① $\mathbb{Q}[x,y]/(x-y,\ x^3+y^3-x)$

3° Th. Omo: A anello, $J \subseteq I$ ideali

$$A/I \simeq \frac{A/J}{I/J} = \frac{A/J}{\pi(I)}$$

Perché serve? Perché

$$A = \mathbb{Q}[x,y], \quad I = (x-y,\ x^3+y^3-x)$$

$$\Rightarrow J \in \{\underbrace{(x-y)}_{\text{BLL!}},\ \underbrace{(x^3+y^3-x)}_{\text{BRTT}}\}$$

TENTATIVO: $A/I \simeq \dfrac{A/J}{I/J}$

$$A/J = \frac{\mathbb{Q}[x,y]}{(x-y)} \simeq \mathbb{Q}[x]$$

↳ abbastanza chiaro

① $\varphi : \mathbb{Q}[x,y] \longrightarrow \mathbb{Q}[x]$, $p(x,y) \longmapsto p(x,x)$. Chiaramente $x-y \in \operatorname{Ker}\varphi$ e φ è surgettivo.

Manca da dim che $\operatorname{Ker}\varphi \subseteq (x-y)$

$\boxed{\subseteq}$ Sia $p \in \operatorname{Ker}\varphi$, cioè t.c. $p(x,x) = 0$, cioè

$$\sum_{i,j=0}^{N} a_{ij}\, x^i x^j = \sum_{i,j=0}^{N} a_{ij}\, x^{i+j} = 0$$

Voglio mostrare che $p \in (x-y)$, o equiv. che $p \equiv 0 \pmod{(x-y)}$

$$p(x,y) \equiv \sum_{i,j=0}^{N} a_{ij}\, x^i y^j \underset{x \equiv y \ (\mathrm{mod}\ (x-y))}{\equiv} \sum_{i,j=0}^{N} a_{ij}\, x^{i+j} \equiv 0 \pmod{(x-y)}$$

■

Per il 1° Th. Omo segue che $\mathbb{Q}[x,y]/(x-y) \simeq \mathbb{Q}[x]$

② $\beta : \mathbb{Q}[x] \longrightarrow \frac{\mathbb{Q}[x,y]}{(x-y)}$

Come la costruisco?

$\beta = p(x) \longmapsto \boxed{p(x) \bmod (x-y)}$

lo interpreto come polinomio in 2 var e poi modulo per $(x-y)$

(.1) $\operatorname{Ker}\beta = \{ p \overset{\in \mathbb{Q}[x]}{:} \beta(p) = \bar{p} = 0 \}$

$= \{ p \overset{\in \mathbb{Q}[x]}{:} x-y \mid p \}$

$= \{ p \in \mathbb{Q}[x] : p(x) = (x-y)\, q(x,y) \}$

Ma allora $\to q(x,y) = 0$ ✓

$\to \deg_y p = \deg_y q(x,y) + 1$ ASSURDO

(.2) β è surg: dato $f(x,y) = \sum_{i,j=0}^{N} a_{ij} x^i y^j$

devo mostrare che $f(x,y) + (x-y) = \beta(p(x))$

$$\underbrace{\sum_{i=1}^{n} a_{ij} x^{i+j}}_{\text{ecco } p!} + (x-y)$$

Dunque $\frac{\mathbb{Q}[x,y]}{(x-y,\ x^3+y^3-x)} \simeq \frac{\mathbb{Q}[x,y]/(x-y)}{J/(x-y)} \simeq \frac{\mathbb{Q}[x]}{\alpha(J)}$

dove $\alpha : \frac{\mathbb{Q}[x,y]}{(x-y)} \longrightarrow \mathbb{Q}[x]$

$p(x,y) \longmapsto p(x,x)$

$\Rightarrow \frac{\mathbb{Q}[x]}{\alpha(J)} \simeq \frac{\mathbb{Q}[x]}{(0,\ 2x^3-x)} \simeq \frac{\mathbb{Q}[x]}{(x(2x^2-1))}$

OSS: $(x) + (2x^2-1) = (x, 2x^2-1) = (1)$

Per il TCR allora $\dfrac{\mathbb{Q}[x]}{(x(2x^2-1))} \simeq \dfrac{\mathbb{Q}[x]}{(x)} \times \dfrac{\mathbb{Q}[x]}{(2x^2-1)}$

$$\simeq \mathbb{Q} \times \mathbb{Q}(1/\sqrt{2})$$

$$\simeq \mathbb{Q} \times \mathbb{Q}(\sqrt{2}). \quad \blacksquare$$

COPRIMALITÀ

Siano $I, J, K \trianglelefteq A$.

