COMPLEMENTI SUGLI ANELLI

Note Title 12/5/2018

LEMMA DI GAUSS

A = UFD, K = campo delle fraz. di A,

$p(x) \in A[x]$. Sono equivalenti:

(i) $p(x)$ è irriid. in $A[x]$

(ii) $p(x)$ è irriid. in $K[x]$ + $p(x)$ è PRIMITIVO, ovvero $c(p(x)) = (1)$

Se $p(x) = a_n x^n + \dots + a_0$, questo vuol dire

$$(a_n, \dots, a_0) = A$$

$A[x]$ PID $\Rightarrow$ A campo

$A[x]$ PID $\Rightarrow$ $A[x]$ dominio $\Rightarrow$ A dominio.

$A = \dfrac{A[x]}{(x)} \Rightarrow$ siccome A è dominio, (x) è primo.

$(x) \neq (0)$, (x) PRIMO $\Rightarrow$ (x) massimale

$\Rightarrow$ A è $A[x]/$ ideale massimale, quindi è un campo.

Legami tra irriducibilità in 1 e 2 variabili

Sia $p(x,y) \in \mathbb{Q}[x,y]$ t.c. $p(x, y_0) \in \mathbb{Q}[x]$ è irriducibile $\forall y_0 \in \mathbb{Q}$. È vero che $p(x,y)$ è irriducibile? **NO**

$$p(x,y) = (y^2+1)(x^2+y^2+1)$$

$$p(x, y_0) = (y_0^2+1)\left(X^2 + (y_0^2+1)\right) \text{ è irrid } \forall y_0$$

Si può però concludere che se

$$p(x,y) = p_1(x,y)\, p_2(x,y)$$

allora uno fra p_1 e p_2 coinvolge solo la y.

$$(1+x^2+y^2)\cdot(yx+1)$$

Supponiamo che $\deg_x p_1 = m > 0$, $\deg_x p_2 = n > 0$

Allora $p_1(x,y) = a_m(y)x^m + \dots + a_0(y)$

$p_2(x,y) = b_n(y)x^n + \dots + b_0(y)$

Siccome $\mathbb{Q}$ è infinito, $\exists\, y_0 \in \mathbb{Q}$ t.c.

$$a_m(y_0) \neq 0 \qquad b_n(y_0) \neq 0$$

$\Rightarrow$ $p(x,y_0) = \underbrace{p_1(x,y_0)}_{\deg m}\ \underbrace{p_2(x,y_0)}_{\deg n}$, il che contraddice l'ipotesi.

Cosa vuol dire che $p(x,y) = \sum_{j=0}^{d} c_j(y)x^j$ è divisibile per un polinomio $q(y)$ nella sola y?

Vuol dire che $q(y) \mid \left(c_0(y), \dots, c_d(y)\right)$

Oss Non serve davvero sapere che $p(x,y_0)$ sia irrid $\forall y_0$, basta provare più valori di y_0 del grado in y del polinomio

IRRIDUCIBILE vs PRIMO: un esempio

$$A = \mathbb{Z}[x]/(x^2+5) \qquad \left(a+b\sqrt{-5} \in \mathbb{Q}(\sqrt{-5}),\ a,b \in \mathbb{Z}\right)$$

Dim che A è integro: se e solo se (x^2+5) è un ideale primo. Siccome $\mathbb{Z}[x]$ è un UFD,

(x^2+5) è primo $\iff$ x^2+5 è primo $\overset{\text{UFD}}{\iff}$ x^2+5 irriducibile in $\mathbb{Z}[x]$

$\iff$ x^2+5 irrid in $\mathbb{Q}[x]$

$\overline{2} \in A$ è irriducibile:

$$2 = (a+b\sqrt{-5})(c+d\sqrt{-5}) \qquad a,b,c,d \in \mathbb{Z}$$

$$\downarrow \text{norma}$$

$$4 = (a^2+5b^2)(c^2+5d^2)$$

Per disuguaglianze $b=d=0$, e $2=ac$ ha solo soluzioni banali

2 non è primo: $2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$

2 non divide nessuno dei 2 fattori:

$$1+\sqrt{-5} = 2 \cdot (e+f\sqrt{-5})$$

$\Rightarrow$ $1=2e$ e $1=2f$ con $e,f \in \mathbb{Z}$, impossibile

(2) non è un ideale massimale, ma è massim. nella famiglia degli ideali principali propri

