LA TEORIA ASTRATTA

Come generalizzare quanto fatto finora al caso di K campo qualsiasi?

Campo di spezzamento e chiusura algebrica

Definizione

Sia $f(x) \in K[x]$. Si dice campo di spezzamento di $f(x)$ su K un'estensione E/K t.c.

1) $f(x)$ si decompone in fattori lineari in $E(x)$
2) Se $\alpha_1 \dots \alpha_n$ sono le radici di $f(x)$ in E, allora $E = K(\alpha_1, \dots, \alpha_n)$

Prop.

Ogni polinomio ha un campo di spezzamento.

Dim:

Per induzione sul grado. Costruiamo $K_1 = K(\alpha)$ in cui $f(x)$ ha una radice. Su K_1 $f(x)$ si decompone $f(x) = (x-\alpha) f_1(x)$ con $\deg(f_1(x)) < \deg(f(x))$. ▣

Inoltre, il campo di spezzamento è unico a meno di K-isomorfismi.

Discende dalla seguente.

Proposizione

Sia $\theta : K_1 \longrightarrow K_2$ isomorfismo

$f(x) \in K_1[x]$, E_1 il campo di spezzamento di $f(x)$ in $K_1[x]$, E_2 il campo di spezzamento di $(\theta f)(x)$ in $K_2[x]$.

Allora θ si estende a un isomorfismo $E_1 \to E_2$.

Dim

Induzione sul grado n. Se $n \geq 1$ sia $F_1 = \frac{K_1[x]}{(f(x))} = K_1(\alpha)$

$F_2 = \frac{K_2(x)}{(\theta f(x))} = K_2(\alpha')$. θ si estende a isom. $\tilde{\theta} : F_1 \to F_2$.

Tale che $\tilde{\theta}(\alpha) = \alpha'$! Su F_1, $f(x)$ si decompone

$$f(x) = (x-\alpha)\, g(x)$$

$$\theta(f(x)) = (x-\alpha')(\theta g)(x)$$

$\deg g(x) < \deg f(x) \Rightarrow$ si applica l'hp. induttiva. ◻

(Variante del teorema $(**)$)

Esistenza della chiusura algebrica

Lemma

Sia K campo e E/K un'estensione algebrica t.c. ogni polinomio $f(x) \in K[x]$ si decompone in fattori lineari in E.

Allora E è una chiusura algebrica di K.

Dim.

Basta provare $\bar{E}$ alg. chiuso, cioè

α algebrico su $\bar{E}$ $\Rightarrow$ $\alpha \in A$.

Poiché $\bar{E}$ algebrico su K

α algebrico su $\bar{E}$ $\Rightarrow$ α algebrico su K.

$\Rightarrow \alpha \in \bar{E}$. ∎

Sia K un campo e S l'insieme dei polinomi unid. a coeff. in K che pensiamo dotato di un buon ordinamento (ogni sottoinsieme non vuoto ha un minimo). Questa hp. è eq.te all'assioma della scelta, e rende possibile l'induzione transfinita.

Pensiamo gli elementi di S come indici di se stessi; quindi $s \in S$ lo scriviamo $f_s(x)$.

Per ogni $s \in S$ costruiamo un campo $K_s \supseteq K$ t.c.

i) f_s si decompone in fattori lineari in K_s

ii) $K_t \subseteq K_s$ se $t \le s$

iii) K_s è algebrico su K.

Poniamo $H = \bigcup_{t<s} K_t$ e K_s = campo di spezzamento di $f_s(x)$ su H.

Poniamo $\tilde{K} = \bigcup_s K_s$

Allora $\tilde{K}$ è algebrico su K e contiene tutte le radici dei polinomi in $K[x]$.
Per il lemma, $\tilde{K}$ è una chiusura alg. di K.

<u>Prop.</u> Sia
1) Sia $\tilde{K}$ una chiusura algebrica di K e F/K estensione algebrica.
Esiste un K-omomorfismo $F \longrightarrow \tilde{K}$
2) Due chiusure algebriche sono F-isomorfe.

<u>Dim</u>
Sia $F = K(T)$ e consideriamo un buon ordinamento su T. Per ogni $t \in T$ poniamo
$F_t = K(T_t) \quad T_t = \{s \in T \mid s < t\}$
Si costruisce $\varphi_t : F_t \longrightarrow \tilde{K}$ t.c. $\varphi_t|_{F_s} = \varphi_s \ \forall s < t$.
- se T_t non ha massimo allora $F_t = \bigcup_{s<t} F_s$ e poniamo $\varphi_t = \varphi_s$ su ogni s.
- se T_t ha massimo u (unico per l'ipotesi di buon ordinamento) allora $T_t = T_u \cup \{u\}$, $F_t = F_u(u)$ (estensione semplice). Quindi φ_u si estende a $\varphi_t : F_t \longrightarrow \tilde{K}$ usando il teorema di estensione (*) e il fatto che $\tilde{K}$ è alg. chiuso.

3) Se $\overline{K}_1$ e $\overline{K}_2$ sono due chiusure alg. di K da (2) esiste K-omom. $j: \overline{K}_1 \longrightarrow \overline{K}_2$.

$j(\overline{K}_1)$ è alg. chiuso, e $\overline{K}_2$ algebrico su K $\Rightarrow$ $j(\overline{K}_1) = \overline{K}_2$. $\boxtimes$

Separabilità

Sia K campo e $\overline{K}$ chiusura algebrica.

Se ripetiamo in questo contesto gli argomenti utilizzati nel caso di sottocampi di $\overline{\mathbb{Q}}$, tutto continua a valere, eccetto la proposizione fondamentale che se $[F:K] = n$ con $F \subseteq \overline{K}$, e posto

$$\mathcal{J}(F/K) = \{ \varphi : F \longrightarrow \overline{K} \mid K\text{-omom.} \}$$

allora $|\mathcal{J}(F/K)| = n$.

