Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

LA CORRISPONDENZA DI GALOIS PER POLINOMI DI TERZO E QUARTO GRADO

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
Monica Idà

Presentata da:
Mirea Di Tonno

I Sessione
Anno Accademico 2013/2014

Alla mia famiglia.

Indice

Introduzione

Questa tesi nasce dal desiderio di comprendere meglio la corrispondenza di Galois tramite un certo numero di esempi studiati nel modo più approfondito possibile.
In ognuno degli esempi si parte sempre dal gruppo di Galois di un polinomio f a coefficienti razionali; si determina il campo di spezzamento E di f come sottocampo di $\mathbb{C}$, e si studiano poi tutte le estensioni intermedie dell'estensione di campi $E/\mathbb{Q}$ mettendole in relazione con i sottogruppi del gruppo di Galois dell'estensione G.
Se $f \in \mathbb{Q}[x]$ ha grado 2 ed è irriducibile su $\mathbb{Q}$, non c'è molto da dire; se α_1 e α_2 sono le sue radici complesse, allora $E = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$, $[E : \mathbb{Q}] = 2$ e quindi $|G| = 2$, quindi $G \cong \mathbb{Z}_2$ ha solo due elementi, l'identità e l'automorfismo

$$\begin{aligned} E &\longrightarrow E \\ a + b\alpha_1 &\longmapsto a + b\alpha_2 \qquad\qquad \forall a, b \in \mathbb{Q} \end{aligned}$$

e non ci sono ovviamente sottogruppi propri.
D'altra parte non appena il grado di f cresce anche di poco, i calcoli necessari a capire chi è G e a comprendere appieno la corrispondenza di Galois possono diventare molto complicati.
In questa tesi ci siamo interessati a polinomi di grado 3 e di grado 4.
In alcuni degli esempi studiati le radici del polinomio non si calcolano con metodi elementari; poichè, come è ben noto, le equazioni algebriche di terzo e quarto grado sono sempre risolubili per radicali, mentre ciò è in generale falso per il grado ≥ 5; abbiamo quindi studiato le formule risolutive generali per polinomi di terzo e quarto grado (Capitolo terzo).
Nel capitolo 1 richiamiamo il teorema fondamentale sulla corrispondenza di Galois e alcuni altri utili teoremi, e stabiliamo le notazioni.
Nel capitolo 2 introduciamo e studiamo il discriminante di un polinomio di grado qualsiasi e i suoi legami con il gruppo di Galois del polinomio.
Nel quarto capitolo diamo due esempi di polinomi di terzo grado irriducibili su $\mathbb{Q}$, uno con tre radici reali e l'altro no, che esauriscono in effetti tutti i casi possibili.
Nel quinto capitolo studiamo in dettaglio due esempi di polinomi di quarto grado, uno irriducibile su $\mathbb{Q}$ e l'altro riducibile.

Capitolo 1

Richiami e notazioni

In questa tesi diamo per nota la Teoria di Galois e tutte le nozioni di Algebra necessarie a comprenderla; si può far riferimento, ad esempio, a [3, Garling], o a [7, Cohn].
Nel seguito stabiliamo le notazioni che useremo nei prossimi capitoli e ricordiamo solo alcuni punti fondamentali della Teoria che verranno utilizzati in seguito.
Sia E/K una estensione di campi; tutte le estensioni che consideriamo sono finite, e $[E : K] := dim_K E$ denota il grado dell'estensione.
Se E/K è un'estensione di Galois, denotiamo con G il suo gruppo di Galois:
$G = Gal(E/K) = \{\sigma \in AutE, \sigma(x) = x \, \forall x \in K\}$.
Sia ora K un campo di caratteristica 0, $f \in K[x]$ sia un polinomio e sia E il campo di spezzamento di f su K.
Se f è irriducibile, oppure è riducibile senza radici multiple, allora E/K è normale e separabile, pertanto è un'estensione di Galois; chiameremo $Gal(E/K)$ *il gruppo di Galois di* f *su* K; e lo denoteremo anche con $Gal(f)$.

Teorema 1.1.
Sia E/K un'estensione di Galois e sia $G = Gal(E/K)$. Valgono i fatti seguenti:

1. *C'è una corrispondenza biunivoca ϕ che rovescia le inclusioni:*

$$\{F|K \subseteq F \subseteq E \quad \textit{torre di sottocampi}\} \xrightarrow{\phi} \{H|H \quad \textit{sottogruppo di Galois}\}$$
$$F \longmapsto F^* := \{g \in G | g(x) = x \, \forall x \in F\}$$

con inversa

$$\{x \in E | h(x) = x \, \forall h \in H\} = H^* \xleftarrow{\phi^{-1}} H$$

Si ha: $|H| = [E : H^*]$, $(G : H) = [H^* : K]$
In particolare $G^* = K$ *e* $E^* = 1$ *e* $|G| = [E : K]$

2. *Siano H, T sottogruppi di G; allora H e T sono sottogruppi coniugati tramite una $\sigma \in G : H = \sigma T \sigma^{-}1$ se e solo se H^* e T^* sono sottocampi coniugati tramite σ, cioè $H^* = \sigma(T^*)$.*
Ne segue: $H \lhd G \Leftrightarrow H^*/K$ è un'estesione normale e in questo caso $Gal(H^*/K) \cong G/H$.

In questa tesi utilizzeremo questo teorema per $K = \mathbb{Q}$ ed $E \subset \mathbb{C}$ campo di spezzamento di un polinomio f su K.