(i) Se $I + J + K = A$

allora $I^n + J^n + K^n = A \quad \forall n \geq 1$

(ii) Se $I + J = I + K = J + K = A$

allora $IJ + JK + KI = A$.

DIM

(i) $\exists\, i \in I, j \in J, k \in K$ t.c. $i + j + k = 1$

La tesi è: $\exists\, i_n \in I^n, j_n \in J^n, k_n \in K^n$

t.c. $i_n + j_n + k_n = 1$.

PRIMO TENTATIVO: elevo alla n $\quad$ ($n=2$ per semplicità)

$$\underset{\substack{\Uparrow\\ I^2}}{i^2} + \underset{\substack{\Uparrow\\ J^2}}{j^2} + \underset{\substack{\Uparrow\\ k^2}}{k^2} + \underset{\substack{\Uparrow\\ IJ}}{2ij} + \underset{\substack{\Uparrow\\ Ik}}{2ik} + \underset{\substack{\Uparrow\\ JK}}{jk} = 1$$

NON FUNZIONA PER COLPA LORO

Se elevo alla N

$$1^N = 1 = (i + j + k)^N = \sum_{a+b+c=N} \binom{N}{a\ b\ c} i^a j^b k^c$$

Voglio fare in modo che almeno uno tra a, b, c sia $\geq n$

$\Rightarrow N := 3n \Rightarrow a + b + c = 3n$ implica che almeno uno è $\geq n$ $\blacksquare$

(ii) Hp $\begin{cases} \cdot\ i_1 + j_1 = 1 \\ \cdot\ j_2 + k_2 = 1 \\ \cdot\ k_3 + i_3 = 1 \end{cases}$

$$(i_1 + j_1)(j_2 + k_2)(k_3 + i_3) = 1$$

$$(i_1 j_2 + i_1 k_2 + j_1 j_2 + j_1 k_2)(k_3 + i_3)$$

$$(i_1 j_2 k_3 + i_1 k_2 k_3 + \dots$$ VBB FUNZIA

~ o ~ o ~ o ~ o ~

EST / CONTR. DI IDEALI

$f : A \to B$ omom.

$J \triangleleft B$, la CONTRAZIONE di J è $f^{-1}(J)$

$I \triangleleft A$, la ESTENSIONE di I è $(f(I))$

- I primo/max in $A \overset{?}{\Longrightarrow} (f(I))$ è primo/max in B?

"È vero che l'estensione di ideali ha una qualche buona proprietà? NO"

CONTROES: $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$

Allora $f((p)) \subseteq \mathbb{Q}$ non è un ideale;

$(f((p))) = \mathbb{Q}$ non è un ideale né primo né max perché non è proprio

- Se J è primo/max di B, allora $f^{-1}(J)$ è primo/max di A?

PRIMO

Se $a \cdot b \in f^{-1}(J)$ vorrei $a \in f^{-1}(J)$ ∨ $b \in f^{-1}(J)$

$$f(ab) = f(a) f(b) \in J \overset{J \text{ primo}}{\Longrightarrow} f(a) \in J \ \vee\ f(b) \in J \quad ✓$$

$\boxed{\text{CONCLUSIONE}}$: la contrazione di un primo è primo

MAX Sia $f: \mathbb{Z} \hookrightarrow \mathbb{Q}$. Allora $J = (0)$ è max in $\mathbb{Q}$

ma $f^{-1}((0)) = (0) \cap \mathbb{Z} = (0)$ che non è MAX in $\mathbb{Z}$.

OSS Ogni max è primo $\Rightarrow$ la contrazione di un max è primo.

