Svolgimento Es 1

$$(*)\begin{cases} 3x \equiv 9 \pmod{21} \\ 2x \equiv 3 \pmod{5} \end{cases}$$

Non è un sistema cinese (i.e. sist. di congruenze monomiche con moduli coprimi a 2 a 2) ma ci si può ricondurre.

Infatti

- I equazione di (*) $MCD(3, 21) = 3 \mid 9$ → compatibile
- II eq. (*) $MCD(2,5) = 1 \mid 3$ → compatibile
- $MCD(21,5) = 1$ ↓ $21 = 7 \cdot 3$

$\nvdash$ sistema riconducibile a un sistema cinese

$$(**)\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \end{cases}$$

con $MCD(m_1, m_2) = 1$ che è comp. con ! soluz. $(\text{mod } m_1 m_2)$

Come faccio?

I equazione

$3x \equiv 9 \pmod{21}$

$3 = 3 \cdot 1$
$9 = 3 \cdot 3$
$21 = 3 \cdot 7$

Compatibile

⇕

$\boxed{x \equiv 3 \mod 7}$ → I eq. semplificata

Oss { la soluzione è 3 in $\mathbb{Z}/7\mathbb{Z}$ campo (! soluzione)
tutte le altre in $\mathbb{Z}$ sono, $x = 3 + 7h$, $h \in \mathbb{Z}$

II equazione

$2x \equiv 3 \pmod 5$

$MCD(2,5) = 1 \Rightarrow$ 2 corrisponde ad un invertibile in $\mathbb{Z}/5\mathbb{Z}$

Ma infatti ponendo $\boxed{\overline{x} := [x]_{\mathrm{mod}\,5}}$ per semplicità

$$U(\mathbb{Z}/5\mathbb{Z}) = \mathbb{Z}/5\mathbb{Z} \setminus \{0\}$$

è gruppo ciclico moltiplicativo di ordine 4

$$U(\mathbb{Z}/5\mathbb{Z}) = \{\overline{2}, \overline{2}^2 = \overline{4}, \overline{2}^3 = \overline{8} = \overline{3}, \overline{2}^4 = \overline{16} = \overline{1}\}$$

$\overline{2}^4 = \overline{1} \Rightarrow \overline{2} \cdot \overline{2}^3 = \overline{1}$ i.e. $(\overline{2})^{-1} = \overline{2}^3 = \overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$

Infatti $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$

Perciò

$2x \equiv 3 \pmod 5 \iff \overline{2} \cdot x = \overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$

$\iff \overline{3} \cdot \overline{2}x = \overline{3} \cdot \overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$ campo

$\iff \boxed{\overline{x} = \overline{9} = \overline{4} \text{ in } \mathbb{Z}/5\mathbb{Z}}$ (unica soluz. di $\overline{2}x = \overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$)

II eq. diventa equiv a

$$\boxed{x \equiv 4 \pmod 5}$$ II equazione semplificata

Pertanto sistema (*) iniziale si riduce ad un Sistema ridotto (o di congruenze modulo moduli coprimi)

che è

$$(**) \begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 4 \pmod 5 \end{cases} \quad \text{con} \quad MCD(5,7) = 1$$

$\Rightarrow$ (**) compatibile con 1 soluzione (mod 35)

E' della forma

$$\begin{cases} X \equiv c_1 \pmod{r_1} \\ X \equiv c_2 \pmod{r_2} \end{cases} \quad \text{i.e.} \quad \begin{cases} X \equiv 3 \pmod 7 \\ X \equiv 4 \pmod 5 \end{cases}$$

Poniamo $R := r_1 \cdot r_2 \Rightarrow$ $\boxed{R = r_1 \cdot r_2 = 35}$

$R_1 := \frac{R}{r_1} = r_2$ e $R_2 := \frac{R}{r_2} = r_1 \Rightarrow$ $\boxed{\begin{matrix} R_1 = r_2 = 5 \\ R_2 = r_1 = 7 \end{matrix}}$