Teorema 1.2.
Sia $f \in K[x]$ un polinomio separabile di grado n, E un campo di spezzamento di f su K e sia $R = \{\alpha_1, ..., \alpha_n\}$ l'insieme delle radici di f. Allora se $\sigma \in Gal(f), \forall\, \alpha_i \in R$ si ha $\sigma(\alpha_i) \in R$, quindi se $S(\alpha_1, ..., \alpha_n)$ denota il gruppo simmetrico sull'insieme delle radici, si ha una mappa

$$\begin{aligned} \psi : Gal(f) &\longrightarrow S(\alpha_1, ..., \alpha_n) \\ \sigma &\longmapsto \begin{pmatrix} \alpha_1 & .... & \alpha_n \\ \sigma(\alpha_1) & .... & \sigma(\alpha_n) \end{pmatrix} \end{aligned}$$

La mappa ψ è un morfismo iniettivo di gruppi.
(Si veda ad es. [Garling] Th. 11.6)

Proposizione 1.3.
Nelle ipotesi del teorema precedente, se f è irriducibile, $Gal(f)$ agisce transitivamente su $\{\alpha_1, ..., \alpha_n\}$, cioè per ogni $\alpha_i, \alpha_j \in \{\alpha_1, ..., \alpha_n\}$, esiste $\sigma \in Gal(f)$ tale che $\sigma(\alpha_i) = \alpha_j$.
(Si veda ad es. [Garling] Cor 2a Th. 7.5)

Notazione
Nel seguito se $f \in K[x]$ è un polinomio separabile di grado n con radici $\alpha_1, ...\alpha_n$ nel campo di spezzamento E, identificheremo il gruppo simmetrico S_n delle permutazioni su $\{1, ..., n\}$ con il gruppo simmetrico $S(\alpha_1, ..., \alpha_n)$ delle permutazioni su $\{\alpha_1, ..., \alpha_n\}$, per cui a volte scriveremo ad esempio $(1\,2)$ per denotare la permutazione $(\alpha_1\, \alpha_2)$.
Inoltre $Gal(f)$ verrà identificato con la sua immagine nel morfismo iniettivo ψ, quindi verrà considerato come sottogruppo di S_n; per cui $(1\,2)$ o $(\alpha_1\, \alpha_2)$ può denotare, nel seguito, l'automorfismo σ di E che scambia le radici α_1 e α_2 e lascia fisse tutte le altre, modulo l'essere certi che un tale automorfismo esista.

Capitolo 2

Il discriminante

Nel seguito K denota sempre un campo.

Definizione 2.1.
Sia $f \in K[x]$ con $carK \neq 2$, siano $\alpha_1, \alpha_2, ..., \alpha_n$ radici di f nel campo di spezzamento L, poniamo

$$\delta = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$$

Se f ha radici multiple $\delta = 0$, contrariamente nel caso in cui f è un polinomio separabile $\delta \neq 0$.
La quantità $\Delta = \delta^2$ è chiamata **discriminante** di f.

$$\Delta = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2$$

Osservazione 1.
É bene notare che δ dipende dall'ordine delle radici, mentre Δ no.

In pratica non è difficile calcolare il discriminante. Dalla proposizione 2.1 segue che la quantità δ è data dal determinante di Vandermonde:

$$\delta = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i) = \begin{vmatrix} 1 & 1 & ... & 1 \\ \alpha_1 & \alpha_2 & ... & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & ... & \alpha_n^{n-1} \end{vmatrix}$$

Proposizione 2.1.
Siano $\alpha_1, ..., \alpha_n \in K$ con $carK \neq 2$ e sia V la matrice di Vandermonde quadrata di ordine n così definita:

$$V = \begin{pmatrix} 1 & 1 & ... & 1 \\ \alpha_1 & \alpha_2 & ... & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & ... & \alpha_n^{n-1} \end{pmatrix}$$

Allora si ha:

$$det(V) = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)$$

Dimostrazione
Se $\alpha_{i_0} = \alpha_{j_0}$ per una coppia i_0, j_0 allora $detV = 0$ e

$$\prod_{1 \le i < j \le n} (\alpha_j - \alpha_i) = 0$$

quindi la proposizione è vera; possiamo quindi supporre $\alpha_i \neq \alpha_j$ se $i \neq j$. Procediamo per induzione su n.
Per $n = 2$ si ha:

$$det(V) = \begin{vmatrix} 1 & 1 \\ \alpha_1 & \alpha_2 \end{vmatrix} = (\alpha_2 - \alpha_1) = \prod_{1 \le i < j \le 2} (\alpha_j - \alpha_i)$$

Quindi l'enunciato è verificato per $n = 2$, supponiamo che sia vero per $n-1$ e proviamolo per n.
Il determinante può essere calcolato sottraendo ad ogni riga la riga precedente moltiplicata per α_1

$$det(V) = \begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ 0 & \alpha_2 - \alpha_1 & \alpha_3 - \alpha_1 & ... & \alpha_n - \alpha_1 \\ 0 & \alpha_2(\alpha_2 - \alpha_1) & \alpha_3(\alpha_3 - \alpha_1) & ... & \alpha_n(\alpha_n - \alpha_1) \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & \alpha_2^{n-2}(\alpha_2 - \alpha_1) & \alpha_3^{n-2}(\alpha_3 - \alpha_1) & ... & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{vmatrix}$$

dividendo, poi, ogni colonna j-esima(tranne la prima) per il termine $\alpha_j - \alpha_1 \neq 0$ che viene portato fuori dalla matrice si ha:

$$det(V) = \begin{vmatrix} 1 & (\alpha_2 - \alpha_1)^{-1} & (\alpha_3 - \alpha_1)^{-1} & ... & (\alpha_n - \alpha_1)^{-1} \\ 0 & 1 & 1 & ... & 1 \\ 0 & \alpha_2 & \alpha_3 & ... & \alpha_n \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & \alpha_2^{n-2} & \alpha_3^{n-2} & ... & \alpha_n^{n-2} \end{vmatrix} \cdot \prod_{j=2}^{n} (\alpha_j - \alpha_1) =$$

$$= \begin{vmatrix} 1 & 1 & ... & 1 \\ \alpha_2 & \alpha_3 & ... & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_2^{n-2} & \alpha_3^{n-2} & ... & \alpha_n^{n-2} \end{vmatrix} \cdot \prod_{j=2}^{n} (\alpha_j - \alpha_1)$$

