Svolgimento Esercizio 1

(i) $\mathbb{K}[x,y]$, $\mathbb{K}$ campo

$\forall\ P = (P_1, P_2) \in \mathbb{A}^2_{\mathbb{K}}$ consideriamo

$$ev_P : \mathbb{K}[x,y] \longrightarrow \mathbb{K}, \quad f(x,y) \longrightarrow f(P_1,P_2)$$

omomorfismo suriettivo anelli $\Rightarrow$

$\ker(ev_P)$ è ideale massimale in $\mathbb{K}[x,y]$

perché

$$\frac{\mathbb{K}[x,y]}{\ker(ev_P)} \cong \mathbb{K} \text{ campo } \{\mathbb{K}[x,y] \text{ comm. unitario}\}$$

Poiché $\mathbb{K}[x,y]$ commutativo unitario $\Rightarrow$ $\ker(ev_P)$ pure ideale primo

$$\ker(ev_P) := \{ f(x,y) \in \mathbb{K}[x,y] \mid f(P_1,P_2) = 0 \}$$

Siccome "derivate parziali" di polinomi sono definibili per ricorsività in $\mathbb{K}[x,y] \cong (\mathbb{K}[x])[y] \cong (\mathbb{K}[y])[x]$ ha senso parlare sviluppo Taylor $\Rightarrow$ $f(x,y) \in \ker(ev_P) \Leftrightarrow$

$$f(x,y) := f(P_1,P_2) + f_x(P_1,P_2)\cdot(x-P_1) + f_y(P_1,P_2)\cdot(y-P_2) +$$
$$f_{xx}(P_1,P_2)\cdot(x-P_1)^2 + f_{xy}(P_1,P_2)\cdot(x-P_1)\cdot(y-P_2) + f_{yy}^{(P_1,P_2)}(y-P_2)^2$$

($f(P_1,P_2) = 0$)

$+ - - - \ldots + - - - \ldots$

$$\Rightarrow \boxed{\ker(ev_P) := (x-P_1, y-P_2) := M_P}$$

(ii) Se $\mathbb{K}$ alg. chiuso e $I = (x-P_1, f(x,y))$ max per hp. $\Rightarrow$

$$\text{Campo} \longrightarrow \frac{\mathbb{K}[x,y]}{I} \cong \frac{\mathbb{K}[y]}{(f(P_1,y))} = \frac{\mathbb{K}[y]}{(\hat{f}(y))} \quad \text{dove } \hat{f}(y) = f(P_1,y) \in \mathbb{K}[y]$$

$\mathbb{K}[y]$ è PID e $\frac{\mathbb{K}[y]}{(\hat{f}(y))}$ campo $\Rightarrow \hat{f}(y) \in \mathbb{K}[y]$ è irriducibile** $\Rightarrow$ per Esercitazione Prof. Flamini Caratterizzazione irriducibili (18 Marzo 2025)

$\hat{f}(y) = (y-P_2)$ a meno invertibili

$$\Rightarrow \boxed{I = (x-P_1, f(x,y)) = (x-P_1, y-P_2)}$$

(iii) se invece $\mathbb{K} = \mathbb{R}$ $\quad I = (x - p_1,\ y^2 + 1)$ è max in $\mathbb{R}[x,y]$ non come di quella forma: $\dfrac{\mathbb{R}[x,y]}{I} \cong \dfrac{\mathbb{R}[y]}{(y^2+1)} \cong \mathbb{C} \Rightarrow a + bi$ con $i^2 = -1$

Più in generale $J^* = (x - p_1,\ y^2 + by + c)$ con $b^2 - 4c < 0$

caratterizz. irriduc. in $\mathbb{R}[y]$ Esercitaz. Prof. Flamini

J^* è un max in $\mathbb{K}[x,y]$ che non è della forma $I = (x - p_1, y - p_2)$

(iv) $J = (y - x^2) \subset \mathbb{K}[x,y]$

J è primo ma non max in $\mathbb{K}[x,y]$

Infatti $\mathbb{K}[x,y]$ comm. unitario

J primo $\Leftrightarrow$ $\dfrac{\mathbb{K}[x,y]}{J}$ dominio intero

J max $\Leftrightarrow$ $\mathbb{K}[x,y]/J$ è campo

$$\begin{array}{ccc} \mathbb{K}[x,y] & \xrightarrow{\varphi_t} & \mathbb{K}[t] \\ x & \longrightarrow & t \\ y & \longrightarrow & t^2 \\ f(x,y) & \longrightarrow & f(t,t^2) \end{array}$$