Allora notiamo che

$MCD(R_1, r_1) = 1 = MCD(R_2, r_2) \Rightarrow$ $\boxed{MCD(7,5) = 1}$

Ma allora consideriamo le congruenze

$R_1 \cdot x \equiv c_1 \pmod{r_1} \rightarrow \exists\,!$ sol. $x_1^0 \pmod{r_1}$

$R_2 \cdot x \equiv c_2 \pmod{r_2} \rightarrow \exists\,!$ sol. $x_2^0 \pmod{r_2}$

infatti $MCD(R_i, r_i) = 1 \mid c_i$, $\forall\, 1 \le i \le 2$

* Nello specifico

(1) $R_1 x \equiv c_1 \pmod{r_1} \iff 5x \equiv 3 \pmod 7$

cioè $\overline{5}x = \overline{3}$ in $\mathbb{Z}/7\mathbb{Z}$ $\quad (\overline{5})^{-1} = \overline{3}$ in $\mathbb{Z}/7\mathbb{Z}$

infatti $\overline{5} \cdot \overline{3} = \overline{15} = \overline{1}$ in $\mathbb{Z}/7\mathbb{Z}$

$\Rightarrow$ $x_1^0 = \overline{5}^{-1} \cdot \overline{3} = \overline{3} \cdot \overline{3} = \overline{9} = \overline{2} \Rightarrow$ $\boxed{x_1^0 \equiv 2 \pmod 7}$

(2) $R_2 x \equiv c_2 \pmod{r_2} \iff 7x \equiv 4 \pmod 5$ ($\overline{7} = \overline{2}$)

cioè $\overline{7} \cdot x = \overline{4}$ in $\mathbb{Z}/5\mathbb{Z} \iff \overline{2} \cdot x = \overline{4}$ in $\mathbb{Z}/5\mathbb{Z}$

Ma $(\overline{2})^{-1} = \overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$ perché $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$ in $\mathbb{Z}/5\mathbb{Z}$

$x_2^0 = \overline{3} \cdot \overline{4} = \overline{12} = \overline{2} \Rightarrow$ $\boxed{x_2^0 \equiv 2 \pmod 5}$

Pongo

$$x^0 := R_1 \cdot x_1^0 + R_2 \cdot x_2^0 = 5 \cdot 2 + 7 \cdot 2 = 10 + 14 = 24$$

Osservazioni

* x^0 soddisfa (***) $\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \end{cases}$

Infatti

(A) • $x^0 = R_1 x_1^0 + R_2 x_2^0 = m_2 \cdot x_1^0 + m_1 x_2^0 \equiv m_2 \cdot x_1^0 \pmod{m_1}$

Ma $m_2 \cdot x_1^0 = R_1 x_1^0 \equiv c_1 \pmod{m_1}$ da (1)

$\Rightarrow x^0 \equiv c_1 \pmod{m_1}$ come volevamo

Nello specifico

$$\begin{cases} x^0 = 24 = 5 \cdot 2 + 7 \cdot 2 \equiv 5 \cdot 2 \pmod{4} \\ 5 \cdot 2 \equiv 3 \pmod{4} \end{cases} \Rightarrow x^0 \equiv 3 \pmod{4}$$

$\Rightarrow 24 \equiv 3 \pmod{4}$ ✓ [in effetti $24 - 3 = 21 = 7 \cdot 3$]

(B) $x^0 = R_1 \cdot x_1^0 + R_2 \cdot x_2^0 \equiv m_1 x_2^0 \pmod{m_2}$

Ma $m_1 x_2^0 = R_2 x_2^0 \equiv c_2 \pmod{m_2}$

$\Rightarrow x^0 \equiv c_2 \pmod{m_2}$

Nello specifico

$$\begin{cases} x^0 = 24 \equiv 7 \cdot 2 \pmod{5} \\ 7 \cdot 2 \equiv 4 \pmod{5} \end{cases} \Rightarrow x^0 \equiv 4 \pmod{5}$$

$\Rightarrow 24 \equiv 4 \pmod{5}$ ✓ [in effetti $20 \equiv 0 \pmod{5}$]

* La soluzione $x^0 = 24$ è unica $(\text{mod } 7 \cdot 5) = (\text{mod } 35)$ (5)