Infine applicando l'ipotesi induttiva per la matrice di ordine $n-1$ si ottiene:

$$det(V) = (\prod_{2 \le i < j \le n} (\alpha_j - \alpha_i))(\prod_{1 = i < j \le n}^{n} (\alpha_j - \alpha_i)) = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i) \qquad \square$$

Proposizione 2.2. *Nelle notazioni di definizione 2.1 si ha:*

$$\Delta = \prod_{1\leq i<j\leq n} (\alpha_j - \alpha_i)^2 = det \begin{pmatrix} n & \lambda_1 & ... & \lambda_{n-1} \\ \lambda_1 & \lambda_2 & ... & \lambda_n \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n-1} & \lambda_n & ... & \lambda_{2n-2} \end{pmatrix}$$

dove $\lambda_j = \alpha_1^j + ... + \alpha_n^j$.

Dimostrazione
Dall'osservazione 1 abbiamo visto che

$$\delta = \begin{vmatrix} 1 & 1 & ... & 1 \\ \alpha_1 & \alpha_2 & ... & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & ... & \alpha_n^{n-1} \end{vmatrix}.$$

Sia $A = \begin{pmatrix} 1 & 1 & ... & 1 \\ \alpha_1 & \alpha_2 & ... & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & ... & \alpha_n^{n-1} \end{pmatrix}$
Se moltiplichiamo tale matrice per la sua trasposta otteniamo:

$$A \cdot A^t = \begin{pmatrix} n & \lambda_1 & ... & \lambda_{n-1} \\ \lambda_1 & \lambda_2 & ... & \lambda_n \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n-1} & \lambda_n & ... & \lambda_{2n-2} \end{pmatrix}$$

dove $\lambda_j = \alpha_1^j + ... + \alpha_n^j$.
Il determinante di quest'ultima matrice, per il teorema di Binet, è:

$$det(A \cdot A^t) = det(A) \cdot det(A^t) = (detA)^2 = \prod_{1\leq i<j\leq n} (\alpha_j - \alpha_i)^2$$

Quindi

$$\Delta = \delta^2 = (detA)^2 = det \begin{pmatrix} n & \lambda_1 & ... & \lambda_{n-1} \\ \lambda_1 & \lambda_2 & ... & \lambda_n \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n-1} & \lambda_n & ... & \lambda_{2n-2} \end{pmatrix} \qquad \square$$

Definizione 2.2.
Un polinomio $h \in K[t_1, ..., t_n]$ è detto simmetrico se $h(t_1, ..., t_n) = h(t_{\sigma(1)}, ..., t_{\sigma(n)}) \, \forall \sigma \in S_n$.
I polinomi simmetrici elementari in n variabili sono:

$$\begin{aligned} s_1 &= s_1(t_1, ..., t_n) = t_1 + ... + t_n, \\ s_2 &= s_2(t_1, ..., t_n) = \sum_{1 \leq i < j \leq n} t_i t_j, \\ &\vdots \\ s_n &= s_n(t_1, ..., t_n) = t_1 \cdot t_2 \cdots t_n. \end{aligned}$$

Teorema 2.3.
Sia h un polinomio simmetrico in $K[t_1, ..., t_n]$; allora esiste un unico polinomio $g \in K[x_1, ..., x_n]$ tale che

$$f(t_1, ..., t_n) = g(s_1, ..., s_n)$$

Dimostrazione
(Si veda per esempio [Garling], teorema 19.4)

Osservazione 2.
Sia $f \in K[x]$ un polinomio monico con radici $\alpha_1, ..., \alpha_n$ in K; allora possiamo scrivere $f = (x - \alpha_1) \cdot \cdots \cdot (x - \alpha_n) = x^n - s_1(\alpha_1, ..., \alpha_n)x^{n-1} + ... + (-1)^n s_n(\alpha_1, ..., \alpha_n)$

Corollario 2.4.
Sia f un polinomio monico, siano $\alpha_1, ..., \alpha_n$ le sue radici nel campo di spezzamento L, e sia $\lambda_j = \alpha_1^j + ... + \alpha_n^j$ per $j \geq 1$. Allora le λ_j si possono scrivere (in modo unico) come polinomi nei coefficienti di f.

Dimostrazione
Le λ_j sono polinomi simmetrici nelle $\alpha_1, ..., \alpha_n$, quindi per il teorema 2.3 si possono scrivere (in modo unico) come polinomi nelle $s_1(\alpha_1, ..., \alpha_n), ..., s_n(\alpha_1, ..., \alpha_n)$, che sono, eventualmente a meno del segno, i coefficienti di f.

Osservazione 3.
É possibile esprimere il discriminante Δ di un polinomio f partendo dai coefficienti di f e senza conoscere le radici di f. Infatti possiamo supporre f monico e concludere grazie al corollario 2.4.

