin{aligned} (d',\delta') \odot (d'',\delta'') &:= (d'd'', \delta'\delta'') \\ (d',\delta') \oplus (d'',\delta'') &:= (d'\delta''+d''\delta', \delta'\delta'') \end{aligned}\right\} \in D \times D^*, \text{ perché } D \text{ è dominio}$$

$\boxed{2}$ Definiamo in $D \times D^*$ la relazione η data da

$$(d_1,\delta_1)\,\eta\,(d_2,\delta_2) \overset{\Delta}{\iff} d_1 \cdot \delta_2 = d_2 \cdot \delta_1$$

$\boxed{\text{IDEA:}}$ $(d_1,\delta_1)\,\eta\,(d_2,\delta_2) \iff$ " $d'/\delta' = d''/\delta''$ "

$\boxed{3}$ η è una equivalenza in $D \times D^*$ (calcoli!!!)

$\boxed{\text{N.B.:}}$ qui serve che D sia dominio, per la (T) !

$\boxed{\text{NOTAZIONE:}}$ $$d/\delta := [(d,\delta)]_\eta \in D \times D^* / \eta =: \boxed{Q(D)}$$

$\boxed{4}$ η è compatibile con le operazioni $\oplus$ e $\odot$ in $D \times D^*$

$\boxed{5}$ $\left[\boxed{1} + \boxed{3} + \boxed{4} + \text{teoria dei gruppoidi}\right] \Longrightarrow \exists$ ben definite in $Q(D) := D \times D^* / \eta$ le operazioni

$$d'/\delta' + d''/\delta'' := \left[(d', \delta') \oplus (d'', \delta'')\right]_\eta = (d'\delta'' + d''\delta') / (\delta'\delta'')$$

$$d'/\delta' \cdot d''/\delta'' := \left[(d', \delta') \odot (d'', \delta'')\right]_\eta = (d' \cdot d'') / (\delta' \cdot \delta'')$$

$\boxed{6}$ $(Q(D); +, \cdot)$ è un campo

CALCOLI!!! P. es., $\exists\ \emptyset_{Q(D)} = \emptyset_D / \delta$

$\forall\ d/\delta \in Q(D)$, $\exists\ -(d/\delta) = (-d)/\delta = d/(-\delta)$

& se $d/\delta \neq \emptyset_{Q(D)}$, $\exists\ (d/\delta)^{-1} = \delta/d$

$\boxed{7}$ $\exists$ la funzione $j_D : D \longrightarrow Q(D)$ data

da $j_D(d) := d^2/d \quad \forall\, d \in D^*$, $j_D(0_D) := 0_{Q(D)} = 0_D/\delta$

che è iniettiva ed è morfismo di anelli

N.B.: è anche $j_D(d) := d^2/d = \dfrac{d\cdot\delta}{\delta} \quad \forall\, \delta \in D^*$

in particolare <u>se</u> $\exists\ 1_D \in D\setminus\{0\}$ allora $j_D(d) = d/1_D$

$\boxed{8}$ $\forall\ d/\delta \in Q(D) := D\times D^*/\eta$, si fattorizza

$$d/\delta = d^2/d \cdot \delta/\delta^2 = d^2/d \cdot \left(\delta^2/\delta\right)^{-1} = j_D(d)\cdot j_D(\delta)^{-1}$$

$$\Longrightarrow \quad d/\delta = j_D(d)\cdot j_D(\delta)^{-1} \quad \text{in } Q(D)$$

con $(d,\delta) \in D\times D^*$, q.e.d. $\square$

Esempi 5:

(1) $D := \mathbb{Z} \implies Q(\mathbb{Z}) = \mathbb{Q}$

(2) $\forall$ campo K, si pone

$$Q(K[x]) =: K(x) = \left\{ h(x)/k(x) \;\middle|\; \begin{array}{l} h(x) \in K[x] \\ k(x) \in K[x] \setminus \{0\} \end{array} \right\} =$$

$\triangleq$ campo delle funzioni razionali in x a coefficienti in K

Esercizio 6:

(I) $\forall$ campo K si ha $Q(K) \cong K$

((Sugg.: dimostrare che $j_K : K \hookrightarrow Q(K)$ è suriettiva))

(II) $\forall$ dominio D si ha $Q(D[x]) \cong \big(Q(D)\big)(x)$

Ideali generati da un sottoinsieme:

$\boxed{\text{Def. 7}}$: $\forall$ anello A, $\forall$ sottoinsieme S $(\subseteq A)$, si dice ideale sinistro/destro/bilatero di A generato da S il minimo (rispetto a $\subseteq$) ideale sinistro/destro/bilatero di A che contenga S.

SE esiste, tale oggetto è unico, indicato rispettivamente con $(I)_s$ / $(I)_d$ / (I)

PROBLEMA: $\exists\ (I)_s\ /\ (I)_d\ /\ (I)$? E com'è fatto?