φ_t morfismo suriettivo a mezzi

$\ker(\varphi_t) = \{ f(x,y) \in \mathbb{K}[x,y] \mid f(t,t^2) \equiv 0 \} \neq \{0\}$ in $\mathbb{K}$

$f(x,y) = a_{00} + a_{10}x + a_{01}y + a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_{30}x^3 + \dots$

$f(t,t^2) = a_{00} + a_{10}t + a_{01}t^2 + a_{11}t^2 + a_{12}t^3 + a_{22}t^4 + a_{30}t^3 + \dots$

$= a_{00} + a_{10}t + (a_{01} + a_{11})t^2 + (a_{12} + a_{30})t^3 + \dots$

Perciò $\begin{cases} a_{00} = 0 \\ a_{10} = 0 \\ a_{11} = -a_{01} \\ a_{12} = -a_{30} \\ \vdots \end{cases} \Rightarrow f(x,y) = a_{01}(y - x^2) + a_{12}x(y - x^2) + \dots$

$\Rightarrow$ $\boxed{\ker(\varphi_t) = (y - x^2)}$ $\rightarrow$ principale

ideale principale è primo perché $\dfrac{\mathbb{K}[x,y]}{(y-x^2)} \cong \mathbb{K}[t]$ dominio intero

ideale non max perché $\mathbb{K}[t]$ no campo

(v) • $\mathbb{K}[x,y]$ non è PID perché in un PID primi = max

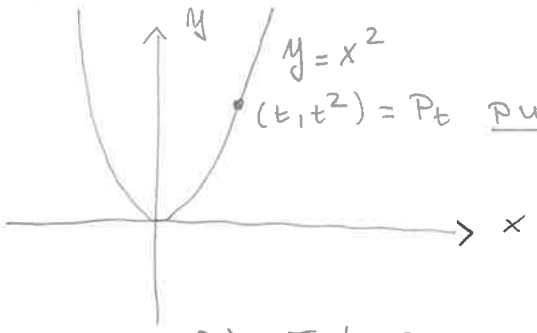
• $\mathbb{K}[x,y]$ è UFD perché $\mathbb{K}[x,y] \cong (\mathbb{K}[x])[y]$ e

$\mathbb{K}[x]$ PID (esercitazione Teorema Hilbert-Hazzidakis)

$\Rightarrow \mathbb{K}[x]$ è UFD $\Leftrightarrow (\mathbb{K}[x])[y]$ è UFD (A UFD $\Rightarrow A[x]$ UFD GAUSS)

• Poiché $(y-x^2)$ è ideale primo $\Rightarrow$ $y-x^2 \in \mathbb{K}[x,y]$ è elemento primo, ma allora irriducibile perché $\mathbb{K}[x,y]$ è dominio di integrità [a].

(vi) In $\mathbb{K}[x,y]$ se $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ $I = (y-x^2)$ è contenuto in infiniti massimali della forma $M_P = (x-t, y-t^2)$



$\forall t \in \mathbb{K}$ $M_{P_t} = (x-t, y-t^2)$ è t.c.

$(y-x^2) \subsetneq (x-t, y-t^2)$

$(y-x^2)$ primo non max

$(x-t, y-t^2)$ max

in $\mathbb{K}[x,y]$

infatti $y - x^2 = \underbrace{(x-t)[-(x+t)] + 1\cdot(y-t^2)}_{M_{P_t}}$, $\forall t \in \mathbb{K}$

Svolgimento Esercizio 2

(i) $\mathbb{Z}[x]$ non è PID ma è UFD (comportamento differente da $\mathbb{K}[x]$)

$\mathbb{Z}[x]$ è UFD perché $\mathbb{Z}$ è UFD (A UFD $\Rightarrow A[x]$ UFD)

Verifichiamo che $\mathbb{Z}[x]$ non è PID

Modo 1 $2 \in \mathbb{Z} \subset \mathbb{Z}[x]$ è irriducibile in $\mathbb{Z}[x]$ (polinomio costante e $U(\mathbb{Z}) = \{\pm 1\}$)

se $\mathbb{Z}[x]$ fosse PID $\Rightarrow$ $(2) \subset \mathbb{Z}[x]$ sarebbe max

Ma $\dfrac{\mathbb{Z}[x]}{(2)} \cong \mathbb{Z}_2[x]$

infatti $(2) = 2\,\mathbb{Z}[x] = \{a_0 + a_1 x + \dots + a_n x^n \mid 2 \mid a_j \ \forall\, 0 \le j \le n\}$

Perciò $[f(x)] \in \dfrac{\mathbb{Z}[x]}{(2)}$ è $f(x)$ con coeff. ridotti (mod 2)

