Caratterizzazione sottoestensioni di grado 2 su $\mathbb{Q}$ di estensioni ciclotomiche p-esime

Alberto Landi

13 aprile 2021

Sommario

Presentiamo una dimostrazione alternativa a quella presente in [1, p. 569] della caratterizzazione delle sottoestensioni di grado 2 su $\mathbb{Q}$ di estensioni ciclotomiche di ordine un primo. Momentaneamente, manca l'introduzione in cui enunciamo le definizioni e i teoremi utilizzati nel seguito. In ogni caso, le nozioni necessarie per la comprensione dello scritto sono argomento di ordinari corsi di algebra, e sono trattate sempre in [1]. Per qualsiasi eventuale errore riscontrato nello scritto, o per qualunque dubbio in merito al contenuto, si prega di scrivere a: *a.landi24@studenti.unipi.it.*

Indice

1 Introduzione

Definizione 1.1. *Definiamo estensione di Galois...*

2 Il Teorema

Ci accingiamo ora a enunciare e dimostrare il seguente

Teorema 2.1 (Caratterizzazione sottoestensioni di grado 2 su $\mathbb{Q}$ di estensioni ciclotomiche p-esime)**.** *Sia $p \in \mathbb{P}$ dispari e consideriamo l'estensione di campi $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Allora $\exists!$ sottoestensione di grado 2 su $\mathbb{Q}$, e essa è*

$$\mathbb{Q}\big(\sqrt{\gamma_p \cdot p}\big)/\mathbb{Q}$$

dove $\gamma_p = (-1)^{\frac{p-1}{2}}$

Ricordando che il gruppo di Galois $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ è ciclico $\forall p \in \mathbb{P}$, sappiamo che esiste un unico sottogruppo di indice 2 di $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Dal Teorema di Corrispondenza di Galois segue dunque il seguente

Lemma 2.1. *Sia $p \in \mathbb{P}$ e consideriamo l'estensione di campi $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Allora tale estensione ha un'unica sottoestensione $\mathbb{Q}(\alpha_p)/\mathbb{Q}$ di grado 2 su $\mathbb{Q}$*

Dal lemma 2.1 segue dunque la prima parte del teorema 2.1.

Per dimostrare la seconda parte, quella meno ovvia, procederemo a step. Innanzitutto, fissiamo la notazione.

Notazione. *Denotiamo con $\phi \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ il generatore di $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$,mentre denotiamo con $\psi \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ un generatore dell'unico sottogruppo del gruppo di Galois di indice 2 (ovvero ψ ha ordine $\frac{p-1}{2}$). Denoteremo con $\alpha \in \mathbb{C}$ il numero $\alpha = \sum_{i \in I} \zeta_p^i$ dove I è tale che $i \in I \iff \zeta_p^i \in Orb_\psi(\zeta_p)$, ovvero*

$$\alpha = \zeta_p + \psi(\zeta_p) + \ldots + \psi^{-1}(\zeta_p)$$

Inoltre, denotiamo con $\mu_\alpha(x) \in \mathbb{Q}[x]$ il polinomio minimo di α su $\mathbb{Q}$. Infine, denotiamo con α' l'associato di α, ovvero l'altra radice di $\mu_\alpha(x)$.

Osserviamo allora che

Osservazione 2.1. *Essendo $\mu_{\zeta_p}(x) = 1 + \zeta_p + \ldots + \zeta_p^{p-1}$ il polinomio minimo di ζ_p su $\mathbb{Q}$, necessariamente $\alpha \notin \mathbb{Q}$. Inoltre, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2$, in quanto α è fissato da ψ, da cui la disuguaglianza segue per il Teorema di Corrispondenza di Galois. Abbiamo allora che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, da cui $\mathbb{Q}(\alpha)/\mathbb{Q}$ è, per unicità, la sottoestensione di grado 2 cercata.*

Il problema si è ridotto a dimostrare che $\alpha \in \mathbb{Q}(\sqrt{\gamma_p \cdot p})$. É sufficiente allora mostrare che il determinante di $\mu_\alpha(x)$ sia

$$\Delta = \gamma_p \cdot p$$

che è ciò che faremo. Dato che ζ_p è un intero algebrico e gli interi algebrici formano un anello, poniamo d'ora in poi $\mu_\alpha(x) = x^2 + ax + b$ con $a \in \mathbb{Z}, b \in \mathbb{Z}$, e mostriamo il seguente

