

UNICITÀ CAMPI DI SPEZZAMENTO

Osservazione 1 Siano R, S anelli commutativi con unità, $\eta: R \rightarrow S$ omomorfismo di anelli e $u \in S$. Allora esiste un unico

$\tilde{\eta}: R[x] \rightarrow S$ omomorfismo estensione di η

(cioè $\tilde{\eta}(r) = \eta(r)$ per ogni $r \in R$)

talché $\tilde{\eta}(x) = u$

[la definizione di $\tilde{\eta}$ deve essere la seguente:

$$\tilde{\eta}\left(\sum a_k x^k\right) = \sum \eta(a_k) u^k$$

2) Sia $\eta: F \rightarrow \bar{F}$ isomorfismo di campi

allora esiste un unico isomorfismo di anelli

$\tilde{\eta}: F[x] \rightarrow \bar{F}[x]$ tale che $\tilde{\eta}(a) = \eta(a)$

per ogni $a \in F$ e $\tilde{\eta}(x) = x$

Notazione: denotiamo $\tilde{\eta}(p(x))$ con $\bar{p}(x)$

Definizione Siano $F \subseteq E$ estensione di campi e $a \in E$ algebrico su F , il polinomio monico $p(x)$ tale che $p(a) = 0$ è detto polinomio minimo di a

Oss il polinomio minimo è irriducibile

(11)

Lemma Sia $\eta: \mathbb{F} \rightarrow \overline{\mathbb{F}}$ isomorfismo di campi

e siano $\mathbb{F} \subseteq \mathbb{E}$ e $\overline{\mathbb{F}} \subseteq \overline{\mathbb{E}}$ estensioni.

Se $\alpha \in \mathbb{E}$ algebrico su $\mathbb{F}$ con polinomio minimo $p(x)$ allora:

η può essere esteso a un monomorfismo $\alpha: \mathbb{F}(\alpha) \rightarrow \overline{\mathbb{E}}$

$\Leftrightarrow$

$\overline{p}(x)$ ha una radice in $\overline{\mathbb{E}}$

Se $\overline{p}(x)$ ha una radice in $\overline{\mathbb{E}}$ il numero delle estensioni di η è lo stesso numero delle radici distinte di $\overline{p}(x)$ in $\overline{\mathbb{E}}$

Dim: Sia $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$

" $\Rightarrow$ " Supponiamo quindi che esista $\alpha: \mathbb{F}(\alpha) \rightarrow \overline{\mathbb{E}}$ monom.

$$p(\alpha) = 0 \Rightarrow \alpha(p(\alpha)) = 0$$

$$\Rightarrow \underset{\alpha \text{ monom}}{\alpha(a_n)} [\alpha(\alpha)]^n + \dots + \alpha(a_0) = 0$$

$$\Rightarrow \underset{\text{est. di } \eta}{\eta(a_n)} [\eta(\alpha)]^n + \dots + \eta(a_0) = 0$$

$$\Rightarrow \overline{p}(\eta(\alpha)) = 0$$

" $\Leftarrow$ " sia $\bar{\alpha}$ una radice di $\bar{p}(x)$

Esiste un omomorfismo $\alpha_0: F[x] \rightarrow \bar{E}$

tale che $\alpha_0(x) = \bar{\alpha}$

[per osservazione precedente]

α_0 deve essere definito nel seguente modo:

$$\alpha_0(q(x)) = \bar{q}(\bar{\alpha})$$

Siccome $\text{Ker } \alpha_0 \supseteq (p(x))$ [perché $\bar{p}(\bar{\alpha}) = 0$]

α_0 induce un omomorfismo $\alpha_1: \frac{F[x]}{(p(x))} \rightarrow \bar{E}$

tale che $\alpha_1(q(x) + (p(x))) = \bar{q}(\bar{\alpha})$

Notiamo che esiste un isomorfismo $F(\alpha) \rightarrow \frac{F[x]}{(p(x))}$

e lo componiamo con α_1

$$\begin{array}{ccccc} F(\alpha) & \xrightarrow{\cong} & \frac{F[x]}{(p(x))} & \xrightarrow{\alpha_1} & \bar{E} \\ & & & \uparrow & \\ & & & \alpha & \end{array}$$

$$q(\alpha) \rightarrow q(x) + (p(x)) \rightarrow \bar{q}(\bar{\alpha})$$

ottenendo α estensione di η

$F(\alpha)$ è un campo e α è un omomorfismo non banale $\Rightarrow \alpha$ è un monomorfismo

Continuamo le estensioni

(13)