MAX IN $\mathbb{Z}[x]$

$M \subseteq \mathbb{Z}[x]$. Sia $f: \mathbb{Z} \hookrightarrow \mathbb{Z}[x]$. Da quanto sopra

$$f^{-1}(M) = M \cap \mathbb{Z} \text{ è un ideale primo di } \mathbb{Z}$$

DUE CASI:

$$\boxed{M \cap \mathbb{Z} = (p)} \qquad \underbrace{(p)\,\mathbb{Z}[x]}_{\text{polinomi a coeff. in } p\mathbb{Z}} \subseteq M \subseteq \mathbb{Z}[x]$$

Per il teorema di corrisp., gli ideali che contengono $(p)\mathbb{Z}[x]$ sono in biiezione con gli ideali di

$$\frac{\mathbb{Z}[x]}{(p)\mathbb{Z}[x]} \simeq (\mathbb{Z}/p\mathbb{Z})[x] \simeq \mathbb{F}_p[x]$$

e gli ideali di $\mathbb{F}_p[x]$ sono tutti della forma $(\bar{f}(x))$

Siccome M è max, corrisponde ad un ideale primo $(\bar{f}(x)) \trianglelefteq \mathbb{F}_p[x]$, cioè tale che $\bar{f}(x) \in \mathbb{F}_p[x]$ sia irriducibile.

Segue quindi che $M = (p, f(x))$ con $\bar{f} \in \mathbb{F}_p[x]$.

$(p)\mathbb{Z}[x] \subseteq M$ ↵

OSS: $$\frac{\mathbb{Z}[x]}{(p, f(x))} \simeq \frac{\mathbb{Z}[x]/p}{(p, f(x))/(p)} \simeq \frac{\mathbb{F}_p[x]}{(\bar{f}(x))}$$

ma $\bar{f}$ è irriducibile $\Rightarrow \simeq \mathbb{F}_{p^n}$ dove $n := \deg \bar{f}(x)$.

OSS: $(3, \underbrace{3x^5}_{\text{svanisce mod } 3} + x^2 + 1) = M$ ma $\frac{\mathbb{Z}[x]}{M} \simeq \mathbb{F}_{3^2}$

CASO 2: $M \cap \mathbb{Z} = (0)$

Vogliamo dim che ciò è assurdo.

OSS: $S = \mathbb{Z} \setminus (0)$ pensato come pr. mlt di $\mathbb{Z}[x]$.

① Ma $S^{-1}\mathbb{Z}[x] = \left\{ \frac{r(x)}{n} : r \in \mathbb{Z}[x], n \in \mathbb{Z} \setminus \{0\} \right\}$

$= \mathbb{Q}[x]$

② $S \cap M = \emptyset$

TEOREMA DI CORRISP.: gli ideali primi di $\mathbb{Z}[x]$ che non intersecano S sono in big. con gli id. primi di $S^{-1}\mathbb{Z}[x] = \mathbb{Q}[x]$

Ma gli ideali primi di $\mathbb{Q}[x]$ sono tutti e soli $(f(x))$ con $f \in \mathbb{Q}[x]$ irriducibile

$\longrightarrow S^{-1}M = (f(x))$ per qualche $f \in \mathbb{Q}[x]$ irriducibile

A meno di moltiplicare per il mcm dei denominatori, posso supporre che f sia a coeff. interi e primitivo

CLAIM: $M = (f(x))$ in $\mathbb{Z}[x]$

$\boxed{\supseteq}$ $f(x) \in S^{-1}M$, cioè $f(x) = \frac{a(x)}{n}$ con $n \in \mathbb{Z} \setminus \{0\}$, $a \in M$.

$\Rightarrow M \ni a = n \cdot f$ ma M è primo

e $n \notin M$ [$n \in \mathbb{Z}$ ma $\mathbb{Z} \cap M = (0)$]

dunque $f \in M$ e quindi $(f) \subseteq M$.

$\boxed{\subseteq}$ Viceversa, se $b \in M \Rightarrow b \in S^{-1}M = (f)$

Dunque $b = f \cdot g$ con $g \in \mathbb{Q}[x]$

Ma per il Lemma di Gauss, siccome $b \in \mathbb{Z}[x]$, $f \in \mathbb{Z}[x]$ e PRIMITIVO, allora $f \mid b$ in $\mathbb{Z}[x]$

e quindi $b \in (f)$ in $\mathbb{Z}[x]$

$\rightsquigarrow M = (f)$ in $\mathbb{Z}[x]$

OSS: finora abbiamo usato solo il fatto che M è primo, non che è massimale. Abbiamo cioè dim. che:

[Se $P \triangleleft \mathbb{Z}[x]$ primo, allora $\exists f \in \mathbb{Z}[x]$ irr e primitivo tale che $P = (f)$.]

