Polinomi in $\mathbb{K}[x]$

Prop. Sia I un ideale in $\mathbb{K}[x]$, allora $\exists\, f(x) \in I \mid I = (f(x))$, ossia è monogenerato.

Considero l'insieme $D = \{ \deg g(x) \mid \underset{\neq 0}{g(x)} \in I \} \subseteq \mathbb{N}$.
Se $D = \emptyset$, $I = (0)$. Altrimenti D ammette un minimo m. Sia allora $f(x) \in I$ t.c. $\deg f(x) = m$.

Dimostriamo che $(f(x)) \supset I$. Prendiamo $h(x) \in I$:
$h(x) = q(x) f(x) + r(x)$. Poiché $\deg r(x) < m$ e $r(x) \in I$, si ha che $r(x) = 0$.
Quindi $h(x) \in (f(x))$. Allora $\underbrace{(f(x))}_{PID} = I$. $\boxtimes$

principal ideal domain
perché monogenerato

Oss. $\mathbb{K}[x]$ ammette quindi solo PID.

Quozienti in $\mathbb{K}[x]$

Def. Sia $f(x) \in \mathbb{K}[x]$ t.c. $\deg f(x) \geq 1$. $f(x)$ si dirà IRRIDUCIBILE se $f(x) = a(x)\, b(x) \Rightarrow a(x)$ o $b(x)$ è invertibile (ossia costante).

Prop. Sia $f(x) \in \mathbb{K}[x]$ polinomio irriducibile, allora $\mathbb{K}[x]/(f(x))$ è un CAMPO.

Siano $I = (f(x))$, $a(x) + I$ un elemento di $\mathbb{K}[x]/(f(x))$ diverso da $0 + I$.

Uso Bézout considerando che $MCD(a(x), f(x)) = 1$ (altrimenti sarebbe $f(x)$, però così $a(x) \in I$, $\lightning$):
$\exists\ \lambda(x), \mu(x) \mid \lambda(x)\, a(x) + \mu(x)\, f(x) = 1$.

Allora $(a(x) + I)(\lambda(x) + I) = a(x)\lambda(x) + I =$
$= 1 + I$, ossia l'identità moltiplicativa. $\boxtimes$

Oss. $f(x)$ è irriducibile $\Leftrightarrow$ $\mathbb{K}[x]/(f(x))$ è un campo.

$$\begin{cases} f(x) = a(x)\, \underset{\deg \geq 1}{b(x)} \Rightarrow (a(x)+I)(b(x)+I) = I \\ I = (f(x)) \end{cases}$$

oss. 2 $\mathbb{K}[x]/(0) = \mathbb{K}[x]$ $\quad \mathbb{K}[x]/(\underset{\neq 0}{c}) \cong \{0\}$

oss. 3 Vale l'aritmetica modulare su $\mathbb{K}[x]$

es. Esistono anelli con ideali non monogenerati, come $\mathbb{R}[x,y]$ con $I = (x,y) = \{ x \underset{\in \mathbb{R}[x,y]}{h(x,y)} + y \underset{\in \mathbb{R}[x,y]}{q(x,y)} \}$.

Un elemento $f(x,y)$ t.c. $I = (f(x,y))$ è tale che
$f(x,y) \mid x \wedge f(x,y) \mid y \implies f(x,y) = c$ $(\deg f(x,y) = 0)$.
Tuttavia $c \notin I$, $\lightning$.

es. 2 Anche $I = (2, x)$ in $\mathbb{Z}[x]$ non è monogenerato.
$I = \{ 2h(x) + x\,q(x) \} \implies f(x) \mid 2 \implies f(x) = 1$ o $f(x) = 2$. Tuttavia $2 \nmid x$, quindi $f(x) = 1$, ma $1 \notin I$, $\lightning$.

Anelli euclidei

Def. Un dominio D si dice ANELLO EUCLIDEO se esiste una funzione grado:

$$g : D \setminus \{0\} \longrightarrow \mathbb{N}$$

tale che:

- $\forall\, a, b \in D$, entrambi non zero, $g(a) \leq g(ab)$
- $\forall\, a, b \in D$ con $b \neq 0$, $\exists\, q, r \in D \mid a = bq + r$ dove $r = 0 \lor g(r) < g(q)$.

Lemma Siano $a, b \neq 0 \in D$, allora $b \mid a \land a \nmid b \Rightarrow$
$\Rightarrow g(b) < g(a)$.

- $a \nmid b \Rightarrow \exists\, r \neq 0 \mid b = \underset{\in D}{aq} + r = \overbrace{bkq}^{a = bk} + r \Rightarrow$

$$\Rightarrow r = b(\underset{\neq 0^*}{1 - kq}) \Rightarrow \begin{cases} g(r) \geq g(b) \\ g(r) < g(a) \end{cases} \Longrightarrow$$

$$\Longrightarrow g(a) > g(b).$$

* altrimenti $r = 0 \Rightarrow a \mid b$, $\lightning$. $\boxtimes$

Lemma $\forall\, a \in D,\ \underset{(i)}{g(1) = g(a)} \iff \underset{(ii)}{a \text{ è invertibile.}}$

(i) $\Rightarrow$ (ii) $\quad 1 = b\cdot a + r \quad g(r) < g(a) = 1$ imp. $\Rightarrow r = 0 \Rightarrow$

$b \cdot a = 1 \Rightarrow$ a è invertibile

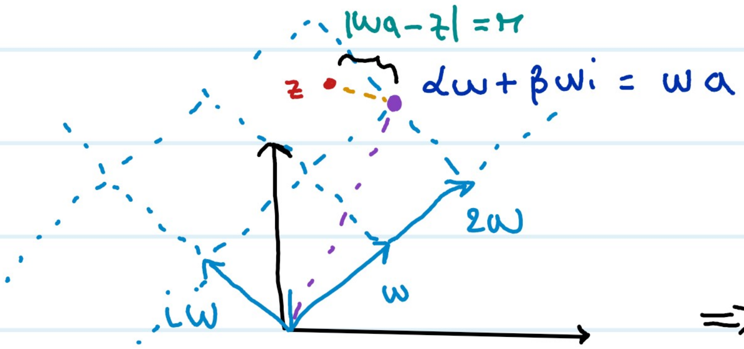
(ii) $\Rightarrow$ (i) $\quad 1 = a\cdot a^{-1} \Rightarrow g(a) \leq \underbrace{g(1)}_{\text{minimo}} \Rightarrow g(a) = g(1)$

$\boxtimes$

es. $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$ è un sottoanello di $\mathbb{C}$, e quindi un dominio.

Prop. $\mathbb{Z}[i]$ è euclideo.

Definisco $g: \mathbb{Z}[i]\setminus\{0\} \to \mathbb{N},\ a+bi \mapsto a^2+b^2 = |a+bi|^2$, che soddisfa le proprietà del grado.



$|wa - z| \leq \dfrac{|w|}{\sqrt{2}} \Rightarrow$

$\Rightarrow g(wa - z) \leq \dfrac{g(w)}{2}$

Dunque $z = wa + r$, con $g(r) \leq \dfrac{g(w)}{2} < g(w)$.

$\boxtimes$

OSS. ogni anello euclideo ammette un'unica fattorizzazione (eccetto per 0), ossia è un UFD (unique-factorization domain), e solo PID come ideali.