$\alpha: F(\alpha) \rightarrow \bar{E}$ monom est di $\eta \Rightarrow \alpha(\alpha)$ radice di $\bar{p}(x)$

Inoltre α è unicamente determinata da $\alpha(\alpha)$

$$\left[\alpha \rightarrow \alpha(\alpha) \Rightarrow \underbrace{a_n \alpha^n + \dots + a_0}_{\text{elemento generico di } F(\alpha) = F[\alpha]} \longrightarrow \eta(a_n) [\alpha(\alpha)]^n + \dots + \eta(a_0) \right]$$

e per ogni radice di $\bar{p}(x)$ possiamo costruire un'estensione



Teorema Siano $\eta: F \rightarrow \bar{F}$ isomorfismo di campi, $p(x) \in F[x]$ non costante.

Consideriamo $E, \bar{E}$ campi di spezzamento di $p(x)$ e $\bar{p}(x) = \tilde{\eta}(p(x))$, rispettivamente.

Allora η ha un'estensione $\alpha: E \rightarrow \bar{E}$ che è un isomorfismo.

Il numero degli isomorfismi che estendono η è minore o uguale a $[E:F]$, se $p(x)$ ha n radici distinte il numero delle estensioni è esattamente $[E:F]$.

Dimostrazione posso supporre $p(x)$ monico
dimostrazione per induzione su $[E:F]$

Sic $[E:F]=1$ in questo caso $E=F$

per cui $p(x) = \prod_i (x - \alpha_i)$ in $F[x]$

e $\bar{p}(x) = \prod_{i=1}^i (x - \sigma(\alpha_i))$ in $\bar{F}[x]$

otteniamo $\bar{F}=\bar{E}$ e σ è l'unica estensione possibile

passo induttivo posso supporre

$[E:F] > 1$ cioè $E \neq F$

Se considero la scomposizione in fattori irriducibili di $p(x)$ in $F[x]$ non può contenere solo fattori lineari

Supponiamo $q(x) \in F[x]$ sia un fattore irriducibile di $p(x)$ tale che $\deg q(x) > 1$

In $E[x]$ abbiamo che $p(x) = \prod_{i=1}^m (x - \alpha_i)$

Siccome $q(x) \mid p(x)$ possiamo supporre

$$q(x) = \prod_{i=1}^m (x - \alpha_i)$$

[scegliendo $q(x)$ monico e riordinando le radici di $p(x)$ in E]

Analogamente abbiamo che

$$\bar{p}(x) = \prod_{i=1}^n (x - \alpha_i) \quad \text{e} \quad \bar{q}(x) = \sum_{i=1}^m (x - \beta_i)$$

[perché se $q(x) \mid p(x)$ abbiamo che $\bar{q}(x) \mid \bar{p}(x)$]

Sia $K = F(\alpha_1)$ $[K : F] = m = (\deg q(x))$

- Per il lemma esistono k monomorfismi $\alpha_1, \dots, \alpha_k$ da K a $\bar{E}$ che estendono η dove k è il numero degli α_i distinti
- E è un campo di spezzamento di $p(x)$ su K e $[E : K] = \frac{[E : F]}{[F : K]} = \frac{[E : F]}{m} < [E : F]$
- inoltre $\bar{E}$ è un campo di spezzamento di $\bar{p}(x)$ su $\bar{K}$

Per induzione esiste un isomorfismo

fra E e $\bar{E}$ che estende α_i

Inoltre l'induzione ci dice che esistono al più $[E : K]$ isomorfismi estensioni di α_i (e quindi anche estensioni di η)

Se le radici sono distinte il numero delle estensioni è esattamente $[E : K]$

numero
estensioni
ottenute $\leq r [E:k] \leq m [E:k] = [E:F]$

Se le radici sono distinte:

numero
estensioni
ottenute $= r [E:k] = m [E:k] = [E:F]$

Le estensioni ottenute con questo processo
sono tutte le estensioni possibili?

ovvero Sia α un'estensione di $\mathcal{U}$
allora α è un'estensione di qualche α_i ?

$\alpha|_K : K \rightarrow \bar{E}$ è un monomorfismo
che estende $\mathcal{U} \Rightarrow \alpha|_K = \alpha_i$ per qualche i 

Osservazione: Considero $E, \bar{E}$ due campi
di spezzamento di $p(x)$ su F . Applico
il Teorema a $\text{Id} : F \rightarrow F$ e ottengo
l'esistenza di $\varphi : E \rightarrow \bar{E}$ isomorfismo.

Corollario: il campo di spezzamento di
un polinomio è unico a meno di
isomorfismi.