LEMMI PRELIMINARI ALLA DIMOSTRAZIONE DEL CRITERIO DI GALOIS PER LA RISOLUBILITÀ PER RADICALI

Def. $\mathbb{F}$ campo, il campo di spezzamento di $x^n - 1$ su $\mathbb{F}$ viene detto **campo ciclotomico di ordine n su $\mathbb{F}$**

Osservazione: Sia $\mathbb{Z}_n$ gruppo ciclico di ordine n, allora $Aut(\mathbb{Z}_n)$ è abeliano ed isomorfo al gruppo moltiplicativo $I = \{$elementi invertibili di $\mathbb{Z}_n$ rispetto al prodotto$\}$

Dim: (per esercizio)

Lemma 1 Se $\text{char}\,\mathbb{F} = 0$, allora il gruppo di Galois del campo ciclotomico di ordine n su $\mathbb{F}$ è abeliano

Dim. Chiamiamo $\mathbb{E}$ il campo ciclotomico

$(x^n - 1)' = n x^{n-1}$ (polinomio derivato di $x^n - 1$)

$MCD(x^n - 1, n x^{n-1}) = 1 \Rightarrow x^n - 1$ non ha radici multiple

Indichiamo nel seguente modo l'insieme delle radici di $x^n - 1$:

$$U = \{z_1, z_2, \dots, z_m\}$$

- U sottogruppo del gruppo moltiplicativo del campo ciclotomico
- U è ciclico di ordine n infatti sia

$$k = \max \{ |z_i| \mid z_i \text{ radice di } x^n - 1 \}$$

($|z_i|$: ordine di z_i)

Allora esiste z_j tale che $|z_j| = k$

Per ogni i $|z_i|$ divide k altrimenti $|z_i z_j| > k$ (ricordo che U è abeliano)

Se fosse $k < n$ z_i sarebbero tutte radici di $x^k - 1$, questo è impossibile

Possiamo concludere $k = n$ e U ciclico

- Usando un argomento già introdotto nel corso sappiamo che
  - se $\eta \in Gal(E/F) \Rightarrow \eta(U) = U$
  - $\eta|_U$ è un automorfismo del gruppo U

- possiamo definire un monomorfismo di gruppi

$$\varphi : Gal\left(E/F\right) \longrightarrow Aut(U)$$
$$\eta \longrightarrow \eta|_U$$

Possiamo concludere:

$$Gal\left(E/F\right) \cong \varphi\left(Gal\left(E/F\right)\right) \leq Aut(U) \cong Aut(\mathbb{Z}_n)$$

Osservazione: non è detto che φ sia suriettivo se $F = \mathbb{C}$, il campo di spezzamento di $x^n - 1$ è $\mathbb{C}$ stesso quindi

$$Gal\left(\mathbb{C}/\mathbb{C}\right) = \{Id_{\mathbb{C}}\}$$

mentre

$Aut(\mathbb{Z}_n)$ non è banale

Def. E si dice un'estensione abeliana (risp. ciclica) su F se E è un'estensione di Galois e $Gal\left(E/F\right)$ è abeliano (risp. ciclico)

Oss: Lemma 1 $\Rightarrow$ un campo ciclotomico su F con $\mathrm{char}\, F = 0$ è un'estensione abeliana su F

Lemma 2: Se F contiene n distinte radici n-esime dell'unità e sia $a \in F$, allora il gruppo di Galois di $x^n - a$ su F è ciclico di ordine un divisore di n

Dim: Siano $U = \{z_1, z_2, \dots, z_n\} \subseteq F$ le radici n-esime dell'unità

- Sia E il campo di spezzamento di $x^n - a$
- Sia r radice di $x^n - a$ in E

Allora se $z_i \in U$ otteniamo $z_i r$ radice di $x^n - a$

Quindi $\{rz_1, \dots, rz_n\}$ sono le radici di $x^n - a$ (e sono tutte distinte) e $E = F(r)$ (perché $U \subseteq F$)

Definiamo $\varphi : Gal(E/F) \longrightarrow U$ (gruppo ciclico moltiplicativo)

$\eta \longrightarrow z$ tale che $\eta(r) = zr$

(ricordo che η manda una radice di $x^n - a$ in una radice di $x^n - a$)

