LEZIONE 1-12-20

GRUPPO DI GALOIS DI $x^4 - 5x^2 + 9$ SU $\mathbb{Q}$ e $\mathbb{F}_{11}$

K = c.d.s. di $x^4 - 5x^2 + 9$

|

$\mathbb{Q}$

$$|Gal(K/\mathbb{Q})| = [K : \mathbb{Q}]$$

Ponendo $t = x^2$ $\rightsquigarrow$ $t^2 - 5t + 9$ $\rightsquigarrow$ $t_{1,2} = \frac{5 \pm \sqrt{25 - 36}}{2} = \frac{5 \pm i\sqrt{11}}{2}$

$$\Rightarrow x_{1,\dots,4} = \pm \sqrt{\frac{5 \pm i\sqrt{11}}{2}}$$

$$\Rightarrow K = \mathbb{Q}\left(\pm \sqrt{\frac{5 + i\sqrt{11}}{2}} ; \pm \sqrt{\frac{5 - i\sqrt{11}}{2}} \right)$$

(i $\pm$ sono inutili)

Vogliamo studiare l'irriducibilità di $x^4 - 5x^2 + 9 =: f(x)$.

OSS $f(x) = (x^2 + 3)^2 - 11x^2 = (x^2 + 3 + \sqrt{11}x)(x^2 + 3 - \sqrt{11}x)$

$x^2 + 3 + \sqrt{11}x$ $\rightsquigarrow$ $x_{1,2} = \frac{-\sqrt{11} \pm i}{2}$

$x^2 + 3 - \sqrt{11}x$ $\rightsquigarrow$ $x_{3,4} = \frac{\sqrt{11} \pm i}{2}$

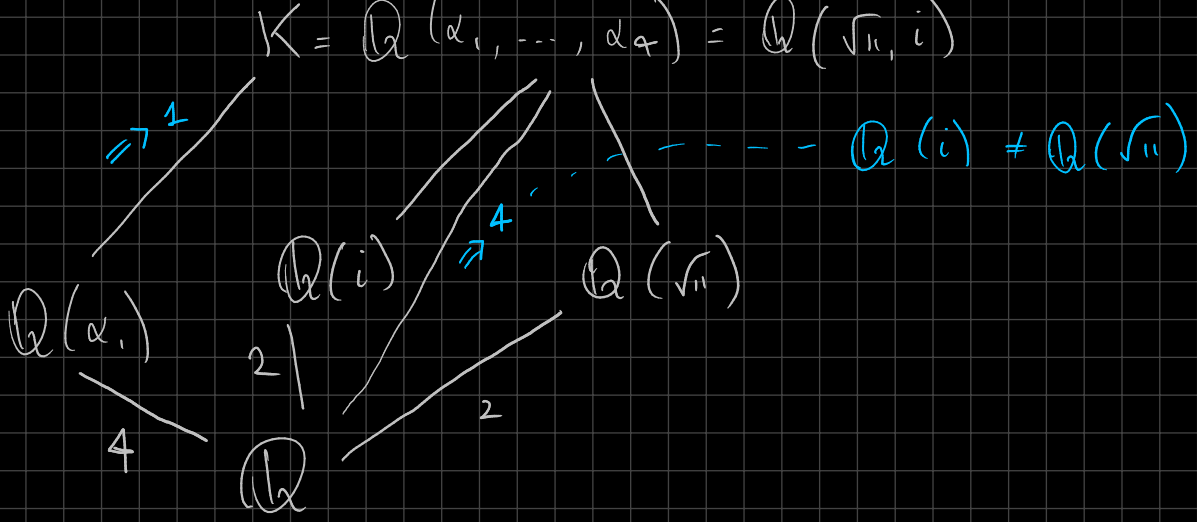
Dunque $\frac{-\sqrt{11} \pm i}{2}$ e $\frac{+\sqrt{11} \pm i}{2}$ devono essere uguali a $\pm\sqrt{\frac{5 \pm i\sqrt{11}}{2}}$ per qualche scelta di segno.

$$\Rightarrow K = \mathbb{Q}\left(\pm \frac{\sqrt{11} \pm i}{2} \right) = \mathbb{Q}(\sqrt{11}, i)$$

Per dim. l'irriducibilità, f sicuramente non ha radici razionali; quindi l'unica chance è fattorizzarla in $f_1 \cdot f_2$, entr. di grado 2.