Proposizione 2.5.
Sia $f = x^3 + px + q$, allora:

1. $\lambda_1 = 0, \quad \lambda_2 = -2p, \quad \lambda_3 = -3q, \quad \lambda_4 = 2p^2$

2. $\Delta = -4p^3 - 27q^2$

Dimostrazione

1. Possiamo scrivere f come:

$$x^3 + px + q = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

Allora otteniamo:

$$\begin{aligned} -\alpha_1 - \alpha_2 - \alpha_3 &= 0 \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= p \\ -\alpha_1\alpha_2\alpha_3 &= q \end{aligned}$$

Quindi

$$\begin{aligned} \lambda_1 &= \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ \lambda_2 &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = \\ &= -2p \\ \lambda_3 &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 = (\alpha_1 + \alpha_2 + \alpha_3)^3 - 3\alpha_1^2\alpha_2 - 3\alpha_1^2\alpha_3 - 3\alpha_2^2\alpha_1 \\ &\quad - 3\alpha_2^2\alpha_3 - 3\alpha_3^2\alpha_1 - 3\alpha_3^2\alpha_2 - 6\alpha_1\alpha_2\alpha_3 = \\ &= -3\alpha_1(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) - 3\alpha_2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\ &\quad - 3\alpha_3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) + 3\alpha_1\alpha_2\alpha_3 = \\ &= 3(-\alpha_1 - \alpha_2 - \alpha_3)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) - 3(-\alpha_1\alpha_2\alpha_3) = -3q \\ \lambda_4 &= \alpha_1^4 + \alpha_2^4 + \alpha_3^4 = (\alpha_1^2 + \alpha_2^2 + \alpha_3^2)^2 - 2(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) = \\ &= (-2p)^2 - 2[(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^2 - 2\alpha_1^2\alpha_2\alpha_3 - 2\alpha_1\alpha_2^2\alpha_3 \\ &\quad - 2\alpha_1\alpha_2\alpha_3^2] = 4p^2 - 2[p^2 + 2(-\alpha_1\alpha_2\alpha_3)(\alpha_1 + \alpha_2 + \alpha_3)] = \\ &= 4p^2 - 2(p^2 + 0) = 2p^2 \end{aligned}$$

2. Calcoliamo ora il discriminante.

$$\Delta = \begin{vmatrix} 3 & \lambda_1 & \lambda_2 \\ \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_2 & \lambda_3 & \lambda_4 \end{vmatrix}$$

Quindi

$$\begin{aligned} \Delta =& 3\lambda_2\lambda_4 + 2\lambda_1\lambda_2\lambda_3 - \lambda_2^3 - 3\lambda_3^2 - \lambda_4\lambda_1^2 = 3\lambda_2\lambda_4 - \lambda_2^3 - 3\lambda_3^2 = \\ =& 3(-2p)(2p^2) - (-2p)^3 - 3(-3q)^2 = -12p^3 + 8p^3 - 27q^2 = \\ =& -4p^3 - 27q^2 \end{aligned}$$

□

Teorema 2.6.
Sia $carK \neq 2, f \in K[x], degf = n, L$ il campo di spezzamento di f su K,e Δ il discriminante di f.
Allora $\Delta = 0$ se e solo se f ha radici multiple in L.
Se $\Delta \neq 0$, detto $G = Gal(L/K)$ il gruppo di Galois di f, si hanno le due possibilità seguenti:

a) se Δ ha una radice quadrata in K, allora $G \subseteq A_n$

b) se Δ non ha una radice quadrata in K, allora $G \nsubseteq A_n$.

Dimostrazione
Ricordiamo che

$$\Delta = \delta^2, \qquad \delta = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i),$$

dove $\alpha_1, ..., \alpha_n$ sono le radici di f in L.
Quindi $\Delta = 0 \Leftrightarrow \delta = 0 \Leftrightarrow f$ ha almeno una radice multipla.
Supponiamo ora $\Delta \neq 0$; se $\sigma \in G$ allora

$$\sigma(\delta) = \prod_{1 \le i < j \le n} (\sigma(\alpha_j) - \sigma(\alpha_i)) = \varepsilon_\sigma \delta$$

dove $\varepsilon_\sigma = 1$ se σ è una permutazione pari di $\alpha_1, ..., \alpha_n$ e $\varepsilon_\sigma = -1$ se σ è una permutazione dispari di $\alpha_1, ..., \alpha_n$.
Se Δ ha una radice quadrata in K, allora $\delta \in K$; dato che $K = G^*$, δ viene fissato da ogni elemento di G, cioè $\varepsilon_\sigma = 1 \, \forall \sigma \in G$, quindi $G \subseteq A_n$.
Se Δ non ha una radice quadrata in K, allora $\delta \notin K = G^*$, quindi esiste almeno una $\sigma \in G$ tale che $\sigma(\delta) \neq \delta$, cioè esiste almeno una $\sigma \in G$ tale che $\varepsilon_\sigma = -1$, cioè $G \nsubseteq A_n$. $\square$

Capitolo 3

Risolubilità per radicali di un polinomio

Convenzione
Sia $\alpha = \rho e^{i\theta}$ un numero complesso $\neq 0$, $\rho = |\alpha|$, e sia θ il rappresentante del suo argomento tale che $0 \leq \theta \leq 2\pi$.
Nel seguito denotiamo con $\sqrt[n]{\alpha}$ la radice $n-$esima di α tale che un rappresentante del suo argomento sia $\frac{\theta}{n}$.
Quindi ad esempio se $n = 2$ $\sqrt{\alpha} = \sqrt[2]{\alpha}$ denota la radice quadrata con parte immaginaria > 0 se $\alpha \notin \mathbb{R}^+$, e se $\alpha \in \mathbb{R}^+$, in accordo con la terminologia corrente, $\sqrt{\alpha}$ denota la radice quadrata > 0.
Le due radici quadrate di α sono $\sqrt{\alpha}$ e $-\sqrt{\alpha}$; le tre radici cubiche di α sono, come ben noto, $\sqrt[3]{\alpha}$, $\sqrt[3]{\alpha}\omega$ e $\sqrt[3]{\alpha}\omega^2$, dove $\omega = e^{i\frac{2\pi}{3}}$ è radice terza dell'unità.