$\mathbb{Z}_2[x]$ è dominio (PID) ma no campo $\Rightarrow$ $J=(2)$ primo massimale

Modo 2

$I = (2, x) \subset \mathbb{Z}[x] \Rightarrow \dfrac{\mathbb{Z}[x]}{I} \cong \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ campo

$\Rightarrow$ I max (e dunque pure primo)

Ora I non può essere principale

se p.a. fosse $f(x) \in \mathbb{Z}[x]$ t.c.

$$(f(x)) = (2, x)$$

$\Rightarrow$ $2 \in (f(x)) \Rightarrow \exists\, h(x) \in \mathbb{Z}[x]$ t.c. $2 = f(x)\cdot h(x)$

Ma $\deg(2) = 0 \Rightarrow f(x), h(x) \in \mathbb{Z}$ e

$f(x) = \begin{cases} \pm 1 \\ \pm 2 \end{cases}$ ⨳ perché $(2, x) = (f(x)) \subsetneq \mathbb{Z}[x]$

$\Rightarrow$ $f(x) = \pm 2 \sim 2$ (a meno inv. in $\mathbb{Z}$)

Ma allora anche $x \in (f(x)) \Rightarrow$ Dovrebbe $k(x) \in \mathbb{Z}[x]$ t.c.

$$x = 2 \cdot k(x)$$ ⨳ perché $k(x) \in \mathbb{Z}[x]$ ■

(ii) $J_1 = (2, x^2+1)$ non è primo in $\mathbb{Z}[x]$

Infatti

$\dfrac{\mathbb{Z}[x]}{J_1} \cong \dfrac{\mathbb{Z}_2[x]}{(x^2+\bar{1})}$ e $\mathbb{Z}_2[x]$ PID perché $\mathbb{Z}_2$ campo

$x^2+\bar{1} \in \mathbb{Z}_2[x]$ ha come radice $x_0 = \bar{1}$ infatti $\bar{1}+\bar{1} = \bar{0}$

$\Rightarrow$ $x^2+\bar{1} \in \mathbb{Z}_2[x]$ riducibile $\nRightarrow$ $(x^2+\bar{1})$ non primo $\Rightarrow$ $\dfrac{\mathbb{Z}_2[x]}{(x^2+\bar{1})}$ non dominio integro

$$\frac{\mathbb{Z}_2[x]}{(x^2+\bar{1})} = \mathbb{Z}_2[\varepsilon] = \{\bar{a} + \bar{b}\varepsilon \mid \bar{\varepsilon}^2 = -\bar{1} = \bar{1}\}$$

ψ

$(\bar{1}+\varepsilon) \neq \bar{0}$ ma $(\bar{1}+\varepsilon)^2 = \bar{1} + \bar{2}\varepsilon + \varepsilon^2 = \bar{1}+\bar{1} = \bar{2} = \bar{0}$ ($\bar{2}\varepsilon = 0$)

$\exists$ nilpotenti in $\mathbb{Z}_2[\varepsilon]$ $\Rightarrow$ no integro

(iii) $J_2 = (2, x^2+x+1)$ è max in $\mathbb{Z}[x]$ e dunque primo in $\mathbb{Z}[x]$

$$\frac{\mathbb{Z}[x]}{(2, x^2+x+1)} \cong \frac{\mathbb{Z}_2[x]}{(x^2+x+\bar{1})} := B$$

$\mathbb{Z}_2[x]$ PID e $x^2+x+\bar{1} \in \mathbb{Z}_2[x]$ irriducibile

infatti

se $\bar{x}_0 = \bar{0}$ $\quad \bar{0}+\bar{0}+\bar{1} \neq \bar{0}$

se $\bar{x}_0 = \bar{1}$ $\quad (\bar{1})^2+\bar{1}+\bar{1} = \bar{1} \neq \bar{0}$

$\Rightarrow$ $x^2+x+\bar{1}$ non ha radici in $\mathbb{Z}_2$ $\Rightarrow$ è irrid in $\mathbb{Z}_2[x]$

che è PID $\Rightarrow$ $(x^2+x+\bar{1})$ è ideale max in $\mathbb{Z}_2[x]$

$\Rightarrow$ quoziente B è campo $\Rightarrow$ poiché $\mathbb{Z}[x]$ commutativo unitario $\Rightarrow$ $J_2 = (2, x^2+x+1)$ è max e dunque primo in $\mathbb{Z}[x]$

(iv) Abbiamo già visto che (2) è solo ideale primo (ma non max) in $\mathbb{Z}[x]$