Se y^0 è altre soluz. di sistema dove (**)

$\Rightarrow \quad y^0 \equiv x^0 \ (\text{mod } r_i), \ \forall \ 1 \le i \le 2$

$\Rightarrow \begin{cases} r_1 \mid (y^0 - x^0) \Rightarrow \exists \ t_1 \in \mathbb{Z} \text{ t.c. } (y^0 - x^0) = r_1 \cdot t_1 \\ r_2 \mid (y^0 - x^0) \Rightarrow r_2 \mid (y^0 - x^0) = r_1 \cdot t_1 \end{cases}$

Ma $MCD(r_1, r_2) = 1 \nRightarrow r_2 \nmid r_1$ in $\mathbb{Z} \Rightarrow r_2 \mid t_1$

$\nRightarrow \quad \exists \ t_2 \in \mathbb{Z} \text{ t.c. } \quad t_1 = r_2 t_2 \quad \Rightarrow$

$$y^0 - x^0 = r_1 r_2 \cdot t_2$$

$\Rightarrow \quad \boxed{y^0 = x^0 + r_1 \cdot r_2 \cdot t_2}$ come volevamo.

* Ritornando al sistema originale (*), devo trovare tutte le soluzioni incongruenti di (*) $(\text{mod } 21 \cdot 5) = (\text{mod } 105)$

Poiché

$$(*) \begin{cases} 3x \equiv 9 \ (\text{mod } 21) \\ 2x \equiv 3 \ (\text{mod } 5) \end{cases}$$

e le soluzioni di (**) in $\mathbb{Z}$ (equiv. a (*)) erano della forma

$$\boxed{X = x^0 + 35 \cdot h, \text{ con } \quad h \in \mathbb{Z}}$$

vedo che

$35 = 7 \cdot 5 \Rightarrow$

$105 = 21 \cdot 5 = 3 \cdot (7 \cdot 5) = \overline{h} \cdot 35 \nRightarrow \boxed{\overline{h} = 3}$

Abbiamo che per $0 \le h \le \overline{h} - 1$ trovo soluzioni minori di 105 per cui incongrue $(\text{mod } 105)$

- $h=0 \longrightarrow x^0 = 24$
- $h=1 \longrightarrow x^1 = x^0 + 35 \cdot 1 = 24+35 = 59$
- $h=2 \longrightarrow x^2 = x^0 + 35 \cdot 2 = 24 + 70 = 94$

Le 3 soluzioni sono → congruenti a 22 a 22 (mod 35)
→ incongruenti (mod 105)

Svolgimento esercizio 2

$$(*) \begin{cases} 2x \equiv 6 \pmod{20} \\ 3x \equiv 15 \pmod{18} \end{cases}$$

Notiamo che I eq. equiv. a $\begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 5 \pmod{6} \end{cases}$ (**

II eq. equiv. a

Non è ciniese perché $M.C.D.(10,6) = 2$

Però ricordo il risultato:

$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ è compatibile $\Leftrightarrow$ $M.C.D.(m,n) \mid (a-b)$

Inoltre ha 1 soluzione (modulo $m.c.m.(m,n)$)

dim

Comp. $\Leftrightarrow$ $\exists\ x_0 \in \mathbb{Z}$ t.c. $\begin{cases} x_0 \equiv a \pmod{m} \\ x_0 \equiv b \pmod{n} \end{cases} \Leftrightarrow \begin{cases} x_0 - a = mt \\ x_0 - b = ns \end{cases}$

$\Leftrightarrow \begin{cases} x_0 = a + mt \\ x_0 = b + ns \end{cases} \Leftrightarrow a + mt = b + ns \Leftrightarrow$

$a - b = m(-t) + n(s) \Leftrightarrow d = MCD(m,n) \mid (a-b)$

Se ora x_0, y_0 2 soluz. $\Rightarrow$ $m \mid (y_0 - x_0) \wedge n \mid (y_0 - x_0)$

$\Rightarrow$ $mcm(m,n) \mid (y_0 - x_0) \Leftrightarrow$ $y_0 = x_0 + mcm(m,n) \cdot h$, $h \in \mathbb{Z}$. ∎