3.1 Risolubilità per radicali

Definizione 3.1.
Siano $K \subseteq L$ un'estensione di campi e β un elemento di L, si dice che β è un radicale su K se $\beta^n \in K$ per un qualche $n > 0$.

Definizione 3.2.
Un'estensione $K \subseteq L$ è detta estensione per radicali se esistono dei campi intermedi

$$K = L_0 \subseteq L_1 \subseteq ... \subseteq L_{r-1} \subseteq L_r = L$$

tali che $L_i = L_{i-1}(\beta_i)$ con β_i radicale su L_{i-1} per $1 \leq i \leq r$.
Quindi $K \subseteq L$ è un'estensione per radicali se L è ottenuto aggiungendo progressivamente radicali.

Facciamo un esempio per capire meglio i concetti sopra enunciati.

Esempio
Sia $f = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$.
Se indichiamo con $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}), L_1 = \mathbb{Q}(\sqrt{2}), L_0 = \mathbb{Q}$, si ottiene che $\mathbb{Q} \subseteq L$ è un'estensione per radicali poichè:

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

e $L_1 = L_0(\sqrt{2})$ con $\sqrt{2}$ radicale su L_0;
$L = L_1(\sqrt{3})$ con $\sqrt{3}$ radicale su L_1

Definizione 3.3.
Sia $f \in K[x]$, diciamo che f è risolubile per radicali se esiste un'estensione per radicali $K \subseteq L$ tale che f si spezza completamente su L.

Osservazione 4.
L non deve essere necessariamente un campo di spezzamento per f.

Il problema che sorge è quello di determinare se un $f \in K[x]$ è risolubile per radicali o meno e, in caso di risposta affermativa, trovare un algoritmo per calcolare le radici di$f$.

Nel seguito mostriamo che un polinomio in $\mathbb{Q}[x]$ di grado 3 o di grado 4 è risolubile per radicali, con un calcolo esplicito delle radici nel caso più generale che il polinomio sia a coefficienti complessi; dato che siamo interessati solo alle radici possiamo supporre che il polinomio sia monico.

3.2 Radici di un polinomio di grado 3

Premessa
In questo capitolo lavoriamo sul campo dei numeri complessi.
Sia f un polinomio cubico, monico, separabile e irriducibile in $\mathbb{C}[x]$:

$$f = x^3 + a_2x^2 + a_1x + a_0$$

É possibile semplificare l'espressione di f eliminando il termine di grado 2; per fare questo occorre ' completare il cubo'. Poniamo $g(x) = f(x - \frac{a_2}{3})$.Si ha:

$$\begin{aligned} g(x) =&(x - \frac{a_2}{3})^3 + a_2(x - \frac{a_2}{3})^2 + a_1(x - \frac{a_2}{3}) + a_0 = \\ =&x^3 - a_2x^2 + \frac{a_2^2}{3}x - \frac{a_2^3}{27} + a_2x^2 + \frac{a_2^3}{9} - \frac{2a_2^2}{3}x + a_1x - \frac{a_2a_1}{3} + a_0 = \\ =&x^3 + (-\frac{a_2^2}{3} + a_1)x + (\frac{2a_2^3}{27} - \frac{a_2a_1}{3} + a_0) = \\ =&x^3 + px + q \end{aligned}$$

dove $p = a_1 - \frac{a_2^2}{3}$ e $q = a_0 + \frac{2a_2^3}{27} - \frac{a_2 a_1}{3}$.
Se y_1, y_2, y_3 sono le radici di g allora le radici di f sono $y_1 - \frac{a_2}{3}, y_2 - \frac{a_2}{3}, y_3 - \frac{a_2}{3}$. Quindi è sufficiente determinare le radici di g; abbiamo ridotto, cioè, il problema al caso in cui il coefficiente del termine di grado 2 sia nullo.
Se $p = 0$ o $q = 0$, le radici si trovano in modo ovvio, per cui possiamo supporre $p \neq 0$ e $q \neq 0$.
Per risolvere

$$x^3 + px + q = 0$$

consideriamo la seguente sostituzione per $z \neq 0$:

$$x = z - \frac{p}{3z}$$

Quindi si ha:

$$\begin{aligned}(z - \frac{p}{3z})^3 + p(z - \frac{p}{3z}) + q =& z^3 + \frac{p^2}{3z} - pz - \frac{p^3}{27z^3} + pz - \frac{p^2}{3z} + q = \\ =& z^3 - \frac{p^3}{27z^3} + q\end{aligned}$$

Moltiplicando per z^3 si ha:

$$z^6 + z^3 q - \frac{p^3}{27} = 0$$

A primo impatto l'equazione trovata non sembra utile, in quanto partendo da un'equazione di terzo grado siamo giunti ad una di sesto; ma possiamo notare che quest'ultima può essere riscritta come:

$$(z^3)^2 + qz^3 - \frac{p^3}{27} = 0 \tag{3.1}$$

Da questa, otteniamo (si ricordi la convenzione 1):

$$z^3 = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Ne segue che z è una delle 3 radici cubiche di $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ o una delle 3 radici cubiche di $-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$; troviamo così le sei soluzioni della 3.1.