OSS $f = (x^2+3+\sqrt{11}x)(x^2+3-\sqrt{11}x) \in \mathbb{R}[x]$
e tale fatt. è unica $\Rightarrow$ la fatt. su $\mathbb{Q}$, se esiste, deve coincidere con questa. ✗ f irriducibile!

ALTRO METODO Sapendo che le radici di f sono $\alpha_1, \dots, \alpha_4$ proviamo provare
$$f_1 = \begin{cases} (x-\alpha_1)(x-\alpha_2) \\ (x-\alpha_1)(x-\alpha_3) \\ (x-\alpha_1)(x-\alpha_4) \end{cases}$$
$\rightarrow$ nessuno sta in $\mathbb{Q}[x]$ RIP :(



ALTRO MODO: Voglio dire che $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_1, \dots, \alpha_4)$

(1) $\alpha_2 = -\alpha_1$, $\alpha_4 = -\alpha_3$ $\Rightarrow$ $\mathbb{Q}(\alpha_1, \dots, \alpha_4) = \mathbb{Q}(\alpha_1, -\alpha_1, \alpha_3, -\alpha_3)$
$= \mathbb{Q}(\alpha_1, \alpha_3)$

(2) $\alpha_1 \alpha_3 = \sqrt{\frac{5+i\sqrt{11}}{2}} \cdot \sqrt{\frac{5-i\sqrt{11}}{2}}$

$= \frac{\sqrt{5^2+11}}{2}$

$= \frac{\sqrt{36}}{2} = 3 \Rightarrow \alpha_3 = \frac{3}{\alpha_1}$

$\Rightarrow \alpha_3 \in \mathbb{Q}(\alpha_1) \Rightarrow \mathbb{Q}(\alpha_3, \alpha_1) = \mathbb{Q}(\alpha_1)$.

Calcolo del GRUPPO DI GALOIS

$$K = \mathbb{Q}(i, \sqrt{11}) \rightsquigarrow Gal(K/\mathbb{Q}) = \{ \varphi : K \longrightarrow \overline{\mathbb{Q}} \text{ con } \varphi|_{\mathbb{Q}} = id \}$$

Dato che ogni el. algebrico viene mandato in un suo coniugato dagli el. del gruppo di Galois, si ha che

$$\varphi(i) \in \{\pm i\} \quad ; \quad \varphi(\sqrt{11}) \in \{\pm\sqrt{11}\}$$

Ho al max 4 scelte; ma $|Gal(K/\mathbb{Q})| = [K:\mathbb{Q}] = 4$

dunque tutte queste scelte si realizzano.

$$\Rightarrow Gal(K/\mathbb{Q}) = \{ \varphi_1, \varphi_2, \varphi_3, \varphi_4 \}$$

dove $\varphi_1 = id$ $\quad \varphi_1 = \begin{cases} i \mapsto i \\ \sqrt{11} \mapsto \sqrt{11} \end{cases}$ $\quad \varphi_2 = \begin{cases} i \mapsto -i \\ \sqrt{11} \mapsto \sqrt{11} \end{cases}$ $\quad \varphi_3 = \begin{cases} i \mapsto i \\ \sqrt{11} \mapsto -\sqrt{11} \end{cases}$

$$\varphi_4 = \begin{cases} i \mapsto -i \\ \sqrt{11} \mapsto -\sqrt{11} \end{cases}$$

OSS $\quad \varphi_1^2 = \varphi_2^2 = \varphi_3^2 = \varphi_4^2 = id$

$$\Rightarrow Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$\sim \quad \circ \quad \sim \quad \circ \quad \sim$

$$K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3})$$

1) $K/\mathbb{Q}$ è normale
2) Gruppo di Gal. di $K/\mathbb{Q}$

1) Basta far vedere che K è un c.d.s. di una famiglia di pol.

