ANELLI

lunedì 20 novembre 2023 10:23

DEFINIZIONI PRINCIPALI

anello $(A,+,\cdot)$ → 1) $(A,+)$ gr. ab.
2) $\cdot$ associativo
3) $\cdot$ distributivo

Anello commutativo → $\cdot$ commutativo

Anello unitario → se $\exists\, 1 \in A$ t.c. $a.1 = 1a = a \quad \forall a$

elt invertibile → $x \in A$ si dice invertibile se $\exists\, y \in A$ t.c. $xy = yx = 1$
$A^* = \{x \in A \mid x$ è invertibile$\}$
$\mathbb{Z}^* = \{\pm 1\}$
$\mathbb{Z}/m\mathbb{Z}^* = \{\bar{a} \mid (a,m) = 1\}$

elt nilpotente → $x \in A$ nilp se $\exists\, n \in \mathbb{N}$ t.c. $x^n = 0$

elt. divisore di zero → $x \in A$ è divisore di 0 se $\exists\, y \neq 0$ $y \in A$ t.c. $xy = yx = 0$
$D(A) = \{x \in A \mid x$ è divisore di $0\}$
$D(\mathbb{Z}/m\mathbb{Z}) = \{\bar{a} \mid (a,m) \neq 1\}$

dominio di integrità → $(A,+,\cdot)$ comm con unità t.c. $D(A) = \{0\}$

campo → $(K,+,\cdot)$ anello comm con 1 t.c. $K^* = K \setminus \{0\}$

Proprietà anelli comm con unità → 1) $a.0 = 0.a$
2) A^* è gruppo comm.
3) $D(A) \cap A^* = \phi$
4) Se A è finito $\Rightarrow A = A^* \cup D(A)$

Slogan → 1) Ogni campo è dominio di integrità
2) Ogni dominio di integrità finito è un campo
controesempio se non è finito $\mathbb{Z}^* \neq \mathbb{Z} \setminus \{0\}$

Sottoanello → $B \subset A$ $B \neq \phi$ B sottoanello di A se è chiuso rispetto a $+, \cdot$ ristrette a B

ideale → $I \subset A$, A anello comm, I è ideale di A se: 1) $(I,+) \triangleleft (A,+)$
2) $aI \subset I$ e $Ia \subset I$ (prop. di assorbimento)
$\forall a \in A$ e $\forall x \in I$, $ax \in I$ $\quad \forall a \in A$ e $\forall x \in I$, $xa \in I$

$\mathbb{Z}$ i suoi ideali sono $\{n\mathbb{Z}\}_{n \in \mathbb{N}}$

Per verificare che un sottoinsieme di un anello comm con 1 è un ideale basta verificare che $(I,+)$ è chiuso per l'op + e vale la prop di assorbimento

ideale generato → $S \subset A$ $\quad (S) = \left\{ \sum_{i=1}^{n} a_i s_i \mid a_i \in A, s_i \in S, n \in \mathbb{N} \right\}$

ideale principale → se $(S) = \{x\}$ $\Rightarrow (x) = \{ax \mid a \in A\} = Ax$
(ideale generato da un elt)

OPERAZIONE TRA IDEALI

I, J ideali di A

- $I \cap J$ è ideale
- $I + J = (I, J) = \{ i + j \mid i \in I, j \in J \}$ è ideale
- $IJ = (\{ xy \mid x \in I, y \in J \})$ è ideale
- $\sqrt{I} = \{ x \in A \mid \exists n \in \mathbb{N} : x^n \in I \}$ è ideale   ($\sqrt{0} = \mathcal{N}$ è ideale
- $(I : J) = \{ x \in A \mid xJ \subseteq I \}$ è ideale
- $I \cup J$ non è ideale in generale
- $IJ \subseteq I \cap J$ vale $=$ $\Leftrightarrow$ $I + J = A$

$m\mathbb{Z} \cap n\mathbb{Z} = [m,n]\mathbb{Z}$
$m\mathbb{Z} \cdot n\mathbb{Z} = m \cdot n\mathbb{Z}$
$m\mathbb{Z} + n\mathbb{Z} = (m,n)\mathbb{Z}$
$\sqrt{n\mathbb{Z}} = p_1 \cdots p_r \mathbb{Z}$ dove $n = p_1^{e_1} \cdots p_r^{e_r}$

Fatto $\longrightarrow$ 1) $I \subsetneq A \Leftrightarrow I \cap A^* = \emptyset$
2) A è un campo $\Leftrightarrow$ gli unici ideali di A sono $\{0\}$ e A