Poniamo

$$z_1 = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Le altre due radici si ottengono, quindi, moltiplicando z_1 per ω e ω^2.
Poichè le radici di 3.1 sono $\neq 0$, possiamo porre:

$$z_2 = -\frac{p}{3z_1}$$

allora

$$x_1 = z_1 + z_2 = z_1 - \frac{p}{3z_1} \tag{3.2}$$

è una radice di $x^3 + px + q$. Per vedere quanto vale z_2 osserviamo che

$$z_1^3 z_2^3 = -\frac{p^3}{27}$$

inoltre

$$z_1^3 \cdot \left(\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right) = \left(\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right) \cdot \left(\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right) = -\frac{p^3}{27}$$

Quindi,

$$z_2^3 = \frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

In definitiva si ottiene che z_2 è quella tra le radici cubiche $\eta := \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \eta\omega, \eta\omega^2$ tale che $z_1 z_2 = -\frac{p}{3}$; sia duque j tale che $0 \leq j \leq 2$, e $z_2 = \omega^j \cdot \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$.

Dalla 3.2 abbiamo visto che $x_1 = z_1 + z_2$ è una radice di $x^3 + px + q$, scegliendo z_1 e z_2 come sopra. Per ottenere le altre radici, osserviamo che 3.2 dà una radice ogniqualvolta le radici cubiche sono scelte in modo che il loro prodotto sia $-p/3$.
Per esempio, se utilizziamo la radice cubica ωz_1 osserviamo che

$$\omega z_1 \cdot \omega^2 z_2 = z_1 \cdot z_2 = -\frac{p}{3}$$

Questo mostra che $x_2 = \omega z_1 + \omega^2 z_2$ è un'altra radice. Analogamente, usando la radice $\omega^2 z_1$ possiamo vedere che

$$\omega^2 z_1 \cdot \omega z_2 = z_1 \cdot z_2 = -\frac{p}{3}$$

di conseguenza, $x_3 = \omega^2 z_1 + \omega z_2$ è la terza radice cercata.
Inoltre i ruoli di z_1 e z_2 sono intercambiabili, perchè se $z_2 = -\frac{p}{3z_1}$ allora $z_1 = -\frac{p}{3z_2}$, quindi l'aver scelto la radice quadrata $+\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ non è restrittivo.

Concludiamo, dunque, affermando che le radici di $g(x) = x^3 + px + q$ sono date da:

$$x_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \omega^j \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

$$x_2 = \omega \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \omega^{j+2} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

$$x_3 = \omega^2 \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \omega^{j+1} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Queste sono chiamate **formule di Cardano**.
Possiamo concludere il nostro studio osservando che, poichè ci siamo ridotti ad un polinomio del tipo x^3+px+q,è già noto il valore del discriminante. Infatti, dalla proposizione 2.5 vista precedentemente nello studio del discriminante, sappiamo che

$$\Delta = -4p^3 - 27q^2$$

É quindi, possibile riscrivere le radici di g utilizzando il discriminante e, in particolar modo, z_1 e z_2 possono essere scritti nella forma:

$$z_1 = \sqrt[3]{\frac{-q}{2} + \sqrt{-\frac{\Delta}{4\cdot 27}}} \quad z_2 = \omega^j \cdot \sqrt[3]{\frac{-q}{2} - \sqrt{-\frac{\Delta}{4\cdot 27}}}$$

3.3 Radici di un polinomio di grado 4

Come nel caso del grado 3, possiamo supporre che il polinomio di quarto grado di cui cerchiamo le radici sia monico, dividendolo eventualmente per il suo coefficiente direttore. Sia quindi f un polinomio di grado 4, monico e irriducibile in $\mathbb{C}[x]$:

$$f = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

É possibile ricondurci ad un polinomio più semplice eliminando il termine di grado 3; per fare questo poniamo $g(x) = f(x - \frac{a_3}{4})$; le radici di g danno le radici di f.
Si ha:

$$\begin{aligned} g(x) &= (x-\frac{a_3}{4})^4 + a_3(x-\frac{a_3}{4})^3 + a_2(x-\frac{a_3}{4})^2 + a_1(x-\frac{a_3}{4}) + a_0 = \\ &= x^4 - a_3x^3 + \frac{3a_3^2}{8}x^2 - \frac{a_3^3}{16}x + \frac{a_3^4}{256} + a_3x^3 - \frac{a_3^2}{4}x^2 + \frac{3a_3^3}{16}x - \frac{a_3^4}{64} + \\ &a_2x^2 + \frac{a_3^2a_2}{16} - \frac{a_2a_3}{2}x + a_1x - \frac{a_1a_3}{4} + a_0 = \\ &= x^4 + x^2(\frac{a_3^2}{8} + a_2) + x(\frac{a_3^3}{8} - \frac{a_2a_3}{2} + a_1) + (-\frac{3a_3^4}{64} + \frac{a_3^2a_2}{16} - \frac{a_1a_3}{4} + a_0) = \\ &x^4 + px^2 + qx + r \end{aligned}$$

con $p = \frac{a_3^2}{8} + a_2$, $q = \frac{a_3^3}{8} - \frac{a_2a_3}{2} + a_1$ e $r = -\frac{3a_3^4}{256} + \frac{a_3^2a_2}{16} - \frac{a_1a_3}{4} + a_0$.
Possiamo supporre $q \neq 0$ (se $q = 0, g = 0$ si risolve come una equazione di 2° grado in x^2).
Cerchiamo di individuare le radici di g, per fare questo possiamo utilizzare un metodo introdotto da Cartesio che consiste nello scrivere g come prodotto di due polinomi di secondo grado monici aventi il coefficiente di x opposto.
Poniamo quindi

$$g(x) = (x^2 + ux + v)(x^2 - ux + w). \tag{3.3}$$

Da 3.3 si ha:

$$\begin{aligned}(x^2+ux+v)(x^2-ux+w) =& x^4-ux^3+wx^2+ux^3-u^2x^2+uwx+vx^2- \\ & uvx+vw = \\ =& x^4+x^2(w-u^2+v)+x(uw-uv)+vw\end{aligned}$$