Tentativo 1: K cols di $x^3 - 3 \Rightarrow K = \mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{3}\zeta_3, \sqrt[3]{3}\zeta_3^2)$

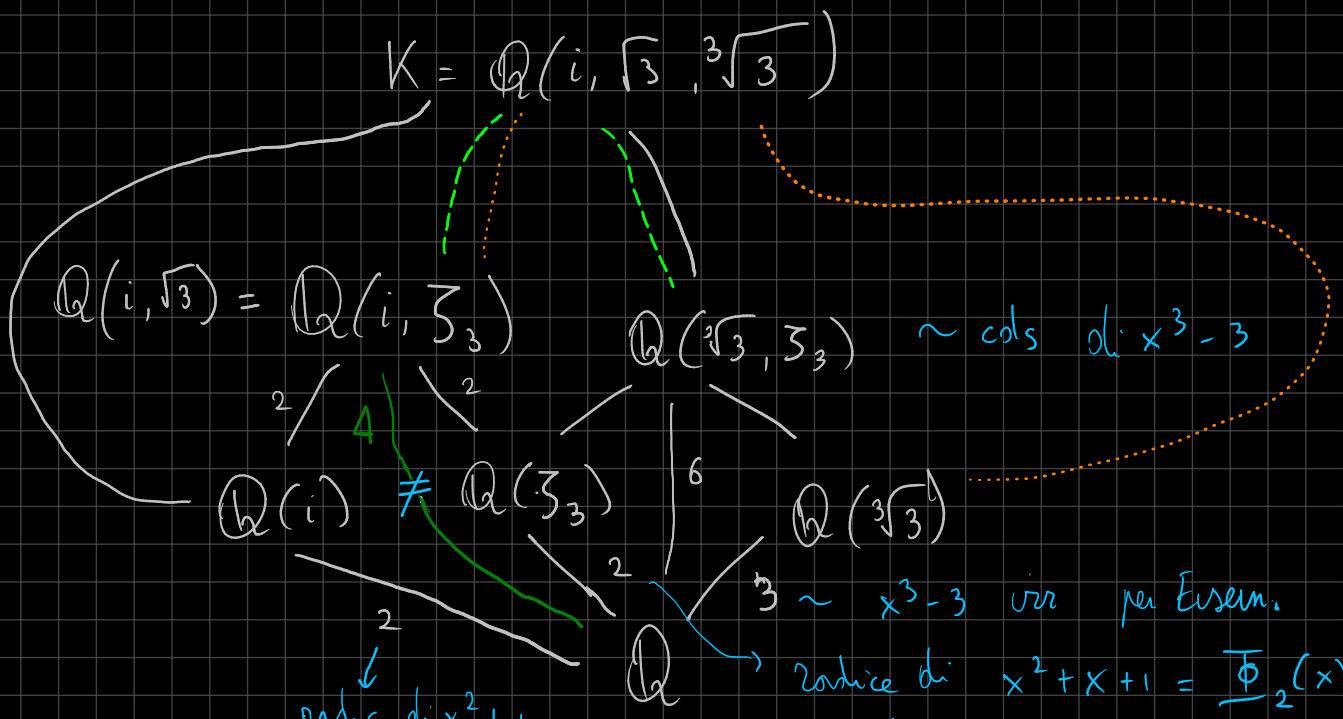
$\Rightarrow K = \mathbb{Q}(\sqrt[3]{3}, \zeta_3)$ dove $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$

$= \mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})$

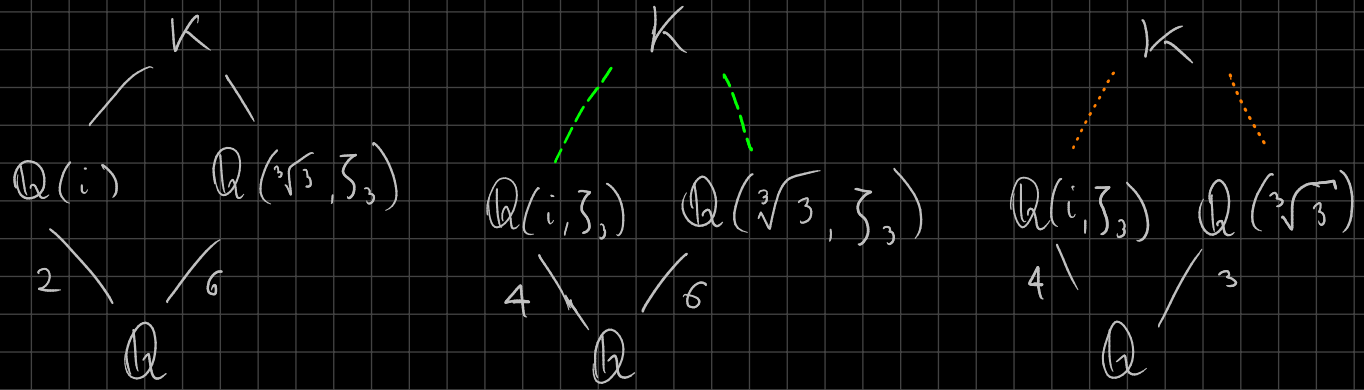
L contiene $i\sqrt{3}$ ma non i oppure $\sqrt{3}$