ANELLI QUOZIENTI E OMO DI ANELLI

omo di anelli $\longrightarrow$ $f : A \to B$ è omo se: 1) $f(a_1 +_A a_2) = f(a_1) +_B f(a_2)$

2) $f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$ $\forall a_1, a_2 \in A$

3) $f(1_A) = 1_B$

anello quoziente $\longrightarrow$ $I \subseteq A$ ideale $(A/I, +, \cdot)$ è l'anello quoziente
$(a + I) + (b + I) = a + b + I$
$(a + I) \cdot (b + I) = ab + I$

proiezione sull'anello quoziente $\longrightarrow$ $\pi_I : A \longrightarrow A/I$ $\operatorname{Ker} \pi_I = I$
$a \longmapsto a + I$

Teo omo di Anelli $\longrightarrow$ 1)

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & B \\ A/I \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

$f = \varphi \circ \pi$
$\operatorname{Im} f = \operatorname{Im} \varphi$

2) $\dfrac{A/I}{J/I} \cong A/J$

3) $\dfrac{I + J}{J} \cong \dfrac{I}{I \cap J}$

Ideali ~ sgr. ◁ $\longrightarrow$ $f : A \to B$ omo
1) $\forall J \subseteq B$ $f^{-1}(J)$ è un'ideale di A
2) Se f è sur $\forall I \subseteq A$ ideale $\Rightarrow$ $f(I) \subseteq B$ ideale

Teo di corrispondenza $\longrightarrow$ $I \subseteq A$ ideale $\pi_I : A \longrightarrow A/I$

$\{H$ ideale di $A/I\} \longleftrightarrow \{H$ ideale di A t.c. $H \supseteq I\}$

preserva: ordinamento per inclusione
indice di sgr
ideali primi
ideali max

T.C.R per anelli → hp1 A comm con unità, hp2 I, J ideali di A $\Bigg\} \Rightarrow f: A \longrightarrow A/_I \times A/_J$, $a \longmapsto (a+I, a+J)$

1) f è omo di anelli
2) $\operatorname{Ker} f = I \cap J$

3) Inoltre $I + J = A \Leftrightarrow f$ è surj e in tal caso $A/_{IJ} \cong A/_I \times A/_J$

ideali PRIMI E MASSIMALI

$(\mathcal{F}, \leq)$ poset, $X \subset \mathcal{F}$, $M \in \mathcal{F}$ è un maggiorante per X se $A \leq M \quad \forall A \in X$

$(\mathcal{F}, \leq)$ poset, $A \in \mathcal{F}$ è massimale se $\forall B \in \mathcal{F}$ t.c. $A \leq B \Rightarrow A = B$

$(\mathcal{F}, \leq)$ poset, $A \in \mathcal{F}$ si dice massimo se $\forall B \in \mathcal{F} \Rightarrow B \leq A$

$(\mathcal{F}, \leq)$ poset, catena di $\mathcal{F}$ è un sottoinsieme di $\mathcal{F}$ totalmente ordinato

$(\mathcal{F}, \leq)$ poset, $(\mathcal{F}, \leq)$ si dice induttivo se ogni catena ammette maggiorante

Lemma di Zorn → Sia $(\mathcal{F}, \leq)$ t.c. 1) poset 2) $\neq \emptyset$ 3) induttivo $\Rightarrow$ contiene elt. massimali

ideale primo → $I \subsetneq A$ si dice primo se $xy \in I \Rightarrow x \in I \vee y \in I \quad \forall x, y \in A$

$(p\mathbb{Z})_{p \text{ primo}}$ sono ideali primi di $\mathbb{Z}$ e anche (0)

ideale massimale → I è massimale se $\forall J \subsetneq A$ t.c. $I \subseteq J \Rightarrow I = J$

Proprietà ideali max → 1) Ogni ideale proprio di A è contenuto in un ideale massimale

2) Ogni elt. non invertibile di A è contenuto in un ideale max

Caratterezzazione ideali primi e max → 1) Sia $I \subsetneq A \Rightarrow I$ è primo $\Leftrightarrow A/_I$ dominio
2) Sia $I \subsetneq A \Rightarrow I$ è massimale $\Leftrightarrow A/_I$ campo

Caratterizzazione ideale primo e max. →
1) A dominio $\Leftrightarrow (0)$ è ideale primo
2) A campo $\Leftrightarrow (0)$ è ideale massimale
3) I massimale $\Rightarrow$ I primo