Lemma 2.2. *Con la notazione introdotta, abbiamo che*

$$a = 1$$

ovvero

$$\alpha' = -1 - \alpha$$

Dimostrazione. Da quanto abbiamo detto, sappiamo che $\psi(\alpha) = \alpha$ da cui $\psi(\alpha') = \alpha'$, in quanto $\psi(\alpha')$ deve essere radice di μ_α e ψ è iniettiva. Sappiamo che $\phi(\zeta_p) = \zeta_p^t$ per un certo $t \in \{1, ..., p-1\}$ e che $\phi^2 \in < \psi >$, da cui $\mu_{\zeta_p}(x) = (x - \alpha)(x - \phi(\alpha))$ e $\alpha' = \phi(\alpha)$. Segue allora che

$$\alpha' = \sum_{i=1}^{\frac{p-1}{2}} \zeta_p^{j_i}$$

dove j_i non compare nella scrittura di α come somma di potenze di ζ_p. Sommando α e α' otteniamo allora

$$-a = \alpha + \alpha' = \sum_{i=1}^{p-1} \zeta_p^i = -1$$

che è la tesi. □

Passiamo adesso a studiare il determinante di μ_α, lavorando separatamente sul suo segno e sul suo valore assoluto. Per il segno, vogliamo mostrare che

Lemma 2.3.

$$\gamma_p = \frac{\Delta}{|\Delta|} = \begin{cases} 1 & p \equiv 1 (mod\ 4) \\ -1 & p \equiv 3 (mod\ 4) \end{cases}$$

Dimostrazione. Denotiamo con f il coniugio complesso, ovvero $\forall x \in \mathbb{C}$ vale $f(x) = \bar{x}$, dove con $\bar{x}$ indichiamo il coniugato di x. Notiamo che, essendo $(p-1)/2$ pari e $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}$ ciclico, l'unico elemento di ordine 2 di tale gruppo di Galois è la restrizione del coniugio complesso a $\mathbb{Q}(\zeta_p)$, in quanto tale applicazione è chiaramente un'immersione di $\mathbb{Q}(\zeta_p)$ in $\mathbb{C}$ che fissa $\mathbb{Q}$. Consideriamo adesso il caso $p \equiv 1 (\text{mod } 4)$. Abbiamo allora che $2 \mid \frac{p-1}{2} = \#Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\alpha))$, da cui, per il Teorema di Corrispondenza di Galois, si ha che $f_{|\mathbb{Q}(\zeta_p)} \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\alpha))$. Segue dunque che α è fissato dal coniugio complesso, ovvero $f(\alpha) = \alpha$, da cui

$$\alpha \in \mathbb{R} \implies \Delta \in \mathbb{R} \implies \gamma_p = 1$$

come voluto. Analogamente, nel caso $p \equiv 3 (\text{mod } 4)$ si ha che $2 \nmid \frac{p-1}{2} = \#Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\alpha))$, da cui $f_{|\mathbb{Q}(\zeta_p)} \notin Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\alpha))$ da cui si ha che $f(\alpha) \neq \alpha$ (più precisamente $f(\alpha) = \alpha'$). Dunque:

$$\alpha \notin \mathbb{R} \implies \Delta \notin \mathbb{R} \implies \gamma_p = -1$$

che è la tesi. □

Occupiamoci ora del modulo del determinante. Vorremmo dimostrare che $|\Delta| = p$. Per farlo, mostriamo che $|\Delta| < p^2$, successivamente che $p \mid \Delta$, e infine che, se supponiamo vera la tesi del teorema 2.1 per ogni $q \in \mathbb{P}$ dispari tale che $q < p$, allora $q \nmid \Delta\ \forall q \in \mathbb{P}\ t.c.\ q < p$. Fatto ciò, potremo concludere per induzione. Dimostriamo allora il seguente

Lemma 2.4. *Vale la seguente disuguaglianza*

$$|\Delta| < p^2$$

Dimostrazione. Dividiamo la dimostrazione in due parti, a seconda della congruenza di p modulo 4. Dato $x \in \mathbb{C}$, denoteremo con $\Re(x)$ la sua parte reale e con $\Im(x)$ la sua parte immaginaria. Sia allora $p \equiv 1 (\text{mod } 4)$. Essendo $\alpha \in \mathbb{R}$ e $\alpha = \sum_{i=1}^{\frac{p-1}{2}} \zeta_p^{j_i}$, si ha che

$$\frac{-1+\sqrt{\Delta}}{2} = \alpha = \Re(\alpha) = \sum_{i=1}^{\frac{p-1}{2}} \Re(\zeta_p^{j_i}) < \sum_{i=1}^{\frac{p-1}{2}} 1 = \frac{p-1}{2}$$

dove abbiamo usato il lemma 2.2 e la formula di risoluzione di equazioni di secondo grado. Segue immediatamente quanto voluto. Analogamente, nel caso in cui $p \equiv 3 (\text{mod } 4)$, si ottiene

$$\frac{\sqrt{\Delta}}{2} = \Im(\alpha) = \sum_{i=1}^{\frac{p-1}{2}} \Im(\zeta_p^{j_i}) \leq \sum_{i=1}^{\frac{p-1}{2}} 1 = \frac{p-1}{2} < \frac{p}{2}$$