Non massimale $\Leftarrow$ non primo, appena visto

$$(2) \subsetneq (\alpha) \overset{?}{\Longrightarrow} (2) = (\alpha) \text{ o } (\alpha) = (1)$$

$$\Downarrow$$

$2 \in (\alpha) \Rightarrow 2 = \alpha \cdot \beta \quad \beta \in A$, ma

2 irrid $\Rightarrow$ $\begin{cases} \alpha \text{ unità} \Rightarrow (\alpha) = (1) \\ \beta \text{ unità} \Rightarrow (\alpha) = (2) \end{cases}$

Cerchiamo un ideale massimale che contenga (2).

$$\left\{ \begin{matrix} \text{ideali di } A \\ \text{contenenti } I \end{matrix} \right\} \longleftrightarrow \left\{ \text{ideali di } A/I \right\}$$

Studiamo $A/(2) = \dfrac{\mathbb{Z}[x]/(x^2+5)}{(2, x^2+5)/(x^2+5)} \simeq \dfrac{\mathbb{Z}[x]}{(2, x^2+5)}$

$$\simeq \frac{\mathbb{Z}[x]/(2)}{(2, x^2+5)/(2)} \simeq \frac{\mathbb{F}_2[x]}{(x^2+5)} \simeq \frac{\mathbb{F}_2[x]}{((x+1)^2)}$$

Ideali di $\dfrac{\mathbb{F}_2[x]}{(x+1)^2}$ $\longleftrightarrow$ ideali di $\mathbb{F}_2[x]$ contenenti $(x+1)^2$

Se voglio $\mathcal{P} \subseteq \mathbb{F}_2[x]$ primo che contenga $(x+1)^2$

è necessariamente $(x+1)$

[$(x+1)^2 \in \mathcal{P} \Rightarrow (x+1) \in \mathcal{P}$; inoltre $(x+1)$

è massimale + $(x+1) \subseteq \mathcal{P} \Rightarrow (x+1) = \mathcal{P}$]

Seguendo $\mathcal{P}$ tramite gli isomorfismi troviamo l'ideale $Q = (1+\sqrt{-5}, 2)$

$$Q \ni 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

$\sqrt{(0)}$ = intersezione dei primi

$$\sqrt{(0)} = \{ a \in A \mid \exists n \ a^n = 0 \}$$

$\sqrt{(0)}$ nilradicale di $A \subseteq \bigcap_{P \text{ primo}} P$

$\forall P$ primo, se $a^n = 0 \in P \Rightarrow a \in P$

Viceversa: dobbiamo mostrare che dato $a \in A$ non nilpotente $\exists P$ primo con $a \notin P$

Considero la famiglia

$$\mathcal{F} = \left\{ \begin{array}{l} I \subsetneq A \text{ ideale proprio} \\ a^n \notin I \quad \forall n \end{array} \right\} \ni (0)$$

Per applicare Zorn serve che ogni catena ammetta un maggiorante:

dato $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$

voglio $I \in \mathcal{F}$ che contenga $I_j \quad \forall j$.

$I = \bigcup I_j$: è un ideale, contiene tutti gli I_j

$I \in \mathcal{F}$? Sì, verifica immediata

$\xRightarrow{\text{Zorn}} \exists\, \mathfrak{M} \in \mathcal{F}$ massimale in $\mathcal{F}$.

Voglio dimostrare che $\mathfrak{M}$ è un ideale primo.

$xy \in \mathfrak{M}, \quad x \notin \mathfrak{M}, \quad y \notin \mathfrak{M}$

$I = (\mathfrak{M}, x) \qquad J = (\mathfrak{M}, y)$

$\notin \mathcal{F} \qquad \notin \mathcal{F}$

$\Rightarrow a^k \in I \quad e \quad a^h \in J$

$a^k = \underset{\in \mathfrak{M}}{m_1} + bx \qquad a^h = \underset{\in \mathfrak{M}}{m_2} + cy$

$a^{k+h} = (m_1 + bx)(m_2 + cy)$

$= \underset{\in}{m_1}(m_2 + cy) + \underset{\in}{m_2}(bx) + \underset{\in}{(xy)}(bc)$

111 111 111

assurdo perché 111 non contiene potenze di a. Quindi 111 è primo e non contiene a, come voluto.

Esercizio A anello comm. t.c. $\forall x \in A \ \exists n$ t.c. $x^n = x$. Allora ideali primi = ideali massimali

Soluzione Sia $\mathfrak{P}$ un ideale primo. Voglio dim. che $A/\mathfrak{P}$ è un campo.