$\mathbb{Z}$ è un dom. ma non un campo ((0) non è max)

ANELLO DELLE FRAZIONI

parte moltiplicativa → A dominio, $S \subset A$ sottoinsieme t.c. 1) $0 \notin S$
2) $1 \in S$
3) $xy \in S \quad \forall x, y \in S$ (chiuso per moltiplicazio)

S si dice parte moltiplicativa di A

anello delle frazioni → • A come sopra, S p.m. $\quad S^{-1}A = \{ \frac{a}{s} \mid a \in A, s \in S \}/\sim \; = \frac{A \times S}{\sim}$

con $\sim$ $\quad \frac{a}{s} \underset{\text{associato}}{\sim} \frac{b}{t} \iff at = bs \qquad (a,s) \sim (b,t)$

• $(S^{-1}A, +, \cdot) =:$ anello delle frazioni di un dominio

$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \qquad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}$

è anello comm con 1 $\quad \frac{0}{1}, \frac{1}{1}$ elt. neutri

estensione di A → • $S^{-1}A$ estensione di A

$A \overset{f}{\hookrightarrow} S^{-1}A \quad f$ è omo inj di anelli

$a \longmapsto \frac{a}{1}$

slogan → Se A è un dom $\Rightarrow S = \underbrace{A \setminus \{0\}}_{A^*}$ è una p.m.

campo dei quozienti → • A dom, $S^{-1}A = Q(A)$ con p.m $S = A \setminus \{0\}$

⚠ $Q(A)$ è la cosa più grande

$A \subseteq Q(A)$ è il più piccolo campo che contiene A

Localizzato → • A dom, $P \subset A$, P ideale primo. $S = A \setminus P$ p.m.

$S^{-1}A = A_P =:$ localizzato di A e P

↳ anello locale (ha un unico ideal max)

invertibili di $S^{-1}A$ → • $(S^{-1}A)^* = \{ \frac{a}{s} \mid \frac{s}{a} \in S^{-1}A \}$ cioè $\exists\, b \in A, t \in S$ t.c. $\frac{s}{a} = \frac{b}{t} \iff st = ab \in S$

non è detto che $a \in S$ ma un suo multiplo sì

$(S^{-1}A)^* = \{ \frac{a}{s} \mid \exists\, b \in A \text{ t.c. } ab \in S \}$

ideali di $S^{-1}A$ → $I \subset A$ ideale $\quad S^{-1}I = \{ \frac{x}{s} \in S^{-1}A \mid x \in I, s \in S \}/\sim \; = \frac{I \times S}{\sim}$

↓

Proprietà $\quad I \subset A$ ideale, $S^{-1}A$ allora

Proprietà → $I \subset A$ ideale, $S^{-1}A$ allora

1) $S^{-1}I \subseteq S^{-1}A$ ideale
2) $\forall J \subseteq S^{-1}A,\ \exists I \subseteq A$ t.c. $J = S^{-1}I$
3) $S^{-1}I \subsetneq S^{-1}A \iff I \cap S = \phi$
4) P ideale primo di A con $P \cap S = \phi \Rightarrow S^{-1}P$ è ideale primo di $S^{-1}A$

$$S^{-1}A = \left\{ \frac{x}{s} \text{ t.c. } s \in S \quad x \in A \right\} \supseteq A = \left\{ \frac{x}{1} \text{ t.c. } x \in A \right\}$$

$J \cap A = I \subseteq A$

$= \left\{ \frac{y}{s} \mid s \in S \quad y \in \otimes \right\}$

per essere primo deve essere proprio ?

DIVISIBILITÀ NEI DOMINI

fatto → $a \mid b \iff (b) \subseteq (a)$

$2 \mid 4 \iff (4) \subseteq (2)$

associato → $a \sim a'$ se vale una delle 3: 1) $a \mid a'$ e $a' \mid a$
2) $\exists u \in A^*$ t.c. $a = ua'$
3) $(a) = (a')$

elt. primo → • A dom $x \notin A^* \cup \{0\}$ x si dice primo se $\forall a, b \in A$ se $x \mid ab \Rightarrow x \mid a$ o $x \mid b$

elt irriducibile → • A dom $x \notin A^* \cup \{0\}$ x si dice irrid. se $\forall a, b \in A$ $x \mid ab \Rightarrow a \in A^*$ V $b \in A^*$