da cui la tesi. □

Per dimostrare che $p \mid \Delta$, è naturale ragionare modulo p, ovvero lavorare sul campo $\mathbb{F}_p$. Dato che $x^p - 1 = (x-1)^p$ in $\mathbb{F}_p$, tale polinomio è completamente riducibile e tutte le sue radici coincidono, da cui ci aspettiamo che anche "le radici corrispondenti" ad α e α' coincidano. Ciò equivale a dire che, in $\mathbb{F}_p$, $\alpha = \alpha'$, ovvero $\frac{-1+\sqrt{\Delta}}{2} \equiv \frac{-1-\sqrt{\Delta}}{2} (\text{mod } p)$, ovvero $p \mid \Delta$. Chiaramente dobbiamo mostrare anche che la scrittura $\sqrt{\Delta}$ ha senso in $\mathbb{F}_p$, ovvero che Δ è un quadrato modulo p.

Lemma 2.5. *Abbiamo che $p \mid \Delta$.*

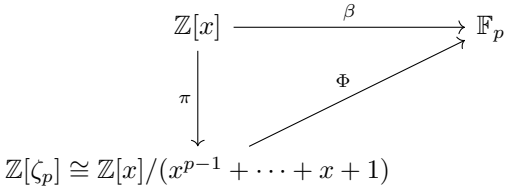
Dimostrazione. Il seguente è un omomorfismo suriettivo di anelli

$$\begin{aligned} \Phi : \mathbb{Z}[\zeta_p] &\longrightarrow \mathbb{F}_p \\ \mathbb{Z} &\longrightarrow \mathbb{Z}/(p) \\ \zeta_p &\longrightarrow \bar{1} \end{aligned}$$

dove intendiamo che $\Phi_{|\mathbb{Z}}$ è la proiezione canonica al quoziente modulo p. Notiamo che la suriettività è ovvia, mentre il fatto che tale applicazione sia un omomorfismo discende dal Primo Teorema di Omomorfismo. Infatti, detto β la composizione della proiezione canonica π al quoziente modulo p e dell'omomorfismo f di valutazione in 1 definiti come segue

$$\begin{aligned} \beta : \mathbb{Z}[x] &\xrightarrow{\pi} \mathbb{F}_p[x] \xrightarrow{f} \mathbb{F}_p \\ \mathbb{Z} &\longrightarrow \mathbb{Z}/(p) \longrightarrow \mathbb{Z}/(p) \\ x &\longrightarrow x \longrightarrow \bar{1} \end{aligned}$$

si ha che $\beta(x^{p-1} + \cdots + x + 1) = p \equiv 0 (\text{mod } p)$, da cui $(x^{p-1} + \cdots + x + 1) \subset Ker(\Phi)$. Segue dal Primo Teorema di Omomorfismo che $\exists! \Phi$ (usiamo lo stesso nome perché mostreremo tra poco essere proprio l'omomorfismo cercato) che completa il diagramma



Esso è suriettivo, essendo β suriettiva, e $\Phi(\zeta_p) = \Phi(\pi(x)) = \beta(x) = 1$ come voluto. Segue che $\Phi(\alpha) = (p-1)/2 = \Phi(\alpha')$, da cui, essendo Φ un omomorfismo,

$$\begin{aligned} 0 = \Phi(\mu_\alpha(\alpha)) = \mu_\alpha(\frac{p-1}{2}) = (\frac{p-1}{2})^2 + \frac{p-1}{2} + b \equiv 0 (\text{mod } p) \\ \implies \Delta = 4b - 1 \equiv 0 (\text{mod } p) \end{aligned}$$

che è la tesi. □

Dal lemma 2.5, si ha allora che $\exists m \in \mathbb{Z}$ *t.c.* $\Delta = m \cdot p$. Sia ora $q \in \mathbb{P}$ dispari tale che $q \mid m$. Dal lemma 2.4 si ha che necessariamente $q < p$, da cui possiamo ragionare per induzione. Passiamo dunque alla dimostrazione del teorema 2.1.

