$A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ non è Euclideo

Sia $\omega := \frac{1+\sqrt{-19}}{2}$; $\mathbb{Z}[\omega]$ = il più piccolo sottoanello di $\mathbb{C}$ contenente $\mathbb{Z}$, ω

$$\omega^2 = \frac{1-19+2\sqrt{-19}}{4} = -9 + \frac{\sqrt{-19}}{2} = \omega - 5$$

$$\Rightarrow \quad A = \{ a\omega + b : a, b \in \mathbb{Z} \}$$

ogni prodotto può essere scritto in questa forma perché $\omega^2 = \omega - 5$

OSS: questo è vero perché ω soddisfa un'eq. polinomiale di secondo grado MONICA

CONTROES: $\mathbb{Z}\left[\frac{1}{\sqrt{2}}\right] \neq \left\{ a \cdot \frac{1}{\sqrt{2}} + b : a, b \in \mathbb{Z} \right\}$

Ad es $\left(\frac{1}{\sqrt{2}}\right)^{100} \notin$ $\longrightarrow$ $2x^2 - 1$

OSS: ① $x^2 - x + 5$ è irr. in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$ per il L.d.G.

$$\Rightarrow \mu_\omega = x^2 - x + 5$$

② $\mathbb{Z}[x] \xrightarrow{\Phi} A$, $p \longmapsto p(\omega)$ è omo

e $\operatorname{Ker} \Phi = (x^2 - x + 5)$.

In effetti se $p(\omega) = 0$, allora $\mu_\omega \mid p$ in $\mathbb{Q}[x]$.
Ma $\mu_\omega, p \in \mathbb{Z}[x]$ e μ_ω è primitivo [è MONICO]

$$\Rightarrow \mu_\omega \mid p \text{ in } \mathbb{Z}[x]$$

$$\Rightarrow \operatorname{Ker} \Phi \subseteq (x^2 - x + 5)\mathbb{Z}[x]$$

L'altra inclusione è ovvia $[x^2 - x + 5$ si annulla in $\omega]$

③ $\Phi(ax+b) = a\omega + b \Rightarrow \Phi$ è surgettiva

$\Rightarrow$ ④ $A \simeq \dfrac{\mathbb{Z}[x]}{(x^2-x+5)}$

Supponiamo A euclideo e sia $d : A \setminus \{0\} \to \mathbb{N}$ t.c.

① $\forall a, b \in A \setminus \{0\} \quad \exists q, r$ t.c. $a = qb + r$ con $r = 0 \vee d(r) < d(b)$

② $\forall a, b \in A \setminus \{0\} \quad d(ab) \geq d(a)$

$\{$El. di grado minimo$\} = A^\times$

$$A^\times = \{a + b\omega \in A \setminus \{0\} : (a+b\omega)^{-1} \in A\}$$

$$(a+b\omega)^{-1} = \frac{\overline{a+b\omega}}{\|a+b\omega\|^2} = \frac{a + \frac{b}{2} - \frac{1}{2}b\sqrt{-19}}{\|a + \frac{b}{2} + \frac{b}{2}\sqrt{19}\,i\|^2}$$

$$= \frac{a + b/2 - \frac{1}{2}b\sqrt{19}\,i}{(a+b/2)^2 + \frac{19}{4}b^2} = \underbrace{c}_{\in\mathbb{Q}} + \underbrace{d}_{\in\mathbb{Q}}\,i$$

Considero tutto dentro $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-19})$

Quando $c, d \in \mathbb{Z}$?

Parti imm: $\dfrac{-\cancel{\frac{1}{2}}b\cancel{\sqrt{19}}}{(a+\frac{b}{2})^2 + \frac{19}{4}b^2} = \cancel{\frac{1}{2}}d\cancel{\sqrt{19}}$

$\llcorner$ è <1 in modulo

Siccome $d \in \mathbb{Z} \Rightarrow b = 0 \Rightarrow a + b\omega = a$

che è invertibile se $a = \pm 1$

CONCLUSIONE: $A^\times = \{\pm 1\}$

Sia ora $x \in A \setminus \{0; 1; -1\}$ di grado minimo.

Div con resto: $\forall a \in A \quad \exists q, r \in A$ t.c.

$$\circledast \qquad a = qx + r \quad \text{con} \quad r = 0 \ \vee \ d(r) < d(x)$$

per come ho scelto x

$\Rightarrow r \in \{0, 1, -1\}$

$\{0; 1; -1\} \twoheadrightarrow A/(x)$: infatti la $\circledast$ dice che ogni resto mod x è rappresentato da uno fra $0, 1, -1$.