PRIMO ⇒ IRRIDUCIBILE

fatto → x è irrid $\iff$ (x) è max nell'insieme degli ideali principali

DOMINI EUCLIDEI

def. di dom. euclideo → Un dom di integrità A si dice ED se $\exists\ g: A \setminus \{0\} \to \mathbb{N}$ t.c.
• $g(x) \leq g(xy) \quad \forall x, y$
• $\forall x \in A,\ \forall y \in A \setminus \{0\}\ \exists\ q, r \in A$ t.c. $x = yq + r$ con $g(r) < g(y)$ opp $r = 0$

$(\mathbb{Z}[i], N) = \{ a + ib \mid a, b \in \mathbb{Z} \}$ $\quad N: \alpha \to N(\alpha) = \alpha \bar{\alpha} = a^2 + b^2$, $\alpha = a + ib$

proprietà → • Dato ED. gli elt. invert. sono quelli di grado min.
$(\mathbb{Z}[i])^* = \{\pm 1, \pm i\}$

• Dato E.D. tutti gli ideali sono principali
(generati da un elt. di grado min)

PID

def PID → A dom. è PID se ogni suo ideale è princ.

proprietà → In un PID gli ideali primi sono (0) e gli id. max

PID non ED $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ con la semi norma.

UFD

def UFD → A dom se $\forall x \notin A^* \cup \{0\}$ si scrive in modo unico come prodotto di elt. irriducibili

$K[X]$, $\mathbb{Z}$

proprietà → UFD $\Rightarrow \exists$ m.c.d

ED, PID, UFD a confronto

ED $\quad d = (a,b)$ con A.E $\quad d = ax_0 + by_0$ (Bezout)

PID $\quad (d) = (a,b)$ non è facile calcolarlo

UFD $\quad \exists$ mcd. $\quad d = \text{mcd}(a,b)$ ma non è detto $(d) = (a,b)$

$(a,b) \subset (d)$

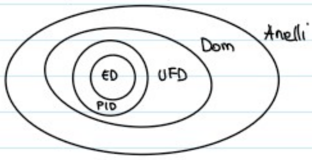
$\mathbb{Z}[x]$ $\quad (2,x)$ $\quad \text{mcd}(2,x) = 1$ ma $1 \notin (2,x)$

Teorema Caratterizzazione UFD → A dominio

1) A UFD
2) I) ogni elt irrid è primo
   II) ogni catena discendente di divisibilità è stazionaria
   $\{a_i\} \subset A$ con $a_{i+1} | a_i \ \forall i \geq 0 \Rightarrow \exists n_0$ tc $a_i \sim a_{n_0} \ \forall i \geq n_0$
   equivalentemente ogni catena ascendente di ideali principali è staz.
   $\{(a_i)\}$ $\quad (a_1) \subseteq (a_2) \subseteq \dots \ \exists n_0$ t.c. $(a_i) = (a_{n_0}) \ \forall i \geq n_0$

PID $\Rightarrow$ UFD

ED $\Rightarrow$ PID $\Rightarrow$ UFD



Anello non UFD $\quad K[\{x^{\frac{1}{n}}\}_{n \geq 1}]$

$\sqrt[4]{x}\sqrt[4]{x} = \sqrt{x}$ $\qquad x^{\frac{1}{2^n}} | \dots | x^{\frac{1}{4}} | x^{\frac{1}{2}} | x$

IRRID $\not\Rightarrow$ PRIMO

$\mathbb{Z}[\sqrt{-5}]$ 2 è irrid ma non primo

$2 | 6 = (1+\sqrt{-5})(1-\sqrt{-5})$ ma 2 non divide i singoli fattori

Polinomi e Anelli

fatto →
- A UFD $\Rightarrow$ A[x] UFD $\qquad$ SI UFD
- A PID $\not\Rightarrow$ A[x] PID $\quad (\mathbb{Z}, \mathbb{Z}[x])$
- A ED $\not\Rightarrow$ A[x] ED

NO PID, ED.

contenuto di f → contenuto di f

A UFD, $f(x) \in A[x]$ $\quad f(x) = \sum_{i=1}^{n} a_i x^i \Rightarrow c(f) = \text{mcd}(a_0, \dots, a_n)$

fatto → • A UFD $\Rightarrow A[x]$ UFD   SI UFD

• A PID $\not\Rightarrow A[x]$ PID $(\mathbb{Z}, \mathbb{Z}[x])$ NO PID, ED.
• $A \in D \not\Rightarrow A[x] \in D$

contenuto di f → contenuto di f
A UFD, $f(x) \in A[x]$ $f(x) = \sum_{i=1}^{n} a_i x^i \Rightarrow c(f) = \mathrm{mcd}(a_0, \ldots, a_n)$

primitivo → f primitivo se $c(f) \sim 1$

Lemma di Gauß → Dati $f, g \in A[x] \Rightarrow c(fg) = c(f)c(g)$
monico $\Rightarrow$ primitivo