WRONG

Tentativo 2: K = c.d.s di $(x^3-3)(x^2+1)$



055 Posso dire che K è el compsto di zolo in 3 modi



Dall'ultimo segue che $[K:\mathbb{Q}] = 12$

2) $\mathrm{Gal}(K/\mathbb{Q}) = ?$

Sia $\varphi : K \hookrightarrow \overline{\mathbb{Q}}$ con $\varphi|_{\mathbb{Q}} = id$.

$$\varphi(i) \in \{\pm i\} \qquad \varphi(\sqrt{3}) \in \{\pm\sqrt{3}\} \qquad \varphi(\sqrt[3]{3}) \in \left\{\sqrt[3]{3}, \sqrt[3]{3}\,\zeta_3, \sqrt[3]{3}\,\zeta_3^2\right\}$$

A priori potrebbero esserci delle relazioni algebriche non banali tra questi elementi.

Tuttavia al massimo abbiamo $2 \cdot 2 \cdot 3 = 12$ possibilità e $|\mathrm{Gal}(K/\mathbb{Q})| = 12 \Rightarrow$ tutte le scelte sono realizzate.

Denotando $\varphi_{\pm,\pm,j}$, e.g. $\varphi_{+,-,2} = \begin{cases} i \longmapsto +i \\ \sqrt{3} \longmapsto -\sqrt{3} \\ \sqrt[3]{3} \longmapsto \sqrt[3]{3}\,\zeta_3^2 \end{cases}$

Dato $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$, allora

$$\varphi|_{\mathbb{Q}(\sqrt[3]{3},\zeta_3)} \in \mathrm{Gal}\left(\mathbb{Q}(\sqrt[3]{3},\zeta_3)/\mathbb{Q}\right)$$

perché $F := \mathbb{Q}(\sqrt[3]{3},\zeta_3)$ è c.d.s. di x^3-3

Stessa cosa per $\varphi|_{\mathbb{Q}(i)} \in \mathrm{Gal}\left(\mathbb{Q}(i)/\mathbb{Q}\right)$

Consideriamo allora

$$\Psi : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{Gal}(F/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$$
$$\varphi \longmapsto \left(\varphi|_F\,,\ \varphi|_{\mathbb{Q}(i)}\right)$$

- Ψ è omom. di gruppi
- Ψ è iniettivo: se $\varphi \in \ker\Psi$ allora $\varphi|_F = id$ e $\varphi|_{\mathbb{Q}(i)} = id$, cioè φ fissa tutti i gen. di $K/\mathbb{Q}$, cioè $\varphi = id$

- Ψ è tra insiemi della stessa cardinalità:

$$|Gal(K,\mathbb{Q})| \overset{?}{=} |Gal(F/\mathbb{Q})| \cdot |Gal(\mathbb{Q}(i)/\mathbb{Q})|$$

$$\begin{array}{ccccc} \| & & \checkmark & & \| \\ [K:\mathbb{Q}] & & & & 6 \cdot 2 \\ \| & & & & \| \\ 12 & & = & & 12 \end{array}$$

Dunque Ψ è un isomorfismo

$$\Rightarrow Gal(K/\mathbb{Q}) \simeq Gal(F/\mathbb{Q}) \times Gal(\mathbb{Q}(i)/\mathbb{Q})$$

$$\simeq S_3 \times \mathbb{Z}/2\mathbb{Z}$$

↳ visto a lezione

ALTRO MODO PER VEDERE L'ISOM.