Per quanto ci furola

$$(x^2+x+1) \subset \mathbb{Z}[x]$$

Notiamo che

$$f(x) = x^2+x+1 \in \mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x]$$

e $\Delta = 1^2-4 < 0$ $\Rightarrow$ $x^2+x+1 \in \mathbb{R}[x]$ irriducibile in $\mathbb{R}[x]$ e monico

Inoltre

$$c(f) = MCD(1,1,1) = 1$$

perciò $f(x)$ è primitivo in $\mathbb{Z}[x]$

Non ha fattorizzazione non banale in $\mathbb{Q}[x]$ ($\mathbb{R}[x]$ è UFD)

e poiché primitivo a coeff. in $\mathbb{Z}[x]$ non ha fattorizzazione non banale in $\mathbb{Z}[x]$ $\Rightarrow$ $f(x)$ è irriducibile in $\mathbb{Z}[x]$

$\Rightarrow$ $f(x)$ è primo in $\mathbb{Z}[x]$ perché $\mathbb{Z}$ PID $\Rightarrow \mathbb{Z}$ è UFD

$\Rightarrow$ $\mathbb{Z}[x]$ è UFD (irrid = primi) $\Rightarrow$ $(f(x))$ ideale primo

Ma $(f(x))$ non max perché $(f(x)) \subsetneq J_2 = (2, x^2+x+1)$

dove J_2 max per (iii)

Svolgimento esercizio 3

(i) $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m \in \mathbb{Z}[x]$

$a_m \neq 0$ i.e. $\deg(f(x)) = m$

Sia $p \in \mathbb{Z}$ primo t.c.

$$p \nmid a_m, \quad p \mid a_i, \ \forall\, 0 \le i \le m-1 \ \text{e} \ p^2 \nmid a_0$$

Allora visto che $f(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ e $\mathbb{Q} = Q(\mathbb{Z})$

$f(x)$ è irriducibile in $\mathbb{Q}[x]$

Se $f(x)$ è primitivo cioè $c(f) = MCD(a_0, \dots, a_m) = 1$ (contenuto di f)

allora $f(x)$ è irriducibile pure in $\mathbb{Z}[x]$ *

dim

Supponiamo per assurdo $f(x)$ riducibile in $\mathbb{Q}[x] \Rightarrow \exists\, g(x), h(x) \in \mathbb{Q}[x]$ t.c.

$$f(x) = g(x) \cdot h(x)$$

$g(x) = b_0 + \dots + b_m x^m$ e $h(x) = c_0 + \dots + c_t x^t$

$b_j = \frac{p_j}{q_j} \in \mathbb{Q}$, $0 \le j \le m$ $\quad c_i = \frac{p'_i}{q'_i} \in \mathbb{Q}$, $0 \le i \le t$

che sono $p_j, q_j, p'_i, q'_i \in \mathbb{Z}$ e $\begin{cases} MCD(p_j, q_j) = 1 \\ MCD(p'_i, q'_i) = 1 \end{cases}$

Se prendiamo

$$Q := mcm(q_j) \quad \text{e} \quad Q' := mcm(q'_i)$$

$$\Rightarrow \quad Q \cdot g(x) = \widehat{p}_0 + \widehat{p}_1 x + \dots + \widehat{p}_m x^m, \quad Q' \cdot h(x) = \widehat{p}'_0 + \dots + \widehat{p}'_t x^t \in \mathbb{Z}[x]$$

Se no

$$P := MCD(\widehat{p}_0, \dots, \widehat{p}_m) \quad \text{e} \quad P' := MCD(\widehat{p}'_0, \dots, \widehat{p}'_t)$$

$$Q \cdot g(x) = P \cdot g^*(x), \quad Q' \cdot h(x) = P' \cdot h^*(x)$$

con $g^*(x), h^*(x) \in \mathbb{Z}[x]$ t.c.

$$c(g^*) = c(h^*) = 1 \quad \Rightarrow \text{primitivi}$$

$$\Rightarrow \quad g(x) = \left(\frac{P}{Q}\right) \cdot g^*(x) \quad \text{e} \quad h(x) = \left(\frac{P'}{Q'}\right) \cdot h^*(x)$$

$g(x) \underset{\text{associato in } \mathbb{Q}[x]}{\sim} g^*(x)$ $\qquad$ $h(x) \underset{\text{associato in } \mathbb{Q}[x]}{\sim} h^*(x)$

$h^*(x), g^*(x) \in \mathbb{Z}[x]$ primitivi

$\Rightarrow$

$$f(x) = \left(\frac{P\cdot P'}{Q\cdot Q'}\right) g^*(x)\cdot h^*(x) \quad \text{con} \quad \frac{\deg(g)=\deg(g^*)}{\deg(h)=\deg(h^*)}$$