Lemma 8: $\forall$ anello A, $\forall$ famiglia $\{I_\sigma\}_{\sigma\in\Sigma}$ di ideali sinistri / destri / bilateri di A, l'intersezione $\bigcap_{\sigma\in\Sigma} I_\sigma$ è un ideale sinistro / destro / bilatero di A.

Dim.: Perfettamente analogo a quella per l'intersezione di sottoanelli! (ESERCIZIO!) $\square$

Proposizione 9: $\forall$ anello A, $\forall\, S \subseteq A$, si ha:

$\exists\, (S)_s$, descritto da $\displaystyle (S)_s = \bigcap_{\substack{I \trianglelefteq_s A \\ I \supseteq S}} I =$

$$= \left\{ \sum_h (\pm \sigma_h) + \sum_k a_k s_k \;\middle|\; a_k \in A,\ \sigma_h, s_k \in S,\ \forall\, h, k \right\}$$

$\exists\, (S)_d$, descritto da $\displaystyle (S)_d = \bigcap_{\substack{I \trianglelefteq_d A \\ I \supseteq S}} I =$

$$= \left\{ \sum_h (\pm \sigma_h) + \sum_k s_k a_k \;\middle|\; a_k \in A,\ \sigma_h, s_k \in S,\ \forall\, h, k \right\}$$

$\exists\, (S)$, descritto da $\displaystyle (S) = \bigcap_{\substack{I \trianglelefteq A \\ I \supseteq S}} I =$

$$= \left\{ \sum_h (\pm \sigma_h) + \sum_k a'_k s'_k + \sum_t s''_t a''_t + \sum_f a^+_f s_f a^-_f \;\middle|\; \begin{array}{l} \sigma_h, s'_k, s''_t, s_f \in S \\ a'_k, a''_t, a^\pm_f \in A \end{array} \right\}$$

NOTE 11: (a) $\forall$ anello A unitorio, la descrizione di $(S)_s$, (S_D) e (S) si semplifica molto.

(b) $\forall$ anello A commutativo si ha "$\trianglelefteq_s = \trianglelefteq_D = \trianglelefteq$", e così anche $(S)_s = (S)_D = (S)$

$\boxed{\textbf{Def. 11:}}$ (a) $\forall$ anello A, un ideale (bilatero) generato da un singolo elemento si dice (ideale) principale

(b) Un anello A si dice anello a ideali principali se ogni ideale in A è principale

$\boxed{\text{NOTE 12:}}$ (1) $\forall$ anello A commutativo unitario gli ideali principali sono tutti e soli i sottoinsiemi della forma

$$\alpha \cdot A := \{\alpha \cdot a \,/\, a \in A\} = (\alpha)\,, \qquad \forall\, \alpha \in A$$

(2) A è a ideali principali $\Longrightarrow$

$\Longrightarrow$ A/I è a ideali principali, $\forall\, I \trianglelefteq A$

Corollario 3 $\leadsto$ $\forall\, J \trianglelefteq A/_I\,,\ \exists\, J' := \pi_I^{-1}(J) \trianglelefteq A$ t.c.

$J = \pi_I(J')$, & $\exists\, \alpha \in A : J' = (\alpha)$; $\Longrightarrow$ $\mathbf{J = (\pi_I(\alpha))}$

(3) $\mathbb{Z}_1$ e $\mathbb{Z}_{1_n}$ $(\forall\, n \in \mathbb{N})$ sono a ideali principali

(4) <u>Controesempio</u>: $\mathbb{Z}[x]$ <u>non</u> è a ideali principali

P. es., $(2, x) := (\{2, x\}) = \{h(x)\cdot 2 + k(x)\cdot x \mid h, k \in \mathbb{Z}[x]\}$

è un ideale che <u>non</u> può essere generato da un singolo elemento, cioè <u>non</u> è principale!

Sia, p.a. $(2, x) = (\ell(x))$ per un certo $\ell(x) \in \mathbb{Z}[x]$

<u>ORA</u> $\{2\} \subseteq \{2, x\} \Rightarrow 2\cdot\mathbb{Z}[x] = (2) \subseteq (2, x) = (\ell(x)) = \ell(x)\cdot\mathbb{Z}[x]$

$\Rightarrow 2 \in \ell(x)\mathbb{Z}[x] \Rightarrow \exists\, t(x) : 2 = \ell(x)\cdot t(x) \Rightarrow \ell(x) \in \{\pm 1, \pm 2\}$

$\{x\} \subseteq \{2, x\} \Rightarrow$ (analogamente) $\exists\, f(x) : x = \ell(x)\cdot f(x) \Rightarrow$

$\Rightarrow \ell(x) \in \{\pm 1, \pm x\} \longrightarrow \ell(x) = \pm 1$

<u>MA</u> $\ell(x) = \pm 1 \Rightarrow 1 \in (\ell(x)) = (2, x) \Rightarrow 1 = \overbrace{h(x)\cdot 2 + k(x)\cdot x}^{(\text{termine noto}) \in 2\cdot\mathbb{Z}}$ $\lightning$