Consideriamo i $\psi_{\pm,\pm,j}$:

- Il primo $\pm$ (che corrisponde a $i \longmapsto \pm i$) è slegato dal resto: la composizione di due ψ ha come "segno su i" semplicemente la comp. dei due segni

$$\rightsquigarrow \mathbb{Z}/2\mathbb{Z}$$

- Stessa cosa per l'azione su $\sqrt{-3}$ (era $\sqrt{3}$, ma scrivendolo $\sqrt{-3}$ così viene meglio)

$$\rightsquigarrow \mathbb{Z}/2\mathbb{Z}$$

- Il fattore $\sqrt[3]{3}$ può andare in $\sqrt[3]{3}, \sqrt[3]{3}\zeta_3, \sqrt[3]{3}\zeta_3^2$

$$\rightsquigarrow \mathbb{Z}/3\mathbb{Z}$$

PROBLEMA Scelto dove mandare $\sqrt{-3}$ modifica la mia scelta per

$$\zeta_3 = \frac{-1+\sqrt{-3}}{2}$$

Per il momento ignoro la scelta di i:

$$\varphi_{\pm,j} = \begin{cases} \sqrt{-3} \longmapsto \pm\sqrt{-3} \\ \sqrt[3]{3} \longmapsto \sqrt[3]{3}\,\zeta_3^j \end{cases}$$

$$\varphi_{\varepsilon_1 j_1} \circ \varphi_{\varepsilon_2 j_2}(\sqrt{-3}) = \varepsilon_1\varepsilon_2\sqrt{-3}$$

$$\varphi_{\varepsilon_1 j_1} \circ \varphi_{\varepsilon_2 j_2}(\sqrt[3]{3}) = \varphi_{\varepsilon_1 j_1}(\sqrt[3]{3}\,\zeta_3^{j_2}) =$$

$$= \varphi_{\varepsilon_1 j_1}(\sqrt[3]{3}) \cdot \varphi_{\varepsilon_1 j_1}(\zeta_3^{j_2})$$

$$= \sqrt[3]{3}\,\zeta_3^{j_1} \cdot \varphi_{\varepsilon_1 j_1}\left(\frac{-1+\sqrt{-3}}{2}\right)^{j_2}$$

FOSS: $\varphi_{+j}(\zeta_3) = \varphi_{+j}\left(\frac{-1+\sqrt{-3}}{2}\right) = \frac{-1+\sqrt{-3}}{2} = \zeta_3$

$\cdot\ \varphi_{-j}(\zeta_3) = \varphi_{-j}\left(\frac{-1+\sqrt{-3}}{2}\right) = \frac{-1-\sqrt{-3}}{2} = \zeta_3^{-1}$

$$= \sqrt[3]{3}\,\zeta_3^{j_1} \cdot \zeta_3^{\varepsilon_1 j_2} = \sqrt[3]{3}\,\zeta_3^{j_1+\varepsilon_1 j_2}$$

$$\rightsquigarrow \quad \varphi_{\varepsilon_1 j_1} \circ \varphi_{\varepsilon_2 j_2} = \varphi_{\varepsilon_1\varepsilon_2,\ j_1+\varepsilon_1 j_2}$$

Legge di composizione di $\mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z} \simeq S_3$.

ULTIMO MODO, SE UNO NON RICORDA CHE $\mathrm{Gal}(F/\mathbb{Q}) \simeq S_3$

$|\mathrm{Gal}(F/\mathbb{Q})| = 6$, inoltre dato che $[F:\mathbb{Q}] = 3$

si ha che $\mathrm{Gal}(F/\mathbb{Q}) \hookrightarrow S_3$

$\Rightarrow \mathrm{Gal}(F/\mathbb{Q}) \simeq S_3$ per card. ∎

GRUPPO DI GAL DELLE EST. CICLOTOMICHE

Sia ζ_n una rad. primitiva n-esima dell'unità, tipo $\zeta_n = \exp\left(\frac{2\pi i}{n}\right) \in \mathbb{C}$.