$f(x) \in \mathbb{Z}[x]$; $\left(\frac{P\cdot P'}{Q\cdot Q'}\right) \in \mathbb{Q}$; $g^*(x)\cdot h^*(x) \in \mathbb{Z}[x]$

Sia $A = c(f) = MCD(a_0, \dots, a_m) \Rightarrow$

$f(x) = A \cdot f^*(x)$, $A \in \mathbb{Z}$ e $f^*(x) \in \mathbb{Z}[x]$ primitivo

Lemma di Gauss

$$c(b_1(x)\cdot b_2(x)) = c(b_1(x))\cdot c(b_2(x))$$

Perciò

$g^*(x)$ e $h^*(x)$ primitivi $\Rightarrow$ $g^*(x)\cdot h^*(x)$ primitivo

Ma allora

$$f^*(x) = \frac{1}{A}\cdot f(x) = \frac{1}{A}\left(\frac{PP'}{QQ'}\right)\cdot g^*(x)\cdot h^*(x)$$

$f^*(x) \in \mathbb{Z}[x]$ primitivo ; $g^*(x)\cdot h^*(x) \in \mathbb{Z}[x]$ primitivo

$\Rightarrow$ $\frac{PP'}{QQ'A} \in \mathbb{Z}$ e se fosse $m \in \mathbb{Z}\setminus\{\pm 1\}$ $\forall$ q primo, $q \mid m$

$\Rightarrow q \mid c(f^*)$ ✗ $\Rightarrow$ $\frac{PP'}{QQ'A} = \pm 1 \Rightarrow \frac{PP'}{QQ'} = \pm A$

$\Rightarrow$ $f(x) = A\cdot f^*(x) = \pm A\cdot g^*(x)\cdot h^*(x) \underset{\text{associato in } \mathbb{Z}[x]}{\sim} A\cdot g^*(x)\cdot h^*(x)$

e se $A \notin U(\mathbb{Z})$ anche A fa parte dei fatt. in $\mathbb{Z}$

i.e. $f(x) \underset{ass}{\sim} g^*(x)\cdot h^*(x)$ in $\mathbb{Z}[x]$ solo se $A \in U(\mathbb{Z})$

Pertanto

$f(x)$ riducibile su $\mathbb{Q}[x] \mapsto f(x)$ riducibile in $\mathbb{Z}[x]$

equiv.

$f(x)$ irriduc. in $\mathbb{Q}[x]$ $\Leftarrow\!\!\mid$ $f(x)$ irriduc. in $\mathbb{Z}[x]$

Dimostriamo sotto le condizioni di Eisenstein che $f(x) \in \mathbb{Z}[x]$ è irriducibile (così sarà irrid. pure in $\mathbb{Q}[x]$)

Se p.a. $f(x)$ fosse riducibile

(**) $\boxed{f(x) = \hat{g}(x) \cdot \hat{h}(x)}$ in $\mathbb{Z}[x]$, $\hat{g}, \hat{h} \in \mathbb{Z}[x]$

$\hat{g}(x) = \hat{b}_0 + \dots + \hat{b}_m x^m$, e $\hat{h} = \hat{c}_0 + \dots + \hat{c}_t x^t \in \mathbb{Z}[x]$

$$\deg(f) = n = \deg(\hat{g} \cdot \hat{h}) = m + t$$

Notiamo $a_0 = \hat{b}_0 \cdot \hat{c}_0$

* $p \mid a_0 \Rightarrow p \mid \hat{b}_0 \cdot \hat{c}_0 \underset{\text{primo in } \mathbb{Z}}{\Longrightarrow}$ o $p \mid \hat{b}_0$ o $p \mid \hat{c}_0$

* per hp $p^2 \nmid a_0 \Rightarrow$ se $p \mid \hat{b}_0$ allora $p \nmid \hat{c}_0$ e viceversa

i.e. p divide solo uno dei due

* Per hp $p \nmid a_n = \hat{b}_m \cdot \hat{c}_t \Rightarrow p \nmid \hat{b}_m$ e $p \nmid \hat{c}_t$

$\Rightarrow$ p non divide nè tutti i coeff di $\hat{g}(x)$ nè tutti i coeff. di $\hat{h}(x)$

Sia $i_0 = \min\{0, \dots, m\}$ t.c. $\boxed{p \mid \hat{b}_0, \dots, p \mid \hat{b}_{i_0-1} \text{ ma } p \nmid \hat{b}_{i_0}}$