OSS: $(x) \neq A$ perché $x \notin A^\times \Rightarrow |A/(x)| \geq 2$

Ma la suriezione $\{0; 1; -1\} \twoheadrightarrow A/(x)$ mi dice che $|A/(x)| \leq 3$

$\Rightarrow |A/(x)| \in \{2; 3\} \Rightarrow A/(x) \in \{\mathbb{F}_2; \mathbb{F}_3\}$

Mostriamo ora che né $\mathbb{F}_2$ né $\mathbb{F}_3$ possono essere quozienti di A.

In effetti $t^2 - t + 5$ ha una radice (ω) in A.

$$\pi : A \twoheadrightarrow A/(x)$$

allora $\pi(\omega)$ è una radice di

$$t^2 + \pi(-1)\,t + \pi(5) \in A/(x)\,[t]$$

$\rightarrow t^2 - t + 5$ ha una radice in $\mathbb{F}_2$ oppure in $\mathbb{F}_3$ (cioè $\pi(\omega)$)

Ma ciò non è vero $\Rightarrow$ ASSURDO

NON È EUCLIDEO

OSS: per dire se un anello è euclideo si fa così:

- grado 0 alle unità
- grado 1 agli elementi che quando usati come divisori danno resti di grado 0
- grado 2 agli el. che quando usati come divisori danno resti di grado 1
- ecc ...

Se mi blocco non funziona $\Rightarrow$ non è un ED

Se l'anello non è euclideo

- $A_0 = A^\times$
- $A_1 = \{ x \in A : \exists r \in \{0\} \cup A_0 \ \exists q \in A \text{ t.c. } a = qx + r \}$
- $\vdots$

~ o ~ o ~

PID

Sia A un PID, $(0) \neq P \triangleleft A$ primo. Mostrare che P è max.

DIM Per def. di PID si ha che $P = (x)$, con $x \neq 0$.

Vogliamo dimostrare che se

$$P \subseteq M \subseteq A$$

allora $P = M$. Siccome A è PID, $M = (y)$. Segue che $x \in (y)$, ovvero $\exists a \in A$ t.c. $x = ay$.

Ma x è primo ($\Rightarrow x$ è irriducibile), dunque uno tra a, y è un'unità.

Se $a \in A^\times$ allora $x \sim y$, cioè $(x) = (y)$.

Se $y \in A^\times$ allora $(y) = A$, da cui la tesi. $\blacksquare$

Due applicazioni

Sia $\varphi : A \twoheadrightarrow B$ omom. surg. con B dominio e A PID.
Allora φ è un isomorfismo oppure B è un campo.

DIM Sia $\operatorname{Ker}\varphi \trianglelefteq A$. Per il 1° Teo. di Iso

$$A/_{\operatorname{Ker}\varphi} \simeq B$$

è un dominio $\Rightarrow$ $\operatorname{Ker}\varphi$ è primo.

Ma A è PID $\Rightarrow$ per il ris. precedente abbiamo 2 casi:

- $\operatorname{Ker}\varphi = 0 \Rightarrow \varphi$ è iso
- $\operatorname{Ker}\varphi$ è max $\Rightarrow B$ è un campo

Seconda appl.

A comm con id. Supponiamo $A[x]$ PID. Allora A è un campo.

DIM "A MANO" $A \hookrightarrow A[x]$ e $A[x]$ è dominio segue che A è dominio.

Sia $a \in A \setminus \{0\}$. Considero $(a, x) \trianglelefteq A[x]$. Per hp.

$$(a, x) = (p(x))$$

Allora $\exists\, q, r \in A[x]$ t.c.

$$a = p(x)\, q(x) \qquad\qquad x = p(x)\, r(x)$$

$$\Big\downarrow \text{deg} \qquad\qquad\qquad \Big\downarrow \text{deg}$$

$$0 = \deg p + \deg q \qquad\qquad 1 = \deg p + \deg r$$

Dunque p è una costante: $p(x) = b \in A$.

Inoltre $r(x)$ è di grado 1 $\Rightarrow$ $r(x) = cx + d$

Quindi $x = b \cdot (cx + d) = bcx + bd$

termini di grado 1 $\rightsquigarrow$ $bc = 1 \Rightarrow \underline{b \in A^\times}$.

