Resta da dimostrare che data E/K ciclica di ordine un divisore di m, esiste $y \in E/K$ t.c. la sua risolvente di Lagrange è non nulla. (Δ)

Estensioni radicali nel caso $\mu_m \not\subseteq K$.

Se K non contiene le radici m-esime dell'unità, il campo di spezzamento di $f(x) = x^m - b$ è $K(\alpha, \omega)$ con $\alpha^m = b$, ω radice primitiva m-esima di 1.

Si ha una torre

$$K \subseteq K(\omega) \subseteq K(\omega, \alpha)$$

- $K \subseteq K(\omega)$: ciclotomica, di gruppo di Galois un sottogruppo di $\mathbb{Z}/m\mathbb{Z}$
- $K(\omega) \subseteq K(\omega, \alpha)$: ciclica di ordine un divisore di m

Quindi

$\mathrm{Gal}\left(\frac{E}{K}\right)$ ha un sottogruppo normale ciclico C con quoziente un gruppo abeliano A

Traccia, norma, discriminante

E/K estensione, $n = [E:K]$, $\mathcal{G}(E/K) = \{\sigma_1, \dots, \sigma_n\}$

Sia $\alpha \in E$ e consideriamo la moltiplicazione per α

$$\begin{aligned} m_\alpha : E &\longrightarrow E \\ \beta &\longmapsto \alpha\beta \end{aligned}$$

è K-lineare ossia $m_\alpha \in \mathrm{End}_K(E)$ (endomorfismi di K-sp. vett.)

Fissata una base $\beta_1, \dots, \beta_n$ di E su K, a m_α corrisponde una matrice m_α ossia $A \in M_n(K)$

$$A = \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}$$

$\alpha\beta_1 \quad \alpha\beta_2 \dots$ nella base $\beta_1 \dots \beta_n$.

Chiamiamo **traccia, norma, polinomio caratteristico** di α la traccia, norma, polinomio caratteristico della matrice A.

$\mathrm{tr}_{E/K}(\alpha)$, $N_{E/K}(\alpha)$, polinomio car. di α

(Cambiando base, A viene trasformata nella sua coniugata per una matrice in $GL_n(K)$: $A' = BAB^{-1}$

Proprietà della traccia

- La traccia è additiva. $\mathrm{tr}_{E/K}(\alpha+\beta) = \mathrm{tr}_{E/K}(\alpha) + \mathrm{tr}_{E/K}(\beta)$
- La norma è moltiplicativa $N_{E/K}(\alpha\beta) = N_{E/K}(\alpha)\, N_{E/K}(\beta)$
- Se il polinomio caratt. di α su K è
  $x^n + a_{n-1}x^{n-1} + \dots + a_0$ si ha $\mathrm{tr}_{E/K}(\alpha) = a_{n-1}$, $N_{E/K}(\alpha) = (-1)^n a_0$
- Se $\alpha \in K$ $\mathrm{tr}_{E/K}(\alpha) = n\alpha$, $N_{E/K}(\alpha) = \alpha^n$

Proposizione Supponi $[E:K] = n$, $\alpha \in E$
Se $f(x)$ è il polinomio minimo di α su K e ha grado m, allora il pol. caratteristico di α su E/K è $f(x)^{\frac{n}{m}}$.

Dim.
Sia $q = \frac{n}{m}$ e $\beta_1 \dots \beta_q$ una base di E su $K(\alpha)$.
Allora
$\mathcal{B} = (\beta_1, \alpha\beta_1, \dots, \alpha^{m-1}\beta_1, \beta_2, \alpha\beta_2, \dots, \alpha^{m-1}\beta_2, \dots, \beta_q, \alpha\beta_q, \dots, \alpha^{m-1}\beta_q)$
è una base di E su K.
Si ha

$$m_\alpha(\beta_i) = \alpha\beta_i$$
$$m_\alpha(\alpha\beta_i) = \alpha^2\beta_i$$
$$\vdots$$
$$m_\alpha(\alpha^{m-2}\beta_i) = \alpha^{m-1}\beta_i$$

Supponiamo $f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_0$

$m_\alpha(\alpha^{i-1}\beta_i) = (-a_0 - a_1\alpha \dots - a_{m-1}\alpha^{m-1})\beta_1$

Quindi la matrice di m_α rispetto alla base $\mathcal{B}$ è una matrice a blocchi

$$A = \begin{pmatrix} M & & \\ & \ddots & \\ & & M \end{pmatrix} \quad \text{dove } M \in M_m(K)$$

e $$M = \begin{pmatrix} 0 & 0 & & 0 & -a_0 \\ 1 & 0 & & \vdots & \vdots \\ 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & & 1 & -a_{m-1} \end{pmatrix}$$

$\Rightarrow$ $\text{pol car}(A) = \text{pol car}(M)^q = f(x)^q$.