Vogliamo ora mostrare che un tale M non può essere max.

Mostriamo che in effetti $\frac{\mathbb{Z}[x]}{M}$ non è un campo, ovvero che esiste un el. di $\rightsquigarrow$ non invertibile.

[ES: se $f = x-1$, allora in $\frac{\mathbb{Z}[x]}{(x-1)}$ gli interi diversi da ± 1 non sono inv.]

Vediamo allora se $p \in \mathbb{Z}$ primo è inv. in $\mathbb{Z}[x]/M$

$\iff \exists \bar{q}(x)$ t.c. $\bar{p} \cdot \bar{q}(x) = \bar{1}$ in $\mathbb{Z}[x]/(f)$

$\iff p \cdot q(x) = 1 + f(x) g(x)$ in $\mathbb{Z}[x]$

riduco mod p

$\implies 0 \equiv \bar{1} + \overline{f(x)}\,\overline{g(x)}$ in $\frac{\mathbb{Z}[x]}{(p)\mathbb{Z}[x]} \simeq \mathbb{F}_p[x]$

$\iff \bar{f}(x)\left(-\bar{g}(x)\right) = \bar{1}$ [$\rightarrow \bar{f}$ è inv. modulo p]

$\iff \deg \bar{f} = 0$

Ma a questo punto se $f(x) = a_n x^n + \dots + a_0$

e scegliamo p t.c. $p \nmid a_n$: troviamo un ASSURDO

perché $\deg \overline{f} = \deg f \neq 0$

$\Rightarrow (f)$ non è massimale $\blacksquare$

CONCLUSIONE: i max di $\mathbb{Z}[x]$ sono tutti e soli

$$(p, f(x)) \triangleleft \mathbb{Z}[x]$$

con $p \in \mathbb{Z}$ primo e $f \in \mathbb{Z}[x]$ tale che $\overline{f(x)} \in \mathbb{F}_p[x]$ è non zero e irriducibile.

~ o ~ o ~

INTERI DI GAUSS

Sappiamo che i seguenti el sono primi in $\mathbb{Z}[i]$

- $p \equiv 3 \ (4)$
- $1+i \sim 1-i$ $\qquad 2 = (1+i)(1-i) = -i(1+i)^2$
- $a+bi, a-bi$ $\qquad$ con $a^2+b^2 = p \equiv 1 \ (4)$

Vogliamo far vedere che non ce ne sono altri:

sia $c+di \in \mathbb{Z}[i]$ un primo.

Scriviamo $(c+di)(c-di) = c^2+d^2 = \prod p_i^{e_i}$

$\boxed{1}$ Supponiamo che uno dei p_i sia $\equiv 3 \ (4)$ e chiamiamolo p.

Allora p è primo anche in $\mathbb{Z}[i] \Rightarrow p \mid (c+di)(c-di)$

$\overset{p \text{ primo}}{\Rightarrow} p \mid c+di \quad \vee \quad p \mid c-di$

$\hookrightarrow c-di = p(e+fi)$

$\Rightarrow c+di = p(e-fi) \Rightarrow$ primo caso

Ma allora $p \mid c+di$ e $c+di$ è irriducibile, dunque

$p \sim c+di \Rightarrow c+di = u \cdot p$ con $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

$\boxed{2}$ Se uno dei $p_i \equiv 1 \ (4)$ $(p := p_i)$ sappiamo che

$p = (a+bi)(a-bi)$ con $a \pm bi$ primi in $\mathbb{Z}[i]$

$$a+bi \mid p \mid \prod p_i^{e_i} = (c+di)(c-di)$$

$$\Rightarrow \underset{2a}{a+bi \mid c+di} \quad \vee \quad \underline{a+bi \mid c-di}$$

$$c-di = (a+bi)(e+fi)$$

$$\underset{2b}{a-bi \mid c+di} \iff c+di = (a-bi)(e-fi)$$

2a Se $a+bi \mid c+di$ essendo $(c+di)$ irr. $\Rightarrow c+di \sim a+bi$

2b Se $a-bi \mid c+di$ // // // $\Rightarrow c+di \sim a-bi$

$\boxed{3}$ Se in $\prod p_i^{e_i}$ non compaiono né primi $\equiv 1 \ (4)$

// // $\equiv 3 \ (4)$

allora o il prodotto è 1 (assurdo)

oppure l'unico primo che compare è 2

$$1+i \mid 2 \mid c^2+d^2 = (c+di)(c-di)$$

$\Rightarrow c+di$ è associato a $1+i$ oppure a $1-i$

ma $1+i \sim 1-i$.