$MCD(10,6) = 2 \mid 3-5 = -2 \Rightarrow$ sist. è compatibile

Prendo I equazione semplificata

$x \equiv 3 \pmod{10} \Rightarrow$ sol. gen. in $\mathbb{Z}$ è $\boxed{x = 3+10t}$, $t \in \mathbb{Z}$

Sostituisco nella II semplificata che era $x \equiv 5 \pmod 6$

$\Rightarrow$ $3+10t \equiv 5 \pmod 6$

$\Rightarrow$ $10t \equiv (5-3) \pmod 6$

$10t \equiv 2 \pmod 6$

$\bar{10}\,t = \bar{2}$ in $\mathbb{Z}/6\mathbb{Z} \Leftrightarrow \bar{4}\,t = \bar{2}$ in $\mathbb{Z}/6\mathbb{Z}$

$\Leftrightarrow$ $4t \equiv 2 \pmod 6$ $\Leftrightarrow$ (tutti divisibili per 2) $2t \equiv 1 \pmod 3$

Leggo la congruenza come equazione $\bar{2}\,t = \bar{1}$ in $\mathbb{Z}/3\mathbb{Z}$ campo

(2) ovvero in $\bar{2}\cdot\bar{2} = \bar{4} = \bar{1} \Rightarrow (\bar{2})^{-1} = \bar{2}$ in $\mathbb{Z}/3\mathbb{Z}$, perciò

$\bar{2}\,t = \bar{1}$ in $\mathbb{Z}/3\mathbb{Z} \Leftrightarrow t = \bar{2}$ in $\mathbb{Z}/3\mathbb{Z}$

$\Leftrightarrow$ $t \equiv 2 \pmod 3$ in $\mathbb{Z} \Leftrightarrow$ $\boxed{t = 2+3h}$, $h \in \mathbb{Z}$

* Risostituendo nell'espressione di x iniziale

$x = 3+10t = 3+10(2+3h) = 23+30h$, $h \in \mathbb{Z}$

$30 = \dfrac{10\cdot 6}{MCD(10,6)} = \dfrac{60}{2}$ $\Rightarrow$ $30 = mcm(10,6)$

infatti $\boxed{10 = 5\cdot 2 \ \text{e} \ 6 = 3\cdot 2}$

$\Rightarrow$ $\boxed{x_0 = 23 \ \text{è 1 soluz. di} \ (**) \pmod{30}}$

o ogni altra soluzione è della forma

$\boxed{x = 23+30h, \ h \in \mathbb{Z}}$

* Per trovare le incongrue di $(*) \pmod{20\cdot 18} = \pmod{360}$

Devo prendere soluzioni del tipo

$$23 \leq 23 + 30h < 360 \quad \lhd\rhd$$

$$0 \leq 30h < 337 \quad \lhd\rhd$$

$$0 \leq h < \frac{337}{30} \approx 11{,}23$$

$\Rightarrow$ $\boxed{0 \leq h \leq 11}$ $\Rightarrow$ ho 12 soluzioni incongrue (mod 360) che sono della forma

$$\{23 + 30h\}_{0 \leq h \leq 11} = \{23, 53, 83, 113, \ldots, 353\}$$

Svolgimento es. 3

(i) Se $I = (0)$ fine!

Se $I = \mathbb{K}[X] \Rightarrow I = (1)$ fine!

Sia $(0) \neq I \subsetneq \mathbb{K}[x]$ ideale qualsiasi non banale

Oss $\nexists\ a \in \mathbb{K}^* = \mathbb{K} \setminus \{0\}$ t.c. $a \in I$

altrimenti $\frac{1}{a} \in \mathbb{K} \subset \mathbb{K}[x]$ e $\frac{1}{a} \cdot \underset{\in I}{a} = 1 \in I \Rightarrow I = (1)$ # perché $I \subsetneq \mathbb{K}[x]$

Perciò $\forall\ f \in I \setminus \{0\} \Rightarrow \deg(f) > 0$

- Dato $\forall\ g \in I \Rightarrow g = a_0 + a_1 x + \dots + a_m x^m$, $a_m \in \mathbb{K}^*$, per $m > 0$