Osserviamo che se $\eta, \xi \in Gal(E/F)$

e $\eta(\alpha) = z\alpha \qquad \xi(\alpha) = z'\alpha$

allora $\eta \circ \xi(\alpha) = \eta(\xi(\alpha)) =$

$= \eta(z'\alpha) = \eta(z')\eta(\alpha) =$

$= z' \eta(\alpha) = z' z \alpha$

↑ perchè $z' \in F$

$\Rightarrow \varphi(\eta \circ \xi) = z z' = \varphi(\eta)\cdot\varphi(\xi)$

$\Rightarrow \varphi$ omomorfismo di gruppi

Inoltre siccome $E = F(\alpha)$

allora η è univocamente determinato dal $\eta(\alpha)$

e φ è iniettivo

$Gal(E/F) \cong \varphi(Gal(E/F)) \leq U$

U è ciclico di ordine n per la dimostrazione del punto precedente e quindi otteniamo la tesi e otteniamo che E su F è un'estensione ciclica ∎

Lemma 3 Sia p un numero primo, se F contiene p distinte radici p-esime dell'unità e E è un'estensione ciclica di grado p di F, allora esiste $d \in E$ tale che $E = F(d)$ con $d^p \in F$

[si può confrontare con il caso delle torri di radici quadrate]

Dim: • Sia $c \in E \setminus F$.

$$[E:F(c)]\,[F(c):F] = [E:F] = p$$

Siccome $[F(c):F] > 1$ allora

$$[E:F(c)] = 1 \quad \text{e} \quad E = F(c)$$

• Siano $U = \{z_1, \dots, z_p\} \subseteq F$ le radici p-esime dell'unità e η il generatore di $Gal(E/F)$

[Ricordo che $|Gal(E/F)| = [E:F] = p$]

Definiamo $c_i = \eta^{i-1}(c)$ $\quad 1 \le i \le p$

da cui $c_1 = c$ e $\eta(c_i) = c_{i+1}$

per $1 \le i \le p-1$ e $\eta(c_p) = c_1$

definiamo la risolvente di Lagrange

$$(z_i, C) = C_1 + C_2 z_i + C_3 z_i^2 + \dots + C_p z_i^{p-1}$$

Notiamo che $\eta(z_i, C) = C_2 + C_3 z_i + \dots + C_1 z_i^{p-1} = z_i^{-1}(z_i, C)$

da cui $\eta((z_i, C)^p) = (\eta(z_i, C))^p = (z_i^{-1}(z_i, C))^p = (z_i, C)^p$

e $(z_i, C)^p \in Gal(E/F) = F$

(η genera $Gal(E/F)$; estensione di Galois)

Possiamo esprimere $C_1, C_2, \dots, C_p$ come combinazione lineare di $(z_1, C)(z_2, C) \dots (z_p, C)$

infatti

$$\begin{pmatrix} 1 & z_1 & \dots & z_1^{p-1} \\ 1 & z_2 & \dots & z_2^{p-1} \\ \vdots & \vdots & & \vdots \\ 1 & z_p & \dots & z_p^{p-1} \end{pmatrix} \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_p \end{pmatrix} = \begin{pmatrix} (z_1, C) \\ (z_2, C) \\ \vdots \\ (z_p, C) \end{pmatrix}$$

questa si chiama matrice di Vandermonde

il cui determinante è $\prod_{i>j} (z_i - z_j) \neq 0$

Siccome $C = C_1$ otteniamo

$$E = F(C) = F((z_1, C), (z_2, C), \dots, (z_p, C))$$

Esiste un i tale che $(z_i, C) \notin F$

(altrimenti $F((z_1,C),(z_2,C),\dots,(z_p,C)) = F$)

Pongo $d = (z_i, C)$, e otteniamo

$[F(d) : F] = p$ da cui $E = F(d)$

(usando lo stesso argomento utilizzato all'inizio della dim.)

e $d^p = (z_i, C)^p \in F$ ∎

Esercizio!

$$\det \begin{pmatrix} 1 & z_1 & \cdots & z_1^{p-1} \\ 1 & z_2 & \cdots & z_2^{p-1} \\ \vdots & \vdots & & \vdots \\ 1 & z_p & \cdots & z_p^{p-1} \end{pmatrix} = \prod_{i>j} (z_i - z_j)$$

Lemma 4: Sia $q(x) \in F[x]$, K estensione di F allora il gruppo di Galois di q su K è isomorfo ad un sottogruppo del gruppo di Galois di q su F

Dim: Sia L campo di spezzamento di q su K L contiene E campo di spezzamento di q su F. Se $q(x) = \prod_i (x - r_i)$ in L

allora $L = K[r_1, \dots, r_n]$ e $E = F[r_1, \dots, r_n]$.