Corollario → $f, g \in A[x]$ con $c(f) = 1$ e $f | g$ in $K[x]$ ($\mathbb{Q}$)
con K campo dei quoz $\Rightarrow f | g$ in $A[x]$ ($=\mathbb{Z}$)

Osservazione → $f(x)$ è riduc in $K[x] \Rightarrow$ è rid in $A[x]$, con polinomi dello stesso gr. associati a quelli mult.

IRRID DI $A[x]$ → • $f(x) \in A$ e irrid. in A (cioè cost)
• $f(x) \in A[x]$ con $\deg(f) \geq 1$ $c(f) = 1$ e f è irrid in $K(x)$

POLINOMI

$A[x] = \{a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \mid n \in \mathbb{N}, a_i \in A\}$ · A anello comm. con unità

$f(x) \in A[x]$ prende il nome di polinomio

$(A[x], +, \cdot)$ è anello comm con unità

Proprietà del grado
1) $\deg(f(x)+g(x)) \leq \max\{\deg f(x), \deg g(x)\}$
2) Se A è dom. d'integrità $\deg(f(x) g(x)) = \deg f(x) + \deg g(x)$

Fatti

A dominio $\Rightarrow A[x]$ dominio

A dominio $\Rightarrow (A[x])^* = A^*$

controesempio $A = \mathbb{Z}/_{4\mathbb{Z}}[x]$ anello che non è un dominio

$(\bar{2}x + \bar{1})^2 = \bar{4}x^2 + \bar{1} + \bar{4}x = \bar{1} \Rightarrow (\bar{2}x - \bar{1})$ è inverso di se stesso ma $(\bar{2}x - \bar{1}) \notin \mathbb{Z}/_{4\mathbb{Z}}^*$

Polinomi a coeff. in un campo

Teo divisione euclidea

$f, g \in \mathbb{K}[x]$, $f \neq 0 \Rightarrow \exists!\ q, r \in K[x]$ t.c. $g(x) = q(x) f(x) + r(x)$ con $0 \leq \deg r(x) < \deg f(x)$.

Teo Ruffini

$f(x) \in \mathbb{K}[x]$, $\alpha \in \mathbb{K}$. Allora $f(\alpha) = 0$ (cioè α è radice di f) $\Leftrightarrow x - \alpha \mid f(x)$

irriducibile $\rightarrow$ $f(x) \in \mathbb{K}[x]$ pol. non cost. f è irriducibile se $f(x) = g(x) h(x)$ con $g, h \in \mathbb{K}[x]$ e $\deg g(x) = 0 \vee \deg h(x) = 0$
cioè un pol. è irrid. quando si può scomporre soltanto come un pol. di grado uguale per una costante (pol. di grado 0, che è invertibile)

primo $\mapsto$ $f(x) \in \mathbb{K}[x]$ si dice primo se quando $f(x) \mid g(x)h(x) \Rightarrow f(x) \mid g(x) \vee f(x) \mid h(x)$

$f(x) \in \mathbb{K}[x]$ è irriducibile $\Leftrightarrow$ è primo

Teo fatt. unica

ogni pol. di $\mathbb{K}[x]$ non cost. si fattorizza in modo unico come prodotto di pol. irriducibili

$f(x) \in \mathbb{K}[x]$ $f(x) \neq 0 \Rightarrow f(x)$ ha al più $\deg f$ radici in $\mathbb{K}$, ciascuna con la propria molteplicità

$\mathbb{C}[x]$

Teo fondamentale dell'algebra $\rightarrow$ Ogni pol. non cost. in $\mathbb{C}[x]$ ammette almeno una radice in $\mathbb{C}$

$p(x) \in \mathbb{C}[x]$ è irriducibile in $\mathbb{C}[x] \Leftrightarrow \deg p(x) = 1$

Ogni pol. non cost. in $\mathbb{C}$ si fattorizza come prodotto di pol. di grado 1

Ogni pol. in $\mathbb{C}[x]$ ha tante radici quanto il suo grado.