$\Rightarrow \frac{1}{a_m} \cdot g \in I$ ed è <u>monico</u>

(a meno di invertibili mi riduco a polinomi monici)

- Sia $m(x) \in I$ <u>monico</u> e di <u>grado minimo</u>

$D := \{ n \in \mathbb{N} \mid n = \deg(f),\ f \in I \} \subseteq \mathbb{N} \setminus \{0\}$

ha necessariamente minimo perché $\mathbb{N}$ è <u>ben ordinato</u>

$\forall\ f(x) \in I \Rightarrow \deg(f(x)) \geq \deg(m(x)) \Rightarrow$ in $\mathbb{K}[x]$

divisione Euclidea $\boxed{f(x) = m(x)\,q(x) + r(x)}$ con $0 \leq \deg(r(x)) < \deg(m(x))$

$\Rightarrow r(x) = \underset{\in I}{f(x)} - \underset{\uparrow I}{m(x)} \cdot \underset{\uparrow \mathbb{K}[x]}{q(x)} \in I \Rightarrow r(x) \in I$ e $\deg(r(x)) < \deg(m(x))$

$\Rightarrow$ se $r(x) \neq 0$ contraddico <u>minimalità di</u> $\deg(m(x))$

$\Rightarrow r(x) = 0 \Rightarrow f(x) = m(x) \cdot q(x) \Rightarrow \boxed{I = (m(x))}$

(ii) $\mathbb{K}[x]$ <u>quello commutativo unitario</u>

$I = (x)$ e $J = (x-1)$ <u>ideali in</u> $\mathbb{K}[x]$

Considero $\mathbb{K}[x] \xrightarrow{ev_0} \mathbb{K}$, $f(x) \longrightarrow f(0)$

- ev_0 suriettiva come applicazione
- $ev_0(f+g) = ev_0(f) + ev_0(g)$
- $ev_0(f \cdot g) = ev_0(f) \cdot ev_0(g)$

ω_0 è morfismo di anelli suriettivo

- $\ker(\omega_0) = \{ f(x) \in \mathbb{K}[x] \mid f(0) = 0 \} \overset{\text{Ruffini}}{=} \{ f(x) \in \mathbb{K}[x] \mid x \mid f(x) \text{ in } \mathbb{K}[x] \}$

$= \{ x \cdot g(x) \mid g(x) \in \mathbb{K}[x] \} = (x) = I$ per il punto (i).

- Per teorema di omomorfismo di anelli

$$\frac{\mathbb{K}[x]}{I} = \frac{\mathbb{K}[x]}{(x)} \cong (\mathbb{K}, +, \cdot) \text{ campo}$$

- Analogo con $\omega_1 : \mathbb{K}[x] \longrightarrow \mathbb{K} : f(x) \xrightarrow{\omega_1} f(1)$

$$\frac{\mathbb{K}[x]}{J} = \frac{\mathbb{K}[x]}{(x-1)} \cong (\mathbb{K}, +, \cdot) \text{ campo}$$

Osserviamo che

- $\mathbb{K}[x]$ è commutativo unitario
- $I = (x)$ e $J = (x-1)$ sono ideali coprimi in $\mathbb{K}[x]$

  i.e. $I + J = \mathbb{K}[x]$

  infatti

$$I + J = \{ f(x) \cdot x + g(x) \cdot (x-1) \mid f(x), g(x) \in \mathbb{K}[x] \}$$

$= (MCD(x, x-1))$ perché ogni ideale è principale come in (i)

$x-1$	x
x	1
-1	

$(x-1) = x \cdot 1 - 1$

$\Rightarrow 1 = x(1) + (x-1)(-1)$

$1 = MCD(x, x-1)$

- Ma allora dalla teoria svolta: $\mathbb{K}[x]$ comm. unitario, I e J coprimi

$\Rightarrow$ $\boxed{I \cap J = I \cdot J}$

cioè $\boxed{(x) \cap (x-1) = (x \cdot (x-1)) = (x^2 - x)}$

Ricorda (Infatti $I \cdot J \subseteq I \cap J$ per ogni coppia di ideali

Viceversa $I \cap J = (I \cap J) \cdot \mathbb{K}[x] = (I \cap J) \cdot (I + J) = I \cdot (I \cap J) + J \cdot (I \cap J) \subseteq I \cdot J$