Se considero il coeff. a_{i_0} di $f(x)$, dalla fattorizz. (**)

$$a_{i_0} = (\hat{b}_0 \cdot \hat{c}_{i_0} + \hat{b}_1 \cdot \hat{c}_{i_0-1} + \dots + \hat{b}_{i_0-1} \cdot c_1 + b_{i_0} \cdot c_0)$$

$$\Rightarrow \hat{b}_{i_0} \cdot \hat{c}_0 = a_{i_0} - (\hat{b}_0 \cdot \hat{c}_{i_0} + \dots + \hat{b}_{i_0-1} \cdot c_1) \quad (***)$$

* Se $i_0 < n \Rightarrow p \mid a_{i_0}$ per ipotesi di Criterio Eisenstein

Ma per def. di $i_0 \Rightarrow$ inoltre $p \mid \hat{b}_0, p \mid \hat{b}_1, \dots, p \mid \hat{b}_{i_0-1}$

di b_0 ma $p \nmid b_{i_0}$

$\Rightarrow p \mid \hat{b}_{i_0} \cdot \hat{c}_0$ da (***)

Ma per def. di i_0, $p \nmid b_{i_0} \Rightarrow p \mid \hat{c}_0$

Ma siccome $p \mid \hat{b}_0 \Rightarrow p \nmid \hat{c}_0$ perchè $p^2 \nmid a_0$ ✱

$\Rightarrow$ $f(x)$ è irriducibile in $\mathbb{Z}[x]$

* Se $\deg = n$

$\Rightarrow$ $m = n$ cioè $\deg(f) = \deg(\hat{g})$ e $\hat{h} = \alpha \in \mathbb{Z}$

$f(x) = \alpha \cdot \hat{g}(x)$ con $\hat{g}(x) \in \mathbb{Z}[x]$ irriducibile

Ma $f(x) = \alpha \cdot \hat{g}(x)$ è fattorizz non banale in $\mathbb{Z}[x]$ se $\alpha \notin U(\mathbb{Z})$

$f(x) = \alpha \cdot \hat{g}(x)$ è invece fattorizz. banale in $\mathbb{Q}[x]$ perché $\alpha \in \mathbb{Z} \subset \mathbb{Q} \Rightarrow \alpha \in U(\mathbb{Q})$

$\vdash\!\triangleright$ $f(x)$ irriducibile in $\mathbb{Q}[x]$

Notiamo inoltre

* $f(x) \in \mathbb{Z}[x]$ irriducibile $\vdash\!\triangleright$ $f(x)$ è primitivo

altrimenti se $c(f) \notin U(\mathbb{Z})$ avremo

$$f(x) = c(f) \cdot \underbrace{f^*(x)}_{\text{primitivo}}$$

sarebbe fatt non banale in $\mathbb{Z}[x]$ ⚡

* Se come prima

$\mathbb{Z}[x] \ni f(x) = \alpha \cdot \hat{g}(x)$ irriol. in $\mathbb{Q}[x]$, $\alpha \in \mathbb{Z}$

$\Rightarrow$ $\hat{g}(x)$ posso considerarlo $c(\hat{g}) = 1$

Ma $c(f) = c(\alpha) \cdot c(\hat{g}) = \alpha$

perciò se $\alpha = 1$

$f(x) = \hat{g}(x)$ pure irriol. in $\mathbb{Z}[x]$

i.e.

$f(x)$ primitivo come in Eisenstein

$f(x) \in \mathbb{Z}[x]$ irr. $\Longleftrightarrow$ $f(x) \in \mathbb{Q}[x]$ irriol

(ii) Per ogni numero primo $p \in \mathbb{Z}_+$ e per ogni intero $m \geq 1$ consideri

$$f_m(x) := p + px + px^2 + \dots + p \cdot x^{m-1} + x^m \in \mathbb{Z}[x]$$

Soddisfa Criterio Eisenstein rispetto al primo p ed inoltre

$c(f_m) = MCD(p, 1) = 1$

$\Rightarrow$ $f_m(x)$ irriducibile in $\mathbb{Q}[x]$ ed in $\mathbb{Z}[x]$

In particolare in $\mathbb{Q}[x]$ (a differenza di $\mathbb{R}[x]$ e di $\mathbb{C}[x]$ ricordare Esercitazione 18 Marzo Prof. Flaminio) esistono polinomi irriducibili di ogni grado $m \geq 1$

(iii) $q(x) = x^2 - 2 \in \mathbb{Z}[x]$ soddisfa criterio Eisenstein

per $p = 2$ $\Rightarrow$ $q(x)$ è irriducibile in $\mathbb{Q}[x]$

Siccome $c(q(x)) = MCD(-1, 0, -2) = 1$ $\Rightarrow$ $q(x)$ primitivo in $\mathbb{Z}[x]$