$\mathbb{R}[x]$

I pol. irriducibili in $\mathbb{R}[x]$ sono quelli : 1) di grado 1

2) di grado 2 con $\Delta < 0$

$$x^4+1 = (x^2+1)^2 - 2x^2 = (x^2+\sqrt{2}\,x+1)(x^2-\sqrt{2}\,x+1)$$

$$x^4+1 = \frac{x^8-1}{x^4-1} = \frac{\prod_{i=0}^{7}(x-\rho_8^i)}{\prod_{j=0}^{3}(x-\rho_4^j)} = (x-\rho_8^1)(x-\rho_8^3)(x-\rho_8^5)(x-\rho_8^7)$$

non avere radici $\not\Rightarrow$ irriducibilità tranne per pol. di grado 2 e 3

$\mathbb{Q}[x]$

$\forall f(x) \in \mathbb{Q}$ $\exists \gamma \in \mathbb{Q}^*$ t.c. $f(x) = \gamma f_1(x)$ con $f_1(x) \in \mathbb{Z}[x]$ ($\subset \mathbb{Q}[x]$)

e l'MCD tra i coeff. di $\gamma f_1(x) = 1$ cioè $f_1(x)$ e' primitivo

Il problema della fatt. di un pol. in $\mathbb{Q}[x]$ si riduce a quello di un pol. in $\mathbb{Z}[x]$

$\mathbb{Z}[x]$

Teorema delle radici razionali

$f(x) \in \mathbb{Z}[x] \Rightarrow$ ogni sua radice razionale è della forma $\frac{\alpha}{\beta}$ con 1) $(\alpha, \beta) = 1$

$\parallel$

$a_0 + a_1 x + \dots + a_n x^n$

2) $\alpha, \beta \in \mathbb{Z}$

3) $\alpha \mid a_0$

4) $\beta \mid a_n$

Il teorema ci permette quindi di trovare tutte le potenziali radici razionali di un polinomio in Z[x], tuttavia, se nessuna di quelle determinate è una radice, allora tutte le sue radici (che esistono per il Teorema Fondamentale dell'Algebra) sono irrazionali o complesse.
Al contrario, se sono state trovate esatta�mente deg f(x) radici razionali, allora il polinomio è completamente fattorizzabile in polinomi di primo grado irriducibili in Z[x] per il Teorema di Fattorizzazione Unica.

Riduzione mod primo

$f(x) \in \mathbb{Z}[x]$ riducibile in $\mathbb{Z}[x] \Rightarrow \forall p$ primo t.c. $p \nmid a_n$ $\pi_p(f(x))$ è riducibile

$f(x) \in \mathbb{Z}[x]$ un pol. primitivo, se $\exists$ p primo $p \nmid a_n$ t.c. $\pi_p(f(x))$ e' irrid. in $\mathbb{Z}/p\mathbb{Z}[x]$

$\Rightarrow f(x)$ e' irrid in $\mathbb{Z}[x]$ ($\Rightarrow$ anche in $\mathbb{Q}[x]$)

$f(x)$ irrid in $\mathbb{Z}[x]$ ($\Rightarrow \mathbb{Q}[x]$) $\not\Rightarrow f(x)$ irrid in $\mathbb{Z}/p\mathbb{Z}[x]$

x^4+1 e' irrid in $\mathbb{Z}[x]$ ma rid. in $\mathbb{Z}/2\mathbb{Z}[x]$

es. rid mod p

$x^2+x+1 \in \mathbb{Z}[x]$ essendo pol. di II grado e' suff. verificare che non abbia radici in $\mathbb{Z}/2\mathbb{Z}$ $\pi_2(x^2+x+1) = x^2+x+\bar{1}$ ($\bar{0}$ e $\bar{1}$ non sono radici)

e' irrid. in $\mathbb{Z}/2\mathbb{Z}[x] \Rightarrow$ e' irrid in $\mathbb{Z}[x]$

I pol. della forma $d_2x^2 + d_1x + d_0$ con d_1, d_2, d_0 dispari e senza fattori comuni sono irrid in $\mathbb{Z}[x]$

Criterio di Eisenstein

$f(x) = a_n x^n + \quad + a_0 \in \mathbb{Z}[x]$ primitivo.

sia p primo se: 1) $p \nmid a_n$

2) $p \mid a_i$ $\forall i = \{0, \dots, n-1\}$

3) $p^2 \nmid a_0$

$\Rightarrow f(x)$ e' irrid in $\mathbb{Z}[x]$ ($\underset{G.}{\Rightarrow}$ $\mathbb{Q}[x]$)