Ora imponiamo il fatto che $(p(x)) \subseteq (a, x)$.

$\Rightarrow \exists\, s, t \in A[x]$ t.c.

$$b = p(x) = a\, s(x) + x \cdot t(x)$$

valutando in $x = 0$

$$b = a \cdot s(0) + 0$$

$b \in A^\times$ $\Rightarrow$ $1 = a \cdot s(0) b^{-1}$

Dunque $a \in A^\times \Rightarrow A$ è un campo. $\boxtimes$

D IM "INTELLIGENTE"

$(x) \trianglelefteq A[x]$ è primo poiché $\frac{A[x]}{(x)} \simeq A$ è dominio

(per quanto detto all'inizio dell'altra dim)

Ma $A[x]$ è PID e $(x) \neq (0)$, quindi (x) è max.

$$\Rightarrow A \simeq \frac{A[x]}{(x)} \text{ è un campo.}$$ $\boxtimes$

A/I^n

A PID. $I \neq (0)$ ideale di A t.c. $|A/I| < \infty$. Allora

$$|A/I^n| = |A/I|^n$$

OSS A/I^2 : $A/I \simeq \frac{A/I^2}{I/I^2}$ $\Rightarrow$ mi basta dim che $|I/I^2| = |A/I|$

Infatti se A/I è finito e I/I^2 è finito allora anche A/I^2 deve essere finito (se quoziento un gruppo infinito per un gruppo finito mi esce un gruppo di card. infinita); inoltre $|A/I^2| = |A/I| \cdot |I/I^2|$

Sia $I = (\alpha)$. Considero

$$\psi : \underbrace{A \xrightarrow{\varphi} A}_{} \xrightarrow{\pi} A/I^2$$
$$x \longmapsto \alpha x \longmapsto \overline{\alpha x}$$

non è omom. di anelli, ma è omom. di gruppi abeliani

$\varphi(x+y) = \alpha(x+y) = \alpha x + \alpha y = \varphi(x) + \varphi(y)$

- $\operatorname{Im} \psi = \pi(\operatorname{Im}(\varphi)) = \pi((\alpha)) = \pi(I) = I/I^2$
- $\operatorname{Ker} \psi = \{x \in A : \pi(\alpha x) = 0\}$
$= \{x \in A : \alpha x \in I^2\}$
$= \{x \in A : \alpha x \in (\alpha^2)\}$
$= \{x \in A : (\exists \beta : \alpha x = \alpha^2 \beta)\}$
$= \{x \in A : (\exists \beta : x = \alpha\beta)\}$
$= \{x \in A : x \in (\alpha) = I\} = I$

1° Teo Omo (di gruppi)

$$I/I^2 \simeq A/I$$
$$\operatorname{Im} \simeq A/\operatorname{Ker}$$

$\Rightarrow |A/I| = |I/I^2| \Rightarrow$ tesi. (per $n = 2$)

GENERALIZZAZIONE

$$\begin{array}{ccccc} A & \longrightarrow & A & \twoheadrightarrow & A/_{I^{k+1}} \\ x & \longmapsto & \alpha^k x & \longmapsto & \overline{\alpha^k x} \end{array}$$

Con lo stesso ragionamento si mostra che

$$\text{Imm} = I^k/_{I^{k+1}} \quad , \quad \text{Ker} = I$$

Segue che $I^k/_{I^{k+1}} \simeq A/_I$

Per induzione allora

$$A/_{I^k} \simeq \frac{A/_{I^{k+1}}}{I^k/_{I^{k+1}}} \Rightarrow \left|A/_{I^{k+1}}\right| = \left|A/_{I^k}\right| \cdot \left|I^k/_{I^{k+1}}\right|$$

$$= \left|A/_{I^k}\right| \cdot \left|A/_I\right|$$

$$= \left|A/_I\right|^k \cdot \left|A/_I\right|.$$

Applicazione: $\mathbb{Z}[i]/_{(a+bi)}$

Dim che $\mathbb{Z}[i]/_{(a+bi)} = a^2 + b^2$ se $(a,b) \neq (0,0)$

DIM $a + bi = \prod p_i^{e_i}$ con $p_i \in \mathbb{Z}[i]$

. $(p_i^{e_i}) + (p_j^{e_j}) = (\text{mcd}(p_i^{e_i}, p_j^{e_j})) = (1)$

$i \neq j$

. TCR: gli id sono coprimi!