TESI: $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è normale e il suo Gal è $\mathbb{Z}/n\mathbb{Z}^\times$

1) $\mathbb{Q}(\zeta_n)$ è c.d.s. di $x^n - 1$ → sono tutte le rad. di x^n-1 poiché ζ_n è primitiva

Infatti $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_n^k : k = 0, \dots, n-1)$
ma vale anche il contrario poiché $\zeta_n^k \in \mathbb{Q}(\zeta_n)$ ✓

2) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$

Per tesina di Galois, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \#\,\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

$= \#\{\psi : \mathbb{Q}(\zeta_n) \hookrightarrow \overline{\mathbb{Q}} : \psi|_{\mathbb{Q}} = id\}$

Ogni ψ è determinata da $\psi(\zeta_n)$, inoltre si ha

$$\psi(\zeta_n)^n = \psi(\zeta_n^n) = \psi(1) = 1$$

e quindi $\psi(\zeta_n)$ è una radice dell'unità

$$\Rightarrow \psi(\zeta_n) = \zeta_n^k \quad \text{con } 0 \leq k \leq n-1$$

Voglio mostrare che i k che vanno bene devono essere coprimi con n.
Sia $d := (n,k)$. Si ha che:

$$\psi(\zeta_n^{n/d}) = \psi(\zeta_n)^{\frac{n}{d}} = \zeta_n^{k\frac{n}{d}}$$

$$= \zeta_n^{\left(\frac{k}{d}\right)\cdot n} = 1 = \psi(1)$$

ma ψ è un omom di campi, quindi è iniettivo,

quindi $\zeta_n^{n/d} = 1 \Rightarrow n \mid \frac{n}{d} \Rightarrow d = 1$

ORA: abbiamo mostrato che le uniche possibilità che vanno bene sono ζ_n^k con k coprimo con n, ma non che TUTTE queste possibilità vadano bene! $\Rightarrow |Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})| \leq \phi(n)$

Vogliamo quindi dire che il pol. minimo di ζ_n su $\mathbb{Q}$ ha grado $\phi(n)$.

DETOUR!

3) $x^n - 1 \in K[x]$ è separabile $\iff$ $\text{char } K \nmid n$

[separabile = non ha rad. multiple in una chiusura algebrica]

Test della derivata: separabile $\iff (x^n - 1, nx^{n-1}) = 1$

Se $\text{char } K \mid n$ allora

$$(x^n - 1, \underbrace{nx^{n-1}}_{0}) = (x^n - 1) \neq (1)$$

e quindi $x^n - 1$ non è separabile

Se $\text{char } K \nmid n$ allora

$$(x^n - 1, nx^{n-1}) = (1)$$

in quanto l'unica radice di nx^{n-1} è 0, che non è radice di $x^n - 1$.

[Ora voglio far vedere che ogni $\zeta_n \longmapsto \zeta_n^k$ con $(k, n) = 1$ è un omom. di campi (= automorfismo di $\mathbb{Q}(\zeta_n)$)

Lo faccio facendo vedere che ζ_n e ζ_n^k sono coniugati, cioè hanno lo stesso pol. minimo.

Faccio questa cosa scomponendo k in fattori primi e mostrandolo per i primi, e poi mettendo tutto insieme]

4) Sia f il polinomio minimo di ζ_n su $\mathbb{Q}$.
Sia $p \in \mathbb{Z}$ un primo che non divide n.
Sia g il pol. minimo di ζ_n^p su $\mathbb{Q}$

Osserviamo che $g(x^p)$ si annulla per $x = \zeta_n$

$g(\zeta_n^p) = 0$ poiché g è pol. minimo di ζ_n^p

$\Rightarrow g(x^p)$ è multiplo di $f(x)$ in $\mathbb{Q}[x]$

Inoltre $f(x) \mid x^n - 1$ in $\mathbb{Q}[x]$, dunque per il Lemma di Gauss $f(x) \in \mathbb{Z}[x]$.

Allora $f(x) \mid g(x^p)$ in $\mathbb{Z}[x]$, cioè

$$(*) \quad g(x^p) = f(x)\, h(x)$$

5) Supponiamo per assurdo $g \neq f$. Allora $(f, g) = 1$

f, g sono irriducibili poiché pol. minimi
$\Rightarrow (f \cdot g) \in \{1, f\}$. Ma se fosse f allora $f \mid g$ e g è irriducibile
$\Rightarrow f = g$ ma allora assurdo altrimenti
$\Rightarrow (f \cdot g) = 1$

ed entrambi dividono $x^n - 1$ ← le loro radici sono ζ_n che ζ_n^p

Siccome $(f, g) = 1$ segue che $f \cdot g \mid x^n - 1$ in $\mathbb{Z}[x]$

Scriviamo $x^n - 1 = f \cdot g \cdot \ell$ in $\mathbb{Z}[x]$.