Dimostrazione (Caratterizzazione sottoestensioni di grado 2 su $\mathbb{Q}$ di estensioni ciclotomiche p-esime)**.** *Dopo aver fissato la numerazione dei numeri primi dispari, $\mathbb{P}^*$, data dall'ordinamento naturale degli interi, ovvero $\mathbb{P}^* = \{p_1 = 3, p_2 = 5 \dots\}$, ragioniamo per induzione sul pedice al variare di $n \in \mathbb{N}$. Il passo base con $p = 3$ è una banale verifica, da cui passiamo direttamente a dimostrare il passo induttivo. Per evitare di appesantire eccessivamente la notazione fissiamo $3 < p \in \mathbb{P}$ e supponiamo la tesi vera $\forall q \in \mathbb{P}$, con $q < p$. Come già detto, dai lemmi 2.5 e 2.4 si ha che $\Delta = \gamma_p \cdot m \cdot p$ con $m < p$. Osserviamo che ai fini della dimostrazione possiamo supporre Δ square free. Sia ora,per assurdo, $q \in \mathbb{P}$ dispari e minore di p tale che $q \mid m$. Per ipotesi induttiva, l'unica sottoestensione di $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ di grado 2 su $\mathbb{Q}$ è $\mathbb{Q}(\sqrt{\gamma_q \cdot q})/\mathbb{Q}$. Consideriamo allora $\mathbb{Q}(\zeta_p, \zeta_q)$ che possiamo mostrare essere uguale a $\mathbb{Q}(\zeta_{pq})$, che ha gruppo di Galois*

$$Gal(\mathbb{Q}(\zeta_{pq})/\mathbb{Q}) \cong Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$$

Sia $G_p = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, $G_q = Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, e $G_{pq} = Gal(\mathbb{Q}(\zeta_{pq})/\mathbb{Q})$. Indichiamo allora gli elementi del gruppo di G_pq visti nel prodotto diretto $G_{pq} \cong G_p \times G_q$. In particolare, siano (ϕ, Id_q) e (ψ, Id_q) rispettivamente il generatore di $G_p \times \{Id_q\}$ e il generatore di $H \times \{Id_q\}$, con $H \subset G_p$ tale che $\mathbb{Q}^H = \mathbb{Q}(\alpha)$. Analogamente, siano $(Id_p, \bar{\phi})$ e $(Id_p, \bar{\psi})$ rispettivamente il generatore di $\{Id_p\} \times G_q$ e il generatore di $\{Id_p\} \times K$, con $K \subset G_q$ tale che $\mathbb{Q}^K = \mathbb{Q}(\alpha)$. Allora, posto $m' = m/q$,

$$(Id_p, \bar{\phi})\big(\sqrt{\gamma_p \cdot pm}\big) = \sqrt{\gamma_p \cdot pm} \implies (Id_p, \bar{\phi})\big(\sqrt{\gamma_p\gamma_q \cdot pm'}\big) = -\sqrt{\gamma_p\gamma_q \cdot pm'}$$

in quanto $(Id_p, \bar{\phi})(\sqrt{\gamma_q \cdot q}) = -\sqrt{\gamma_q \cdot q}$ per ipotesi induttiva. Supponiamo che $m = q$. Allora quanto scritto sopra diventa

$$(Id_p, \bar{\phi})\big(\sqrt{\gamma_p\gamma_q \cdot p}\big) = -\sqrt{\gamma_p\gamma_q \cdot p} \tag{1}$$

Notiamo che possiamo ridurci sempre a questo caso. Infatti, se $m = q_1 \cdots q_n \cdot q$ con q_i primi dispari distinti, allora possiamo considerare l'estensione $\mathbb{Q}(\zeta_{pm})/\mathbb{Q}$ e l'elemento $(Id_p, Id_{q_1} \dots, Id_{q_n}, \bar{\phi})$ del gruppo di Galois corrispondente, visto come prodotto diretto dei vari gruppi di Galois dati dalle singole radici dell'unità (coinvolte), che agisce in modo banale su $\sqrt{m'}$, come è facilmente dimostrabile (per induzione) considerando le estensioni $\mathbb{Q}(\zeta_q, \zeta_{q_i})$, al variare di i. Torniamo adesso al caso $m = q$ e mostriamo che l'equazione 1 è impossibile. Infatti, possiamo considerare l'estensione $\mathbb{Q}(\zeta_q, \sqrt{\gamma_p\gamma_q \cdot p})/\mathbb{Q}$ e il relativo gruppo di Galois, che è isomorfo al prodotto diretto dei gruppi di Galois corrispondenti alle estensioni $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ e $\mathbb{Q}(\sqrt{\gamma_p\gamma_q \cdot p})/\mathbb{Q}$, essendo estensioni di Galois con intersezione vuota. Allora otteniamo che $(Id, \bar{\phi})(\sqrt{\gamma_p\gamma_q \cdot p}) = \sqrt{\gamma_p\gamma_q \cdot p}$, che contrasta con la 1, considerando la naturale inclusione di $\mathbb{Q}(\zeta_q, \sqrt{\gamma_p\gamma_q \cdot p})$ in $\mathbb{Q}(\zeta_p, \zeta_q)$. Segue che è impossibile che $\exists q \in \mathbb{P}^*$ minore di p tale che $q|m$, da cui $m = 1$. Segue che $\Delta = \gamma_p \cdot p$, che è la tesi.

Riferimenti bibliografici

[1] Artin, Michael (1991) *Algebra*, Prentice Hall, New Jersey.