$$\frac{\mathbb{Z}[i]}{(a+bi)} \quad \text{con } (a+bi)(a-bi) = p \equiv 1 \ (4)$$

Siccome $(a+bi) \triangleleft \mathbb{Z}[i]$ è primo allora il quoziente è un dominio. Inoltre $p \in (a+bi)$ quindi

$$\frac{\mathbb{Z}[i]}{(a+bi)} \simeq \frac{\mathbb{Z}[i]/(p)}{(a+bi)/(p)} \quad \mathbb{Z}[i]/(p) \to \{\bar{c}+\bar{d}i \ : \ 0 \leq c, d \leq p-1\}$$

Il numeratore è finito, quindi quozientando ancora rimane finito

$\Rightarrow$ è un CAMPO di caratteristica p.

Inoltre $\left| \mathbb{Z}[i]/(a+bi) \right|$ divide p^2, ma se fosse $=$

allora $\left| \frac{\mathbb{Z}[i]/(p)}{(a+bi)/(p)} \right| = p^2$, ma già il num. ha p^2

elementi $\Rightarrow (a+bi)/(p)$ è banale

$\Rightarrow (a+bi) = (p)$

Ma ciò è assurdo perché $p = (a+bi)\underline{(a-bi)}$

NON INVERTIBILE

$$\Rightarrow \frac{\mathbb{Z}[i]}{(a+bi)} \simeq \mathbb{F}_p$$

ES: $\frac{\mathbb{Z}[i]}{(2-i)} \simeq \mathbb{F}_5$. Quoziento per la relazione "$2 = i$" e in più quoziento mod 5 perché $5 \in (2-i)$.

Somma di 2 Quadrati

$$x^2+y^2=n \quad \text{dove} \quad n = \underset{1}{\underset{\equiv}{5}} \cdot \underset{3}{\underset{\equiv}{7}} \cdot \underset{3}{\underset{\equiv}{11}} \cdot \underset{1}{\underset{\equiv}{13}} \cdot \underset{1}{\underset{\equiv}{17}}$$

$\Updownarrow$

$$(x+yi)(x-yi) = 7 \cdot 11 \cdot (2+i)(2-i) \cdot (3+2i)(3-2i) \cdot (4+i)(4-i).$$

Nel caso di 7 e 11: $\quad 7 \mid x+yi \quad \vee \quad 7 \mid x-yi$

$$\Downarrow$$

$$7 \mid x+yi$$

$$\Rightarrow \quad x+iy = 7(c+di) \quad \Rightarrow \quad x = 7c,\ y = 7d$$

$$\Rightarrow \quad x^2+y^2 \equiv 0 \quad (49)$$

$\rightsquigarrow$ NESSUNA SOLUZIONE : $n \not\equiv 0 \quad (49)$

Ripartiamo

$$x^2+y^2=n \quad \text{dove} \quad n = \underset{1}{\underset{\equiv}{5}} \cdot \underset{3}{\underset{\equiv}{7}}^2 \cdot \underset{3}{\underset{\equiv}{11}}^2 \cdot \underset{1}{\underset{\equiv}{13}} \cdot \underset{1}{\underset{\equiv}{17}}$$

$\Updownarrow$

$$(x+yi)(x-yi) = 7^2 \cdot 11^2 \cdot (2+i)(2-i) \cdot (3+2i)(3-2i) \cdot (4+i)(4-i).$$

$\rightsquigarrow \quad x, y \mid 7, 11$

$\Rightarrow$ Studiamo quindi equiv.

$$(x+yi)(x-yi) = (2+i)(2-i) \cdot (3+2i)(3-2i) \cdot (4+i)(4-i).$$

OSS: $\quad 2+i \mid x+iy \quad \Leftrightarrow \quad 2-i \mid x-iy$

$$\Rightarrow \quad x+iy = u \cdot (2\pm i)(3\pm 2i)(4\pm i) \quad \text{con } u \in \mathbb{Z}[i]^\times$$