$\Rightarrow$ è irriducibile in $\mathbb{Z}[x]$

Invece in $\mathbb{R}[x]$ (e dunque in $\mathbb{C}[x]$) si ha

$$q(x) = (x - \sqrt{2}) \cdot (x + \sqrt{2}) \quad \text{riducibile}$$

* Perciò

$$\frac{\mathbb{R}[x]}{(x^2-2)} \quad \text{e} \quad \frac{\mathbb{C}[x]}{(x^2-2)} \quad \text{non domini integri}$$

* $\dfrac{\mathbb{Q}[x]}{(x^2-2)}$ è campo. Studiamo la struttura di questo campo

Gli elementi di $\dfrac{\mathbb{Q}[x]}{(x^2-2)} = \{ a + b\overline{x} \mid a, b \in \mathbb{Q} \text{ e } \overline{x}^2 = 2 \}$

* $(a + b\overline{x}) + (c + d\overline{x}) := (a+c) + (b+d)\overline{x}$
* $(a + b\overline{x}) \cdot (c + d\overline{x}) := (ac + 2bd) + (ad + bc)\overline{x}$
* $a + b\overline{x} \neq 0$:
  - $a \in \mathbb{Q}^* \Rightarrow a^{-1} = \frac{1}{a} \in \mathbb{Q}^*$
  - $b\overline{x}, b \in \mathbb{Q}^* \Rightarrow (b\overline{x})^{-1} = \frac{1}{2b}\overline{x}$
  - $a + b\overline{x}, a, b \in \mathbb{Q}^* \Rightarrow (a + b\overline{x})^{-1} = ?$

$$(a + b\overline{x})(c + d\overline{x}) = (ac + 2bd) + (ad + bc)\overline{x} = 1 \iff$$

$$\begin{cases} ad + bc = 0 \\ ac + 2bd = 1 \end{cases} \Rightarrow \begin{cases} ad = -bc \\ ac + 2bd = 1 \end{cases} \Rightarrow \begin{cases} d = \left(-\frac{b}{a}\right)c \\ ac + 2b\left(-\frac{b}{a}\right)c = 1 \end{cases}$$

$$\Rightarrow \quad c \cdot \left(\frac{a^2 - 2b^2}{a}\right) = 1 \quad \Rightarrow \quad c = \left(\frac{a^2 - 2b^2}{a}\right)^{-1}$$

Notiamo che

$$a^2 - 2b^2 \neq 0$$

altrimenti in $\mathbb{R}$ $\quad (a - \sqrt{2}\,b)(a + \sqrt{2}\,b) = 0$

$a = \sqrt{2}\,b \notin \mathbb{Q}$ e $a = -\sqrt{2}\,b \notin \mathbb{Q}$ ⁂

Perciò

$$c = \frac{a}{a^2 - 2b^2} \Rightarrow d = \left(-\frac{b}{a}\right) \cdot \frac{a}{a^2 - 2b^2} = -\frac{b}{a^2 - 2b^2}$$

$$\Rightarrow \quad (a + b\bar{x})^{-1} = \left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\,\bar{x}\right) \in \frac{\mathbb{Q}[x]}{(x^2 - 2)}$$

* $\dfrac{\mathbb{Z}[x]}{(x^2 - 2)}$ è dominio di integrità

$[f] = [a + bx] \iff f(x) - (a + bx) = (x^2 - 2) \cdot g(x)$

Tutti gli elementi sono rappresentabili come

$$a + b\bar{x} \mid a, b \in \mathbb{Z} \text{ e } \bar{x}^2 = 2 \in \mathbb{Z}$$

$+$ e $\cdot$ come caso precedente

Però NO CAMPO $\quad a \in \mathbb{Z} \setminus \{0, \pm 1\} \subset \dfrac{\mathbb{Z}[x]}{(x^2 - 2)}$ (# 0)

$\Rightarrow$ a non invertibile in $\mathbb{Z}$

a non invertibile in $\dfrac{\mathbb{Z}[x]}{(x^2 - 2)}$

Infatti $\quad a \cdot (c + d\bar{x}) = 1 \iff ac + ad\bar{x} = 1 \iff$

$\begin{cases} ac = 1 \Rightarrow c = a^{-1} \text{ in } \mathbb{Z} \text{ ⁂ perché } a \notin U(\mathbb{Z}) \\ ad = 0 \Rightarrow d = 0 \ (\mathbb{Z} \text{ intero}) \end{cases}$