(I e J coprimi; commutativo)

* Abbiamo un'applicazione $(ev_0 \times ev_1)$ — da prima $\cong \mathbb{K} \times \mathbb{K}$

$$\mathbb{K}[X] \xrightarrow{(ev_0 \times ev_1)} \frac{\mathbb{K}[x]}{I} \times \frac{\mathbb{K}[x]}{J}$$

$$f(x) \longrightarrow \big(f(x)+(x),\ f(x)+(x-1)\big) = \big(f(0), f(1)\big)$$

Morfismo suriettivo di anelli con $(\mathbb{K} \times \mathbb{K}, +, \cdot)$ prodotto diretto di campi con operaz. $(a,b)+(c,d) := (a +_{\mathbb{K}} c,\ b +_{\mathbb{K}} d)$ e $(a,b)\cdot(c,d) = (a \cdot_{\mathbb{K}} c,\ b \cdot_{\mathbb{K}} d)$

* $\ker(ev_0 \times ev_1) = \left\{ f(x) \in \mathbb{K}[x] \;\middle|\; \begin{cases} f(0) = 0 \\ f(1) = 0 \end{cases} \right\}$

$$= \left\{ f(x) \in \mathbb{K}[x] \;\middle|\; x \mid f(x) \text{ e } (x-1) \mid f(x) \text{ in } \mathbb{K}[x] \right\} =$$

$$= (x) \cap (x-1) = I \cap J = I \cdot J$$

$\downarrow$

I e J coprimi e $\mathbb{K}[x]$ com. unitario

Per Teorema Cinese tra Ideali coprimi

$$\boxed{\frac{\mathbb{K}[x]}{I \cdot J} \cong \frac{\mathbb{K}[x]}{I} \times \frac{\mathbb{K}[x]}{J}}$$

da prima con $(ev_0 \times ev_1)$

$$\boxed{\mathbb{K} \times \mathbb{K} \cong \frac{\mathbb{K}[x]}{(x)} \times \frac{\mathbb{K}[x]}{(x-1)} \cong \frac{\mathbb{K}[x]}{(x(x-1))}}$$

* $\mathbb{K}$ era campo $\Rightarrow$ privo di zero-divisori

$(\mathbb{K} \times \mathbb{K}, +, \cdot) \cong \frac{\mathbb{K}[x]}{(x\cdot(x-1))}$ ha zero divisori

Sia

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

$$\Rightarrow ev_0(f) = a_0 \equiv a_0 + x(a_1 + \cdots + a_n x^{n-1}) = a_0 + (x) \text{ in } \frac{\mathbb{K}[x]}{I}$$

$$ev_1(f) = f(1) \equiv (a_0 + a_1 + \cdots + a_n) + f'(1)\cdot(x-1) + \cdots + f^{(n)}(1)(x-1)^n$$

$$= (a_0 + \cdots + a_n) + (x-1) \text{ in } \frac{\mathbb{K}[x]}{J}$$

$$= b_0 + (x-1), \text{ con } \boxed{b_0 = a_0 + a_1 + \cdots + a_n}$$

in $\mathbb{K}[x]/J$

$$\mathbb{K}[x] \xrightarrow{ev_0 \times ev_1} \mathbb{K} \times \mathbb{K}$$

$$f(x) \longrightarrow (a_0, b_0)$$

Pertanto

$$\mathbb{K}[x] \xrightarrow{ev_0 \times ev_1} \mathbb{K} \times \mathbb{K} \cong \frac{\mathbb{K}[x]}{(x)} \times \frac{\mathbb{K}[x]}{(x-1)}$$

$$x \longrightarrow (0,-1) \neq 0$$

$$x-1 \longrightarrow (-1,0) \neq 0.$$

Ma $(0,1)\cdot(-1,0) = (0,0)$ in $\mathbb{K}\times\mathbb{K}$

infatti $(0\cdot(-1), (-1)\cdot 0) = (0,0)$

$$(0,1)\cdot(-1,0) = (ev_0 \times ev_1)(x\cdot(x-1)) = (0,0)$$

$(0,1)\cdot(-1,0)$: morfismi di anelli; $x\cdot(x-1)$: generatore $\ker(ev_0 \times ev_1)$