Questo fatto era stato dimostrato a partire dal fatto che nel caso di campi di numeri un polinomio irrid. ha radici distinte.

In generale abbiamo visto che questo non è vero se $\mathrm{car}(K) = p$ $\left(K = \mathbb{F}_p(x) \quad f(y) = y - x^p \right)$.

Def.

Sia K un campo.

1) Un polinomio $f(x) \in K[x]$ si dice separabile

se ha radici distinte in $\bar{K}$

2) Se α è algebrico su K, α si dice separabile su K se il suo polinomio minimo (su K) è separabile

3) Un'estensione algebrica E/K si dice separabile se tutti i suoi elementi sono separabili su K.

Campo perfetto: se $\bar{K}$ è separabile (per es. se car$(K)=0$).

Quando un polinomio (monico) irrid. $f(x) \in K[x]$ non è separabile?

Deve essere $MCD(f(x), f'(x)) \neq 1 \Rightarrow f'(x) \mid f(x) \Rightarrow f'(x) = 0$.

$f(x) = X^n + a_{n-1}X^{n-1} + \dots + a_0 = 0$

$f'(x) = nX + (n-1)a_{n-1}X^{n-1} + \dots + a_1 = 0 \iff$

car$(K) = p$ e i soli coeff. non nulli di $f(x)$ sono indicizzati da multipli di p

$f(x) = X^{mp} + a_{(m-1)p}X^{(m-1)p} + \dots + a_pX^p + a_0$

Teorema

Sia car$(K) = p$ t.c. $Frob_p : K \longrightarrow K$ automorfismo allora K è perfetto.

Dim.

Si ha $a_{jp} = b_j^p$ per qc. $b_j \in K$

Quindi $f(x) = X^{mp} + b_{m-1}^pX^{(m-1)p} + \dots + b_1^pX^p + b_0 = (X^m + b_{m-1}X^{m-1} + \dots + b_1X + b_0)^p$

contro l'irriducibilità di $f(x)$.

<u>Corollario</u>: i campi finiti sono perfetti.

Se K è perfetto allora
- $|\mathcal{J}(E/K)| = [E:K]$ per ogni est. finita E/K
- Vale il teorema dell'elem. primitivo

<u>Def.</u> • Un'estensione finita E/K si dice normale se $\forall \varphi \in E/K$ si ha $\varphi(E) \subseteq E$
• si dice Galois se è separabile e normale.

Se E/K è di Galois allora
$$Gal(E/K) = Aut(E/K) = \mathcal{J}(E/K)$$
e $|Gal(E/K)| = [E:K]$

Vale la corrispondenza di Galois tra sottocampi intermedi $K \subseteq F \subseteq E$ e sottogruppi di $Gal(E/K)$ come dimostrato nel caso dei campi di numeri.

Teorema di Galois per campi finiti

Ogni campo finito ha cardinalità p^t per qc. p.
Viceversa, per ogni primo p e $t \in \mathbb{N}$, $t \geq 1$, esiste un campo di ordine p^t, unico a meno di isom.
Poniamo $\mathbb{F}_{p^t}$ = campo di ordine p^t.
Si ha

1) $\mathbb{F}_{p^t}$ contiene un campo di ordine $p^r \iff r \mid p$
2) Ogni $\alpha \in \mathbb{F}_{p^t}$ è radice del polinomio $X^{p^t} - X$.
3) $\forall t$, c'è l'automorfismo di Frobenius

$$\varphi : \mathbb{F}_{p^t} \longrightarrow \mathbb{F}_{p^t}$$
$$\alpha \longmapsto \alpha^p.$$

Sia $\overline{\mathbb{F}_p}$ una chiusura algebrica di $\mathbb{F}_p$.

Prop.

1) $\forall t$, esiste un unico campo $\mathbb{F}_{p^t}$ in $\overline{\mathbb{F}_p}$ con p^t elementi.
2) $\mathbb{F}_{p^t}$ è il campo di spezzam. in $\overline{\mathbb{F}_p}$ del polinomio $X^{p^t} - X$
3) $\mathbb{F}_{p^t}/\mathbb{F}_p$ è di Galois e $Gal\left(\mathbb{F}_{p^t}/\mathbb{F}_p\right)$

Dim.

1) e 2) discendono dal fatto che il campo di

spezzamento di un polinomio in una chiusura algebrica esiste ed è unico.

3) $\mathbb{F}_{p^t}/\mathbb{F}_p$ è di Galois in quanto $\mathbb{F}_{p^t}$ è un campo di spezzamento, e $[\mathbb{F}_{p^t} : \mathbb{F}_p] = t$.
Si ha $\varphi \in Gal\left(\mathbb{F}_{p^t}/\mathbb{F}_p\right)$ e $\forall r$
$\varphi^r : \alpha \longmapsto \alpha^{p^r}$.
Quindi $\mathbb{F}_{p^t}^{\varphi^r} = \mathbb{F}_{p^r}$
Ne segue che φ ha periodo esattamente t in $Gal\left(\mathbb{F}_{p^t}/\mathbb{F}_p\right)$, quindi
$$Gal\left(\mathbb{F}_{p^t}/\mathbb{F}_p\right) = \langle \varphi \rangle \simeq \mathbb{Z}_t$$

Come corollario, se $r \mid t$
$$Gal\left(\mathbb{F}_{p^t}/\mathbb{F}_{p^r}\right) = \langle \varphi^r \rangle \simeq \mathbb{Z}_{t-r}$$

$\Rightarrow$ tutte le estensioni di campi finiti sono estensioni cicliche.