$$\frac{\mathbb{Z}[i]}{(a+bi)} \simeq \prod \frac{\mathbb{Z}[i]}{(p_i^{e_i})}$$

- $\left|\frac{\mathbb{Z}[i]}{(a+bi)}\right| = \prod_i \left|\frac{\mathbb{Z}[i]}{(p_i^{e_i})}\right| \overset{\text{fatto prec}}{=} \prod \left|\frac{\mathbb{Z}[i]}{(p_i)}\right|^{e_i}$

- $p_i \in \{ 1+i;\ p \in \mathbb{Z} \equiv 3 \mod 4;$
  $x+iy$ con $x^2+y^2 = p \equiv 1\ (4) \}$

(*) $\frac{\mathbb{Z}[i]}{(p)} \simeq \mathbb{F}_{p^2}$ se $p \equiv 3\ (4)$ $\rightsquigarrow$ card $p^2 = p^2+0^2$

(*) $\frac{\mathbb{Z}[i]}{(x+iy)} \simeq \mathbb{F}_p$ con $p = x^2+y$ $\rightsquigarrow$ card $p = x^2+y^2$

(*) $\frac{\mathbb{Z}[i]}{1+i} \simeq \mathbb{F}_2$ $\rightsquigarrow$ card $2 = 1^2+1^2$

$\Rightarrow \frac{\mathbb{Z}[i]}{(x+yi)} = \prod \left|\frac{\mathbb{Z}[i]}{(p_i)}\right|^{e_i} = \prod \|p_i\|^{2e_i}$

$= \left\| \prod p_i^{e_i} \right\|^2 = \|a+bi\|^2 = a^2+b^2.$ ■

CAMPI $K = \widetilde{\mathbb{C}(t)} = \widetilde{\text{Frac}}(\widetilde{\mathbb{C}[t]})$

$= \left\{ \frac{p}{q} : p, q \in \mathbb{C}[t],\ q \neq 0 \right\}$

Sia $u = t^3 + \frac{1}{t^3} \in K.$

$$\begin{array}{c} \mathbb{C}(t) \\ \Big| \ \infty, \text{trasc.} \\ \mathbb{C} \end{array}$$

OSS: $K/\mathbb{C}$ è trascendente:

(*) $\mathbb{C}$ è alg. chiuso

$\Rightarrow$ non esiste un' est. alg. non banale

(*) se t fosse algebrico dovrebbe esistere $p \in \mathbb{C}[x]$ t.c. $p(t) = 0.$

Scrivendo $p = a_n x^n + \dots + a_0$ si ha che

$$p(t) = a_n t^n + \dots + a_0 \in K$$

e $p(t)$ non è lo 0 di K.

Vogliamo ora dim che

$$\mathbb{C} - \mathbb{C}(u) - \mathbb{C}(t)$$

$$\begin{tikzcd}
K \arrow[d, dash, "\infty"'] \arrow[dr, dash, "\text{finita?}"] & \\
\mathbb{C} \arrow[r, dash, "\text{finita?}"'] & \mathbb{C}(u)
\end{tikzcd}$$

Polinomio minimo di t su $\mathbb{C}(u)$?

$$u = t^3 + \frac{1}{t^3} \Rightarrow t^6 + 1 - u t^3 = 0$$

$\Rightarrow$ Il polinomio $p(x) = x^6 - u \cdot x^3 + 1 \in \mathbb{C}(u)[x]$ si annulla in t!

$$\Rightarrow \quad \begin{tikzcd}
K \arrow[dd, dash, "\infty"'] \arrow[dr, dash, "\text{finita}"] & \\
& \mathbb{C}(u) \\
\mathbb{C} \arrow[ur, dash, "\infty"'] &
\end{tikzcd}$$

Oss $\mathbb{C}(t) \simeq \mathbb{C}(u)$ come campi!

Infatti u è trascendente poiché $[\mathbb{C}(u) : \mathbb{C}] = \infty$

Dunque le due ext. sono generate da un singolo el. trasc.

e quindi $\mathbb{C}(t) \longrightarrow \mathbb{C}(u)$ è un isomorfismo.

$$\frac{f(t)}{g(t)} \longmapsto \frac{f(u)}{g(u)}$$

Tuttavia $\mathbb{C}(t) \neq \mathbb{C}(u)$! L'isom. non è l'inclusione!