IDEALI E POLINOMI

$A = \mathbb{K}[x]$ $\quad f(x) \in \mathbb{K}[x]$ $\quad (f(x)) = f(x)\,\mathbb{K}[x] = \{f(x)a(x) \mid a(x) \in \mathbb{K}[x]\}$

$\left(\frac{\mathbb{K}[x]}{(f(x))}, +, \cdot\right)$ è un anello comm con 1

è dato dai resti della div. per $f(x)$ cioè dai polinomi $r(x)$ con $\deg r < \deg f$.

dimensione

$\frac{\mathbb{K}[x]}{(f(x))}$ è un $\mathbb{K}$-sp.v. di dim $= \deg(f(x))$ e base $\{1, \overline{x}, \dots, \overline{x}^{\deg f(x)-1}\}$

elt.

$\overline{a(x)} \in \frac{\mathbb{K}[x]}{(f(x))}$

1) $\overline{a(x)}$ è invertibile $\Leftrightarrow (a(x), f(x)) = 1$

2) $\overline{a(x)}$ è un divisore di 0 $\Leftrightarrow (a(x), f(x)) \neq 1$

$\frac{\mathbb{K}[x]}{(f(x))}$ è un campo $\Leftrightarrow f(x)$ è irrid in $\mathbb{K}[x]$

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ è un campo

esempio

$\mathbb{K} = \mathbb{F}_2$ $f(x)$ irrid. in $\mathbb{F}_2[x]$ di grado n.

$\frac{\mathbb{F}_2[x]}{(f(x))}$ è un campo (è anche uno sp. vett. di dim n)

il campo ha 2^n elt ed è $\cong$ a $\mathbb{F}_2^n$

criterio della derivata

$\mathbb{K}$ campo, $f(x) \in \mathbb{K}[x]$ allora $(f(x), f'(x)) \neq 1 \Leftrightarrow \exists \alpha \in \overline{\mathbb{K}}$ t.c. $f(x) = (x-\alpha)^2 g(x) \in \overline{\mathbb{K}}[x]$

esempio

$f(x) = x^3 - 5x^2 + 7x - 3$ $\qquad A = \frac{\mathbb{F}_5[x]}{(f(x))}$

1) $\# A$

2) $\# D(A)$

3) $\# A^*$

4) $\# \mathcal{N}(A)$

Soluzione

$f(x)$ è irriducibile? $f(x) = x^3 + 2x + 2$ in $\mathbb{F}_5$

1 è radice $1+2+1$ $\quad (x-1)$

3 è radice $27+6+2$ $\quad (x-3)$ $\Big] \; x^2 - 4x + 3$

$$\begin{array}{l|l} x^3 + 2x + 2 & x^2 - 4x + 3 \\ x^3 - 4x^2 + 3x & x + 4 \\ \hline 4x^2 - x + 2 & \\ 4x^2 - 16x + 12 & \\ \hline 15x - 10 \equiv 0 \ (5) & \end{array}$$

$f(x) = (x+4)(x-3)(x-1) = (x-1)^2(x+2)$

$\# A = \# \{ a_0 + a_1 x + a_2 x^2 \mid a_0, a_1, a_2 \in \mathbb{F}_5 \} = 5^3$

base $= \{1, x, x^2\}$ sp vett $\mathbb{F}_5{}^3$

$\# D(A) = \{ p(x) \text{ t.c. } (f(x), p(x)) \neq 1 \}$

$D_1 = \{ p(x) \text{ t.c. } x-1 \mid p(x) \}$

$D_2 = \{ p(x) \text{ t.c. } x+2 \mid p(x) \}$

grado $3-1 = 2$

$\# D_1 = \# \{ (x-1) h(x) \} = 25$

$h(x) = \underset{\substack{\downarrow \\ 5 \text{ modi}}}{a}x + \underset{\substack{\downarrow \\ 5 \text{ modi}}}{b}$ di grado ≤ 2

$\# D_2 = \# \{ (x+2) h(x) \} = 25$

$\# (D_1 \cup D_2) = \# D_1 + \# D_2 - \# (D_1 \cap D_2) = 25 + 25 - 5$

$\hookrightarrow \begin{cases} x-1 \mid g(x) \\ x+2 \mid g(x) \end{cases} \Rightarrow g(x) = (x-1)(x+2) \underset{\mathbb{F}_5}{\overset{\cap}{k}}$

invertibili $5^3 - \underset{D(A)}{\underset{\shortparallel}{45}} = 80$

nilpotenti. Sono le classi $\overline{g(x)}$ divisibili per ognuno dei fattori irriducibili di $f(x)$
$=$ multipli di $(x-1)(x+2) = D_1 \cap D_2$