$\Rightarrow$ ho zero divisori in $(\mathbb{K}\times\mathbb{K}, +, \cdot)$

* Però non sono nilpotenti infatti $\frac{\mathbb{K}[x]}{(x(x-1))}$ è privo di nilpotenti

$\overline{a(x)} := a(x) + (x(x-1))$ per semplificare notazione

$\Rightarrow$ $\overline{a(x)} \in \frac{\mathbb{K}[x]}{(x(x-1))}$ è t.c. $\overline{a(x)}^k = 0 \iff a(x)^k \in (x(x-1))$ in $\mathbb{K}[x]$

$\iff$ $x\cdot(x-1) \mid a(x)^k$ in $\mathbb{K}[x]$ $\iff$ $x \mid a(x)^k$ e $(x-1) \mid a(x)^k$

Ma x è irriducibile in $\mathbb{K}[x]$ $\Rightarrow$ x è primo in $\mathbb{K}[x]$ $\Rightarrow$ $x \mid a(x)$ in $\mathbb{K}[x]$

$(x-1)$ è irriducibile in $\mathbb{K}[x]$ $\Rightarrow$ $(x-1) \mid a(x)$ in $\mathbb{K}[x]$ $\Rightarrow$ $(x-1) \mid a(x)$ in $\mathbb{K}[x]$

$\Rightarrow$ $a(x) = x(x-1)\cdot q(x)$ $\Rightarrow$ $\overline{a(x)} = \bar{0}$ in $\frac{\mathbb{K}[x]}{(x(x-1))}$

(iii) $I = (x)$ $\Rightarrow$ $I\cdot I = (x^2) \subsetneq I \cap I = (x)$

Provo come prima

$$\mathbb{K}[x] \xrightarrow{(ev_0 \times ev_0 \circ \frac{d}{dx})} \mathbb{K} \times \mathbb{K}$$

$$f(x) \longrightarrow (a_0, a_1)$$

se $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

Ora • $ev_0(f) = a_0$

• $\left(ev_0 \circ \frac{d}{dx}\right)(f(x)) = \left(a_1 + 2a_2 x + \dots + n a_n x^{n-1}\right)\Big|_{x=0} = a_1$

• ev_0 morfismo suriettivo di anelli $\mathbb{K}[x] \xrightarrow{ev_0} \mathbb{K}$

• Ma $\left(ev_0 \circ \frac{d}{dx}\right)$ non è morfismo di anelli (è solo additivo)

$$\left(ev_0 \circ \frac{d}{dx}\right)(f(x)+g(x)) = ev_0\left(f'(x)+g'(x)\right) = f'(0)+g'(0)$$

$$= \left(ev_0 \circ \frac{d}{dx}\right)(f(x)) + \left(ev_0 \circ \frac{d}{dx}\right)(g(x)) = a_1 + b_1$$

$$\left(ev_0 \circ \frac{d}{dx}\right)(f(x)\cdot g(x)) = ev_0\left(f\cdot g' + f'\cdot g\right) = a_0 b_1 + a_1 b_0$$

se $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

$g(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m$

non posso fare come prima!