È come se fossero sp. vett. di dimensione infinita: possono essere isomorfi ma diversi

p è pol. minimo $\iff$ è irr in $\mathbb{C}(u)[x]$

$\mathbb{C}[u][x] \quad \mathrm{Frac}(\mathbb{C}[u])[x]$

Dal L. di Gauss, p è irr in $\mathbb{C}(u)[x]$ se e solo se è primitivo ed è irriducibile in

$$\mathbb{C}[u][x] \simeq \mathbb{C}[u,x] \simeq \mathbb{C}[x][u]$$

Quindi inv. di dimostrare che $x^6 - ux^3 + 1 \in \mathbb{C}[u][x]$ è irriducibile, dimostro che è irr in $\mathbb{C}[x][u]$

$$\text{Ma } p = u(-x^3) + (x^6+1) \quad \rightsquigarrow \deg 1 \text{ in } u$$

e se fosse rid. allora

$$p(u,x) = a(u,x)\, b(u,x)$$

$$\Downarrow \deg$$

$$1 = \deg_u p = \deg_u a + \deg_u b$$

$\Rightarrow$ almeno uno tra a e b ha grado 1 in u

Supponiamo WLOG $\deg_u a = 0$, $\deg_u b = 1$

$$u \cdot (-x^3) + (x^6+1) = a(x) \cdot (\underbrace{u \cdot c(x) + d(x)}_{b})$$

$$\Rightarrow -x^3 = a \cdot c, \quad x^6 + 1 = a \cdot d$$

$$\Rightarrow a \mid -x^3 \quad \wedge \quad a \mid x^6 + 1 \quad \text{in } \mathbb{C}[x]$$

$$\Rightarrow a \mid (-x^3, x^6+1) = 1 \quad \text{in } \mathbb{C}[x]$$

e dunque a è invertibile in $\mathbb{C}[x]$.

Segue dunque che la fatt. $p = a \cdot b$ è banale (a è invertibile) e quindi p è irriducibile.

$\Rightarrow$ p è il polinomio minimo di t su $\mathbb{C}(u)$

In particolare $[\mathbb{C}(t) : \mathbb{C}(u)] = \deg_x p = 6.$

OSS GENERALE:

$$\begin{array}{c} \mathbb{C}(t) \\ | \\ \mathbb{C}\left(\frac{p(t)}{q(t)}\right) \end{array}$$

è finita e se $(p, q) = 1$ il grado è $\max\{\deg p, \deg q\}$.

Immersioni $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \hookrightarrow \mathbb{C}$

Fissata $\mathbb{Q} \xhookrightarrow{\varphi} \mathbb{C}$, data $\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$

esistono $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] =: n$ estensioni di φ a

delle immersioni $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \xhookrightarrow{\varphi_i} \mathbb{C}$

OSS: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[rr, phantom, "\neq"] \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\Rightarrow 2^2$

OSS 2: è la stessa cosa dire che $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \hookrightarrow \overline{\mathbb{Q}}$

o $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \hookrightarrow \mathbb{C}$ ($\overline{\mathbb{Q}} \subseteq \mathbb{C}$)

OSS 3:

$$\varphi_i(\sqrt{2})^2 = \varphi_i(2) = 2 \qquad \varphi_i(\sqrt{2}) = \pm\sqrt{2}$$
$$\varphi_i(\sqrt{3})^2 = \varphi_i(3) = 3 \quad \Rightarrow \quad \varphi_i(\sqrt{3}) = \pm\sqrt{3}$$
$$\varphi_i(\sqrt{2}\sqrt{3})^2 = \varphi_i(6) = 6 \qquad \varphi_i(\sqrt{6}) = \pm\sqrt{6}$$

$$\Rightarrow \varphi_i(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})$$
$$= a \pm b\sqrt{2} \pm c\sqrt{3} \pm d\sqrt{6}$$

8 scelte ... ?

NO: $\sqrt{6} = \sqrt{2}\sqrt{3} \longmapsto \varphi_i(\sqrt{2})\varphi_i(\sqrt{3})$

NON È INDIP!

$$(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$$

sono una $\mathbb{Q}$ - base dello sp. vett. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \overset{\varphi_1 = id}{\longmapsto} a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \overset{\varphi_2}{\longmapsto} a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \overset{\varphi_3}{\longmapsto} a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \overset{\varphi_4}{\longmapsto} a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$