Quindi otteniamo il seguente sistema:

$$\begin{cases} w+v=p+u^2 \\ u(w-v)=q \\ vw=r \end{cases} \tag{3.4}$$

Si ha quindi: $(w-v)^2=v^2+w^2-2vw=(v+w)^2-4vw=(p+u^2)^2-4r$.
Elevando al quadrato i due membri, la seconda equazione del sistema 3.4 diventa:

$$u^2((p+u^2)^2-4r)=q^2. \tag{3.5}$$

Sviluppando si ha:

$$\begin{aligned} u^2(p^2+u^4+2pu^2-4r)&=q^2 \\ u^6+2pu^4+(p^2-4r)u^2-q^2&=0\end{aligned}$$

Questa scrittura risulta essere un'equazione cubica nell'incognita u^2; quindi possiamo trovare le radici u_1^2,u_2^2,u_3^2 (tutte $\neq 0$ perchè $q\neq 0$) utilizzando le formule di Cardano introdotte nello studio dei polinomi cubici; abbiamo così $\pm u_1,\pm u_2,\pm u_3$.
Sia $\overline{u}$ uno qualsiasi di questi sei valori, e poniamo:

$$\begin{aligned}\overline{w} =& \frac{1}{2}\left(p+\overline{u}^2+\frac{q}{\overline{u}}\right) \\ \overline{v} =& \frac{1}{2}\left(p+\overline{u}^2-\frac{q}{\overline{u}}\right)\end{aligned}$$

Si osservi incidentalmente che $\overline{u}$ dà lo spezzamento $g=(x^2+\overline{u}x+\overline{v})(x^2-\overline{u}x+\overline{w})$ e $-\overline{u}$ dà lo spezzamento $g=(x^2-\overline{u}x+\overline{w})(x^2+\overline{u}x+\overline{v})$, cioè $\overline{u}$ e $-\overline{u}$ danno lo stesso spezzamento di g.
Si vede che $\overline{v}$ e $\overline{w}$ così fatti verificano il nostro sistema, poichè:

$$\begin{aligned}\overline{w}+\overline{v} &= \frac{p}{2}+\frac{\overline{u}^2}{2}+\frac{q}{\overline{u}}+\frac{p}{2}+\frac{\overline{u}^2}{2}-\frac{q}{\overline{u}}=p+\overline{u}^2 \\ \overline{w}-\overline{v} &= \frac{p}{2}+\frac{\overline{u}^2}{2}+\frac{q}{\overline{u}}-\frac{p}{2}-\frac{\overline{u}^2}{2}+\frac{q}{\overline{u}}=\frac{q}{\overline{u}} \\ &\rightarrow \overline{u}(\overline{w}-\overline{v})=q \\ \overline{v}\cdot\overline{w} &= \frac{1}{4}\left((p+\overline{u}^2)^2-\frac{q^2}{\overline{u}^2}\right)\end{aligned}$$

Essendo $\overline{u}$ soluzione di 3.5, si ha $q^2 = u^2((p+u^2)^2 - 4r)$; allora si ottiene:

$$v \cdot w = \frac{1}{4}((p+u^2)^2 - (p+u^2)^2 + 4r) = r$$

Quindi ognuna delle 6 radici $\overline{u}$ della 3.5 dà una soluzione per il sistema 3.4, cioè dà lo spezzamento 3.3 di g cercato.
In conclusione, una volta trovati i valori di $\overline{w}$ e $\overline{v}$ possiamo ricavare le quattro radici di g, poichè queste saranno le radici di $x^2 + \overline{u}x + \overline{v}$ e di $x^2 - \overline{u}x + \overline{w}$, cioè:

$$x_1 = \frac{-\overline{u} + \sqrt{\overline{u}^2 - 4\overline{v}}}{2}$$
$$x_2 = \frac{-\overline{u} - \sqrt{\overline{u}^2 - 4\overline{v}}}{2}$$
$$x_3 = \frac{\overline{u} + \sqrt{\overline{u}^2 - 4\overline{w}}}{2}$$
$$x_4 = \frac{\overline{u} - \sqrt{\overline{u}^2 - 4\overline{w}}}{2}$$

Capitolo 4

La corrispondenza di Galois per polinomi razionali di terzo grado: esempi

4.1 Esempio 1: un polinomio cubico razionale con una radice in $\mathbb{R} \setminus \mathbb{Q}$ e due radici in $\mathbb{C} \setminus \mathbb{R}$

Sia $f = x^3 - 5 \in \mathbb{Q}[x]$.
Vogliamo costruire il campo di spezzamento di f come sottocampo di $\mathbb{C}$.
Iniziamo con l'osservare che nel campo dei complessi abbiamo tre radici: $\sqrt[3]{5}$, $\sqrt[3]{5}\mu$, $\sqrt[3]{5}\mu^2$ dove $1, \mu, \mu^2$ sono le radici terze dell'unità:
$\mu = \frac{-1+i\sqrt{3}}{2}$, $\mu^2 = \frac{-1-i\sqrt{3}}{2} = \bar{\mu}$
Denotiamo le tre radici di f come $\alpha_1 = \sqrt[3]{5}$, $\alpha_2 = \sqrt[3]{5}\mu$, $\alpha_3 = \sqrt[3]{5}\mu^2 = \bar{\alpha_2}$