Riduciamo mod p

$$(**) \quad x^n - 1 = \overline{f} \cdot \overline{g} \cdot \overline{\ell}$$

D'altra parte $(*) \Rightarrow \overline{f} \cdot \overline{h} = \overline{g(x^p)} = \overline{g(x)}^p$

e quindi ogni radice di $\overline{f}$ in $\overline{\mathbb{F}_p}$ è radice di $\overline{g}$

Sia $\alpha \in \overline{\mathbb{F}_p}$ una radice di $\overline{f}$ (e quindi di $\overline{g}$)

Allora in (**) il fattore destro ha la radice α di molt. almeno 2 (una volta come rad. di $\overline{f}$, una come radice di $\overline{g}$)

$\Rightarrow x^n - 1$ ha una radice doppia in $\overline{\mathbb{F}_p}$

Ma ciò è assurdo: abbiamo detto che ciò accade se e solo se $p \nmid n$.

Segue quindi che l'ipotesi di assurdo è falsa, cioè $f = g$, cioè ζ_n e ζ_n^r hanno lo stesso polinomio minimo.

6) Deduciamo che ζ_n e ζ_n^k con $(k,n) = 1$ hanno lo stesso pol. minimo.

Scrivo $k = p_1 p_2 \cdots p_r$ dove ogni primo può comparire più volte e ogni $p_i \nmid n$.

Allora ζ_n e $\zeta_n^{p_1}$ hanno lo stesso polinomio minimo

↳ è ancora una rad. prim. n-esima dell'unità

$\Rightarrow \zeta_n^{p_1}$ e $\zeta_n^{p_1 p_2}$ hanno lo stesso pol. minimo

$\Rightarrow \cdots$

$\Rightarrow \zeta_n^{p_1 \cdots p_{r-1}}$ e $\zeta_n^{p_1 \cdots p_r} = \zeta_n^k$ hanno lo stesso pol. minimo

$\Rightarrow \zeta_n$ e ζ_n^k hanno lo stesso pol minimo!

7) Il pol di ζ_n ha quindi tra le sue radici ζ_n^k $\forall k$ coprimo con n

Queste sono tutte distinte

$\Rightarrow \deg f(x) \geq \phi(n) = \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$

$[\mathbb{Q}(\zeta_n)/\mathbb{Q}] \leq \phi(n)$ $\qquad \Rightarrow \deg f = \phi(n)$

e in particolare

$$f(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n-1} (x - \zeta_n^k) \qquad (\text{in } \overline{\mathbb{Q}}[x])$$

8) $F : Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathbb{Z}/n\mathbb{Z}^\times$

$$(\psi : \zeta_n \longmapsto \zeta_n^k) \longmapsto k$$

Questa applicazione è iniettiva e i due insiemi hanno la stessa cardinalità, dunque è biiettiva.

Inoltre $\psi_{k_1} \circ \psi_{k_2}(\zeta_n) = \psi_{k_1}(\zeta_n^{k_2}) = \psi_{k_1}(\zeta_n)^{k_2}$

$$= \zeta_n^{k_1 k_2}$$

$$\Rightarrow \psi_{k_1} \circ \psi_{k_2} = \psi_{k_1 k_2}$$

$$\Rightarrow F(\psi_{k_1} \circ \psi_{k_2}) = F(\psi_{k_1 k_2}) = k_1 k_2 = F(\psi_{k_1}) \cdot F(\psi_{k_2})$$

∎

COROLLARIO Sia Φ_n pol. min di una radice n-esima prim. di 1. Si ha

$$x^n - 1 = \prod_{d \mid n} \Phi_d(n)$$

DIM 1) Sono entr. polinomi monici

2) Ogni radice di $\prod_{d \mid n} \Phi_d(n)$ è radice di $x^n - 1$

3) Viceversa ogni radice di $x^n - 1$ è ζ_n^i avrà ordine $\frac{n}{(n,i)} = d$ e quindi è radice di Φ_d ∎

COROLLARIO 2 Prendendo i gradi si ha che

$$n = \sum_{d \mid n} \phi(n)$$

∎