$\bar{x} \in A/\mathfrak{P}$. Due casi. $\bar{x} = 0$ ✓

$\bar{x} \neq 0 \iff x \notin \mathfrak{P}$

Per hp, $x^n = x \iff x(\underbrace{x^{n-1} - 1}_{\in \mathfrak{P} \text{ (primalità)}}) = 0 \in \mathfrak{P}$

$\Rightarrow x^{n-1} \equiv 1 \ (\mathfrak{P}) \iff \bar{x}^{n-1} = 1$ in $A/\mathfrak{P}$

Inverso di $\bar{x} = \bar{x}^{n-2}$ □

CAMPI

$\phi : K \longrightarrow K$ omomorf. di campi $\Rightarrow$ iniettivo

Se $\phi : K \longrightarrow K$ è surgettiva $\Rightarrow$ isomorfismo

Il viceversa non vale:

$$K = \mathbb{F}_p(t) = \left\{ \frac{a(t)}{b(t)} \;\middle|\; \begin{array}{c} a(t), b(t) \in \mathbb{F}_p[t] \\ b(t) \neq 0 \end{array} \right\}$$

$$\begin{array}{rccc} \phi : & K & \longrightarrow & K \\ & f(t) & \longmapsto & (f(t))^p \end{array} \qquad \text{omomorfismo}$$

$$(f_1(t) + f_2(t))^p = f_1(t)^p + f_2(t)^p$$

$$= f_1(t^p) + f_2(t^p)$$

è iniettivo ma non surgettivo $(t \notin \operatorname{Im}\phi)$

Esercizio Determinare $\operatorname{Aut}(\mathbb{F}_{p^2})$

Soluzione $\varphi \in \operatorname{Aut}(\mathbb{F}_{p^2})$. $\varphi(1) = 1$

$$\varphi(1)\varphi(1) = \varphi(1)$$

$$X^2 = X \Rightarrow \varphi(1) \in \{0, 1\}$$

$$\varphi(1+1) = \varphi(1) + \varphi(1) = 2$$

$$\Rightarrow \quad \varphi|_{\mathbb{F}_p} = id$$

Esempio: $\mathbb{F}_9 = \dfrac{\mathbb{F}_3[x]}{(x^2+1)} = \{ a+b\bar{x} \mid a,b \in \mathbb{F}_3 \}$

$$\left(= \{ a+bi \mid a,b \in \mathbb{F}_3 \} \right)$$

Un automorfismo di $\mathbb{F}_9$ è determinato da $\varphi(\bar{x})$:

$$\varphi(a+b\bar{x}) = \varphi(a) + \varphi(b)\,\varphi(\bar{x})$$

$$= a + b\,\varphi(\bar{x})$$

$$\bar{x}^2+1 = 0 \quad \Rightarrow \quad \varphi(\bar{x})^2 + 1 = 0$$

$$\varphi(\bar{x}) \in \{ \bar{x}, -\bar{x} \}$$

$$\updownarrow$$

$$\varphi \in \{ id, \; \begin{matrix} a+bi \\ \downarrow \\ a-bi \end{matrix} \}$$

C'è un automorfismo non banale: $c \longmapsto c^3$

$$\bar{x} \longmapsto \bar{x}^3 = -\bar{x}$$

In generale: $\mathbb{F}_{p^2} = \mathbb{F}_p \oplus \mathbb{F}_p\,\alpha$

Se ho $\phi : \mathbb{F}_{p^2} \longrightarrow \mathbb{F}_{p^2}$ so che $\phi|_{\mathbb{F}_p} = id$,

quindi ϕ è determinato da $\phi(\alpha)$

$$\phi(a+b\alpha) = \phi(a) + \phi(b)\,\phi(\alpha)$$
$$= a + b\,\phi(\alpha)$$

Il pol. minimo di α è di grado 2, diciamo

$$m(x) = x^2 + c_1 x + c_0$$

$$\Rightarrow \quad \alpha^2 + c_1\alpha + c_0 = 0 \quad \Rightarrow \quad \phi(\alpha)^2 + c_1\phi(\alpha) + c_0 = 0$$

Quindi: $\phi(\alpha)$ è una radice di $m(x)$ in $\mathbb{F}_{p^2}$.

$m(x)$ ha 2 radici $\Rightarrow$ al max due possib. per ϕ

I due ϕ sono: l'identità e $\underbrace{x \longmapsto x^p}_{\text{Frobenius}}$

Basta verificare che Frob $\neq$ id.

- Se Frob $=$ id $\Rightarrow \forall\, c \in \mathbb{F}_{p^2}$, $c^p = c$, assurdo perché per questioni di grado ci sono $\leq p$ elementi t.c. $c^p = c$.
- $(\mathbb{F}_{p^2})^\times$ è ciclico di ordine p^2-1. Sia γ un generatore. Frob $=$ id $\Rightarrow \gamma^p = \gamma \Rightarrow \gamma^{p-1} = 1$,

ma questo è assurdo perché $\mathrm{ord}(\gamma) = p^2 - 1$