Se $\eta \in Gal\left(\frac{L}{K}\right)$ allora $\eta(\{r_1, \dots, r_n\}) = \{r_1, \dots, r_n\}$ e $\eta(F) = F$ perché $F \subseteq K$ da cui $\eta(E) = E$

Costruisco $\varphi : Gal(L/K) \longrightarrow Gal(E/F)$

$$\eta \longrightarrow \eta|_E$$

Osserviamo che se $\eta \neq Id_L \Rightarrow$

$\Rightarrow \eta$ agisce in maniera non banale su $\{r_1, \dots, r_n\}$

$\Rightarrow \eta|_E \neq Id_E$

Questo implica che φ è un monomorfismo e

$$Gal(L/K) \cong \varphi(Gal(L/K)) \leq Gal(E/K)$$

▨

Supponiamo $F \subseteq E$ campi con $[E:F] < \infty$

$\Rightarrow$ esistono $a_1, \dots, a_n \in E$ tali che $E = F(a_1, \dots, a_n)$ e a_i algebrici su F

[abbiamo già considerato questa implicazione]

Sia $q_i(x)$ il polinomio minimo di a_i su F

Definiamo $q(x) = \prod q_i(x)$ e K il campo di spezzamento di $q(x)$ su E

allora K è anche il campo di spezzamento di $q(x)$ su F

(perché $E = F(a_1, \dots, a_n)$ dove a_i radici di $q(x)$.)

Osserviamo che:

- se $q(x)$ è separabile (per esempio se $\mathrm{char} F = 0$) otteniamo che K su F è un'estensione normale (essendo il campo di spezzamento di $q(x)$ è un estensione di Galois)
- Ogni estensione normale di F contenente E contiene un campo di spezzamento di $q(x)$ su F (perché è normale e E contiene una radice di ogni fatt. irriducibile $q_i(x)$ di $q(x)$)

Questo si può tradurre dicendo che ogni estensione normale di F contenente E contiene un sottocampo isomorfo a K

i.e. a meno di isomorfismi, K è la minima estensione normale di F contenente E

Questo implica che a meno di isomorfismi K è determinato da E ed F.

Def. Chiamiamo K la chiusura normale di E su F (supponiamo sempre $q(x)$ separabile)

• se $\eta \in Gal(K/F)$, chiamiamo $\eta(E)$ il coniugato di E su F in K

Osservazione: i coniugati di E su F generano K

Dim: K' sottocampo di K generato da $\{\eta(E) \mid \eta \in Gal(K/F)\}$

Osserviamo che $\eta(K') = K' \Rightarrow \eta|_{K'} \in Gal(K'/F)$,

$$G' = \{\eta|_{K'} \mid \eta \in Gal(K/F)\} \leq Gal(K'/F)$$

e $Fix G' = F$

Per caratterizzazione estensioni di Galois otteniamo

K' normale su $F \Rightarrow K' = K$

$\mathrm{Id}(E) = E \subseteq K'$
e
K minima est. normale $\supseteq E$

□

Lemma 5 Siano $F \subseteq E$ campi e supponiamo ci sia una torre di radici

$F = F_1 \subseteq F_2 \subseteq \dots \subseteq F_{r+1} = E$ con $F_{i+1} = F(d_i)$ e $d_i^{m_i} \in F_i$

Supponiamo $E = F(a_1, \dots, a_t)$ con a_i avente polinomio minimo separabile

Allora K, la chiusura normale di E su F, ha una torre di radici su F per cui gli m_i sono gli stessi di $\{F_i\}$

Dim. K è generata dagli $\eta(E)$ con $\eta \in \mathrm{Gal}(K/F)$

- $\eta(F_i)$ è una torre di radici di $\eta(E)$ su F e $\eta(F_{i+1}) = \eta(F_i)(\eta(d_i))$ con $(\eta(d_i))^{m_i} \in \eta(F_i)$
- $K = F(\eta_1(d_1), \dots, \eta_1(d_r), \eta_2(d_1), \dots, \eta_2(d_r), \eta_3(d_1), \dots)$ con $\mathrm{Gal}(K/F) = \{\eta_1, \eta_2, \dots\}$

Usando gli $\eta_\ell(d_i)$ costruisco le torre di radice

□