Ma infatti **dimostriamo che**

$$\frac{\mathbb{K}[x]}{(x^2)} \not\cong (\mathbb{K}\times\mathbb{K}, +, \cdot)$$

infatti $\frac{\mathbb{K}[x]}{(x^2)}$ **ha elementi nilpotenti** (invece $(\mathbb{K}\times\mathbb{K},+,\cdot)$ NO! come visto in (ii))

Poniamo

$$\mathbb{K}[\varepsilon] := \{a + b\varepsilon \mid \varepsilon^2 = 0,\ a, b \in \mathbb{K}\}$$ con operazioni di anello così definite

$$(a+b\varepsilon) + (c+d\varepsilon) := (a +_{\mathbb{K}} c) + (b +_{\mathbb{K}} d)\varepsilon$$

$$(a+b\varepsilon)\cdot(c+d\varepsilon) := (a \cdot_{\mathbb{K}} c) + (a \cdot_{\mathbb{K}} d + b \cdot_{\mathbb{K}} c)\varepsilon \quad (\text{perché } \varepsilon^2 = 0)$$

Ora

$$\mathbb{K}[x] \xrightarrow{\varphi_\varepsilon} \mathbb{K}[\varepsilon]$$

applicazione

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \longrightarrow a_0 + a_1 \varepsilon$$

$$1 \longrightarrow 1$$

$$x \longrightarrow \varepsilon$$

$$\varphi_\varepsilon(f+g) = \varphi_\varepsilon(f) + \varphi_\varepsilon(g)$$

$$\varphi_\varepsilon(f\cdot g) = \varphi_\varepsilon\left((a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n)\cdot(b_0 + b_1 x + \dots + b_m x^m)\right)$$

$$= \varphi_\varepsilon(a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \dots) = a_0 b_0 + (a_0 b_1 + a_1 b_0)\varepsilon =$$

$$= (a_0 + a_1\varepsilon)\cdot(b_0 + b_1\varepsilon) = \varphi_\varepsilon(f(x))\cdot\varphi_\varepsilon(g(x))$$

STAVOLTA E' MORFISMO ANELLI

$$\ker(\varphi_\varepsilon) = \{ f(x) \in \mathbb{K}[x] \mid \varphi_\varepsilon(f(x)) = 0 \}$$

$$= \{ f(x) = a_0 + a_1 x + \dots + a_n \cdot x^n \mid a_0 \equiv a_1 = 0 \}$$

$$= \{ x^2 \cdot (a_2 + a_3 x + \dots + a_n x^{n-2}) \} = (x^2) \subset \mathbb{K}[x]$$

(da (i))

$$\Rightarrow \quad \frac{\mathbb{K}[x]}{(x^2)} \cong \mathbb{K}[\varepsilon]$$

In $\mathbb{K}[\varepsilon]$ tutti gli zero divisori sono nilpotenti

zero-divisori se e solo se

$$(a + b\varepsilon) \cdot (c + d\varepsilon) = 0 \iff \begin{cases} a \cdot_{\mathbb{K}} c = 0 \\ a \cdot d_{\mathbb{K}} + b \cdot_{\mathbb{K}} c = 0 \end{cases} \quad \text{in } \mathbb{K}$$

Poiché $\mathbb{K}$ campo $\Rightarrow$ $\nexists$ zero-divisori in $\mathbb{K}$ $\Rightarrow$

$$a \cdot_{\mathbb{K}} c = 0 \Rightarrow \begin{cases} a = 0 \\ c = 0 \end{cases}$$

se $a = 0$ $\Rightarrow$ $a \cdot_{\mathbb{K}} d + b \cdot_{\mathbb{K}} c = 0 \iff \boxed{b \cdot_{\mathbb{K}} c = 0}$

se $b = 0$ $\Rightarrow$ $a + b\varepsilon = 0$ era già zero in $\mathbb{K}[\varepsilon]$

se $c = 0$ e $b \neq 0$ $\Rightarrow$ $a + b\varepsilon = b\varepsilon$ ($b \neq 0$)

$c + d\varepsilon = d\varepsilon \rightarrow$ se $d = 0$ $\Rightarrow$ $c + d\varepsilon = 0$ era già 0

se $d \neq 0$ $\Rightarrow$ $d\varepsilon \neq 0$

$\Rightarrow$ $(b\varepsilon) \cdot (d\varepsilon) = bd\varepsilon^2 = 0$ zero divisori

Ma $(b\varepsilon)^2 = b^2\varepsilon^2 = 0$, $(d\varepsilon)^2 = d^2\varepsilon^2 = 0$ $\nearrow$ sono nilpotenti

Conta anche se $c = 0$