I nilpotenti sono 5

Interi di Gauss

$\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$
$\mathbb{Z}[i]$ e' un dom. euclideo $N: \mathbb{Z}[i] \longrightarrow \mathbb{N}$
$a+ib \longmapsto a^2+b^2$

$(\mathbb{Z}[i])^* = \{1,-1,i,-i\}$

$p \in \mathbb{Z}$, se $p \equiv 3\ (4) \Rightarrow p$ e' irriducibile in $\mathbb{Z}[i]$

Dato $a+ib \in \mathbb{Z}[i]$ se $N(a+ib)$ e' primo in $\mathbb{Z} \Rightarrow a+ib$ è irriducibile in $\mathbb{Z}[i]$

Fatto
- $1+i$ è irriducibile in $\mathbb{Z}[i]$
- $(2)\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i] = (1-i)^2\mathbb{Z}[i]$
- $\dfrac{\mathbb{Z}[i]}{(1+i)} \cong \mathbb{F}_2$

Fatto
- p primo $p \in \mathbb{Z}$ se $p \equiv 1\ (4) \Rightarrow p = (a+bi)(a-bi)$ con $a+bi, a-bi \in \mathbb{Z}[i]$ primi e non associati
cioè $p = a^2+b^2 = (a+bi)(a-bi)$

Gli elt. primi di $\mathbb{Z}[i]$ sono, a meno di associati, tutti e solo gli elt. della forma
1) $1+i$
2) i primi p di $\mathbb{Z}$ t.c. $p \equiv 3\ (4)$
3) $a+ib,\ a-ib \in \mathbb{Z}[i]$ t.c. $a^2+b^2 = p$ e' un primo di $\mathbb{Z}$ $p \equiv 1\ (4)$

Quozienti di $\mathbb{Z}[i]$

$p \in \mathbb{Z}$ primo dispari

1) se $p \equiv 3\ (4) \Rightarrow \mathbb{Z}[i]/(p) \cong \mathbb{F}_{p^2}$

2) se $p \equiv 1\ (4)$ e $p = (a+ib)(a-ib) \Rightarrow \dfrac{\mathbb{Z}[i]}{(a+ib)} \cong \mathbb{F}_p$
in questo caso $\dfrac{\mathbb{Z}[i]}{(p)} \cong \mathbb{F}_p \times \mathbb{F}_p$

$\# \mathbb{Z}[i]/(\alpha) = N(\alpha)$ con α primo di $\mathbb{Z}[i]$

operazioni fra ideali

$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

$\dfrac{\mathbb{Q}[x,y]}{(x-y)} \cong \mathbb{Q}[x]$ $\varphi: \mathbb{Q}[x,y] \longrightarrow \mathbb{Q}[x]$
$p(x,y) \longrightarrow p(x,x)$

φ è surj e $\operatorname{Ker}\varphi = (x-y)$

Ideali primi e max di $\mathbb{Z}[x]$

$A \subseteq R$ anelli $P \subseteq R$ ideale primo di R $\Rightarrow$ $P \cap A$ è ideale primo di A

M max in $\mathbb{Z}[x]$. Supp. $M \cap \mathbb{Z}$ contenga un numero primo $\Rightarrow$ $M = (p, f(x))$ dove $f(x)$ e' irrid in $\mathbb{F}_p[x]$

(0)
$(p)\mathbb{Z}[x]$ con $p \in \mathbb{Z}$ primo
$(p, f(x))$ con $p \in \mathbb{Z}$ primo e $\overline{f(x)}$ irrid. in $\mathbb{F}_p[x]$
$(f(x))$ con $f(x)$ primitivo e irriducibile in $\mathbb{Z}[x]$

primi

$(p, f(x))$ con $\overline{f(x)}$ irrid. in $\mathbb{F}_p[x]$ max.

PID

A PID, ogni ideale primo diverso da (0) di A e' un ideale max

A PID, B dom. $\varphi: A \to B$ omo di anelli surj $\Rightarrow$ φ è iso / B è campo

Se C è anello t.c. $C[x]$ è PID $\Rightarrow$ C campo.