(iv) $g(x) = x^2 + 10x + 25 \in \mathbb{Z}[x]$

$p = 5$ soddisfa (a) e (b) di Eisenstein ma $p^2 \mid a_0 = 25$ (no (c))

Ed inoltre $g(x) = (x + 5)^2$ in $\mathbb{Z}[x]$ e in $\mathbb{Q}[x]$ RIDUCIBILE

Non soddisfacendo Eisenstein

(v) Eisenstein criterio sufficiente ma non nec. per i RIBID.

$$r(x) = x^2 + 2x + 4 \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$$

$p = 2$ primo in $\mathbb{Z}$

$p \mid 4 = a_0$ e $p^2 \mid 4 = a_0$

$p \mid 2 = a_1$

$p \nmid 1 = a_2$

però

$$\mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x]$$

In $\mathbb{R}[x]$: $\Delta = 4 - 4 \cdot 4 = 4 - 16 < 0$

$r(x)$ è <u>irriducibile in $\mathbb{R}[x]$</u>

se ammettesse fattorizz. in $\mathbb{Q}[x] \subset \mathbb{R}[x]$

avrebbe una fattorizzazione in $\mathbb{R}[x]$ ⨯

$\mathbb{R}[x]$ è UFD.

$\Rightarrow$ $r(x)$ è <u>irriducibile in $\mathbb{Q}[x]$</u>

Essendo primitivo, è <u>irriducibile pure in $\mathbb{Z}[x]$</u>

<u>però non soddisfa criterio Eisenstein.</u>

(vii) $\forall$ primo $p \in \mathbb{Z}_+$

$$\Phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 \in \mathbb{Z}[x]$$

<u>è irriducibile in $\mathbb{Q}[x]$</u>

Notiamo che, con divisione euclidea in $\mathbb{Q}[x]$

$$\Phi_p(x) \cdot (x-1) = x^p - 1$$

$$\Rightarrow \boxed{\Phi_p(x) = \frac{x^p - 1}{x - 1}}$$

<u>Oss</u> Sia $T_{(x+1)} : \mathbb{K}[x] \longrightarrow \mathbb{K}[x]$

$f(x) \longrightarrow f_1(x) := f(x+1)$

$$T_{(x+1)}(f(x) + g(x)) = T_{(x+1)}(f(x)) + T_{(x+1)}(g(x))$$

<u>Morfismo anelli</u>

<u>T_{x+1} iniettivo</u> $T_{(x+1)}(f) = 0$

se $f(x) = a_0 + a_1 x + \dots + a_m x^m$

$\Downarrow$

$f(x+1) = a_0 + a_1(x+1) + \dots + a_m (x+1)^m \equiv 0$

$\Updownarrow$

$$\begin{cases} a_0 + a_1 + \dots + a_m = 0 \\ \\ a_n = 0 \end{cases}$$

sistema a scala con tutti pivots

$\Rightarrow$ $\boxed{a_i = 0 \ \forall i}$

$\Rightarrow$ $f(x) \equiv 0$ come elemento in $\mathbb{K}[x]$

$T_{(x+1)} : \mathbb{K}[x] \longrightarrow \mathbb{K}[x]$ $\Rightarrow$ $T_{(x+1)}$ isomorfismo di $\mathbb{K}[x]$ che conserva gradi degli elementi

Perciò

$T_{(x+1)}(x^p - 1) = (x+1)^p - 1 \in \mathbb{Q}[x]$

$T_{x+1}(x-1) = x \in \mathbb{Q}[x]$

$\Rightarrow$ Per Newton $(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k}$

$$T_{(x+1)}(\Phi_p) = \frac{(x+1)^p - 1}{x} = \frac{\binom{p}{0}x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p}x^0 - 1}{x}$$

$$= \frac{x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p-1}x + \cancel{1} - \cancel{1}}{x}$$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1} \cdot 1$$

$$= x^{p-1} + \underset{\| \, a_{p-2}}{p}\, x^{p-2} + \dots + \binom{p}{k}x^{p-k} + \dots + \underset{\| \, a_0}{p} = \Phi_p(x+1)$$

$p \mid a_0$

$p \mid a_{p-k}$

$\vdots$

$p \mid a_{p-2}$

$p \nmid a_{p-1}$

e $p^2 \nmid a_0 \Rightarrow$ per Eisenstein $\Phi_p(x+1)$ è irriducibile in $\mathbb{Q}[x]$ e in $\mathbb{Z}[x]$ perché primitivo

$\Phi_p(x+1) = T_{(x+1)}(\Phi_p(x))$

$\Rightarrow$ $T_{(x+1)}$ esiste anche che anche $\Phi_p(x)$ è irriducibile in $\mathbb{Z}[x]$