- Se $\mathcal{I}(E/K) = \{\sigma_1, \dots, \sigma_m\}$ allora

  $\text{tr}_{E/K}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_m(\alpha)$

  $N_{E/K}(\alpha) = \sigma_1(\alpha) \cdot \dots \cdot \sigma_m(\alpha)$

  Il pol. car. di α su K è

  $(x - \sigma_1(\alpha)) \dots (x - \sigma_m(\alpha))$

- Se $K \subseteq F \subseteq E$ e $\alpha \in E$

  $\text{tr}_{E/K} = \text{tr}_{F/K} \circ \text{tr}_{E/F}$ $\qquad$ $N_{E/K} = N_{F/K} \circ N_{E/F}$

Discriminante

Siano $a_1, \dots, a_n \in E$; $\mathcal{I}(E/K) = \{\sigma_1, \dots, \sigma_n\}$

$\Delta = D(a_1, \dots, a_n) = \det(\sigma_i(a_j))$

Prop.

i) $\Delta^2 \in K$

ii) Se $a_1, \dots, a_n$ sono l.i. su K allora $\Delta \neq 0$

Dim.

Sia $A = \sigma_i(a_j)$

$({}^tA A)_{ij} = \sum_k \sigma_k(a_i)\sigma_k(a_j) = tr_{E/K}(a_i a_j) \in K$

$\Rightarrow \det(A)^2 = \det({}^tA A) \in K.$

ii) $\varphi : E \times E \longrightarrow K$ forma bilineare
$(a, b) \longmapsto tr(ab)$

Se fosse degenere esisterebbe $a \in E$ t.c. $\forall b \in E \; h(ab) = 0$

Ma $\varphi(a, a^{-1}) = h(aa^{-1}) = h(1) = n \neq 0$

Segue φ non degenere $\Rightarrow \det({}^tAA) \neq 0 \Rightarrow \Delta \neq 0$

Corollario

Siano $\lambda_1, \dots, \lambda_n$ numeri complessi non tutti nulli; $\mathcal{I}(E/K) = \{\sigma_1, \dots, \sigma_n\}$

esiste $\beta \in E$ t.c. $\lambda_1\sigma_1(\beta) + \dots + \lambda_n\sigma_n(\beta) \neq 0$.

Dim.

Altrimenti la funzione $\lambda_1\sigma_1 + \dots + \lambda_n\sigma_n$ sarebbe nulla su E

Presi $\alpha_1 \dots \alpha_n$ base di E/K si avrebbe

$$\begin{cases} \lambda_1 \sigma_1(\alpha_1) + \dots + \lambda_n \sigma_n(\alpha_1) = 0 \\ \vdots \\ \lambda_1 \sigma_1(\alpha_n) + \dots + \lambda_n \sigma_n(\alpha_n) = 0 \end{cases}$$

$\Rightarrow \det(\sigma_i(\alpha_j)) = 0 \Rightarrow D(\alpha_1 \dots \alpha_n) = 0.$ ☐

In particolare:

Se E/K ciclica $\Rightarrow$ esiste $\alpha \in E$ t.c. la risolvente di Lagrange $\sum_i \eta^i \sigma^i(\alpha) \neq 0$ $\Rightarrow$ dimostro (△)

Risolubilità per radicali

Es: equazioni quadratiche $ax^2+bx+c=0$ $\quad a,b,c \in \mathbb{Q}$

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{a} \qquad x \in \mathbb{Q}(\sqrt{\Delta})$$

(esistono formule risolutive per equazioni di 3° grado (formula di Cardano) e di 4° grado (Cartesio).

Ad esempio l'equazione di 3° grado $x^3+aX+b=0$ ha come soluzioni

$$\alpha_1 = \sqrt[3]{-\frac{b}{2}+\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}} + \sqrt[3]{-\frac{b}{2}-\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}}$$

$$\alpha_2 = \omega(\quad\quad) + \omega^2(\quad\quad)$$

$$\alpha_3 = (\quad\quad) + \omega(\quad\quad)$$

Nella formula risolutiva compaiono funzioni razionali di radicali di funzioni razionali di radicali ecc. ecc.

Diamo una formulazione precisa alla nostra idea di "equazione risolubile per radicali"

Def:

Sia $K \subseteq \bar{\mathbb{Q}}$, e $f(x) \in K[x]$.

L'equazione $f(x)=0$ si dice risolubile per radicali su K se esiste una successione di campi

$$K_0 = K \subseteq K_1 \subseteq \dots \subseteq K_m$$

tale che K_m contiene tutte le radici di $f(x)$ e

per $i = 0, \dots, m-1$, $K_{i+1} = K_i(\alpha_i)$ con $\alpha_i^{n_i} \in K_i$ $(n_i \in \mathbb{N})$
Quindi K_{i+1} è un'estensione radicale di K_i.

Se $f(x)$ è risolubile per radicali, ogni radice α si esprime iterata di funzioni razionali di radicali dei coefficienti di $f(x)$ ma questo dà l'eq. risolutiva nel caso delle equazioni di $2^\circ, 3^\circ, 4^\circ$ grado.

Il Teorema di Abel-Ruffini (1788 - 1824) stabilisce la controparte galoisiana della risolubilità per radicali.

Def.
Un gruppo G si dice risolubile se esiste una catena di sottogruppi $G = G_0 \rhd G_1 \rhd G_2 \dots \rhd G_m = \{1\}$ tale che $G_{i+1} \lhd G_i$ e G_i / G_{i+1} è abeliano per $i = 0, \dots, m-1$. ∎

Teorema (Abel-Ruffini)
Il polinomio $f(x) \in K[x]$ è risolubile per radicali su $K \Leftrightarrow$ il suo gruppo di Galois su K è risolubile.