Consideriamo la prima radice α_1. Il suo polinomio minimo su $\mathbb{Q}$ è $x^3 - 5$, in quanto questo polinomio monico si annulla in $\sqrt[3]{5}$ e risulta essere irriducibile per il criterio di Eisenstein. Quindi l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{5})$ ha grado 3 e non risulta essere un'estensione normale, infatti $\mathbb{Q}(\sqrt[3]{5}) \subset \mathbb{R}$ ma $\alpha_1, \alpha_2 \in \mathbb{C} \setminus \mathbb{R}$ quindi $\alpha_2, \alpha_3 \notin \mathbb{Q}(\sqrt[3]{5})$.
Quindi per costruire il campo di spezzamento di f su $\mathbb{Q}$ dobbiamo aggiungere le altre due radici α_2 e α_3.
Su $\mathbb{Q}(\sqrt[3]{5})$ f si spezza come

$$f = (x - \sqrt[3]{5})(x^2 + \sqrt[3]{5}x + \sqrt[3]{25}),$$

e osservando il polinomio $g = x^2 + \sqrt[3]{5}x + \sqrt[3]{25}$ notiamo che questo risulta essere irriducibile su $\mathbb{Q}(\sqrt[3]{5})$ poichè se non lo fosse le sue radici α_2 e α_3 starebbero in $\mathbb{Q}(\sqrt[3]{5})$, quindi g è il polinomio minimo di α_2 su $\mathbb{Q}(\sqrt[3]{5})$.
Poniamo $E = \mathbb{Q}(\sqrt[3]{5}, \alpha_2)$, questa estensione risulta avere grado 2 su $\mathbb{Q}(\sqrt[3]{5})$; inoltre su E è possibile scrivere f come $f = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, cioè f si spezza completamente su E, ovvero il campo di spezzamento di f su $\mathbb{Q}$ è E.

In conclusione l'estensione $\mathbb{Q} \subseteq E$ è un'estensione di grado 6, tale affermazione risulta essere immediata considerando il teorema della torre; infatti:
$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 6$.
In definitiva abbiamo mostrato che aggiungendo α_1 e poi estendendo ancora con α_2 è possibile individuare il campo di spezzamento del nostro polinomio iniziale f su $\mathbb{Q}$.

Proviamo ora a vedere cosa accade aggiungendo a $\mathbb{Q}$ prima la radice α_2.
Il polinomio minimo di α_2 su $\mathbb{Q}$ è $x^3 - 5$ per le stesse motivazioni di prima, ne viene che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_2)$ ha grado 3 ed f sul nuovo campo $\mathbb{Q}(\alpha_2)$ si spezza in questo modo:

$$f = (x - \alpha_2)(x^2 - \sqrt[3]{5}\frac{1 - i\sqrt{3}}{2}x + \sqrt[3]{25}\frac{-1 - i\sqrt{3}}{2}).$$

Poniamo $h = x^2 - \sqrt[3]{5}\frac{1-i\sqrt{3}}{2}x + \sqrt[3]{25}\frac{-1-i\sqrt{3}}{2}$; è possibile osservare che h è irriducibile su $\mathbb{Q}(\alpha_2)$, poichè le radici α_1 e $\alpha_3 \notin \mathbb{Q}(\alpha_2)$ in quanto già abbiamo mostrato che il grado del campo di spezzamento E su $\mathbb{Q}$ è > 3. Mostriamo esplicitamente con un conto diretto che $\alpha_1 \notin \mathbb{Q}(\alpha_2)$.
Se $\alpha_1 \in \mathbb{Q}(\alpha_2)$ allora dovrebbero esistere $a, b, c \in \mathbb{Q}$ tali che α_1 si potrebbe scrivere come:

$$\alpha_1 = a + b\alpha_2 + c\alpha_2^2$$

Sviluppando i calcoli otteniamo:

$$\begin{aligned}\sqrt[3]{5} &= a + b\sqrt[3]{5}\frac{-1 + i\sqrt{3}}{2} + c\sqrt[3]{25}\frac{-1 - i\sqrt{3}}{2} = \\ &= (a - b\frac{\sqrt[3]{5}}{2} - c\frac{\sqrt[3]{25}}{2}) + (b\sqrt[3]{5}\frac{\sqrt{3}}{2} - c\sqrt[3]{25}\frac{\sqrt{3}}{2})i\end{aligned}$$

Quindi in particolar modo dovrebbe essere $b\sqrt[3]{5}\frac{i\sqrt{3}}{2} - c\sqrt[3]{25}\frac{i\sqrt{3}}{2} = 0$ cioè $b - c\sqrt[3]{5} = 0$, ma non esistono b e $c \in \mathbb{Q}$ che verificano questa equazione.
In conclusione abbiamo provato che $\alpha_1 \notin \mathbb{Q}(\alpha_2)$, e se una radice di h non sta in un campo, non ci sta neanche l'altra, dato che $degh = 2$.
Il polinomio minimo di α_1 su $\mathbb{Q}(\alpha_2)$ è proprio h e quindi ritroviamo che $E = \mathbb{Q}(\alpha_2, \alpha_1, \alpha_3) = \mathbb{Q}(\alpha_2, \alpha_1)$ è un' estensione di grado 6 su $\mathbb{Q}$.

Osserviamo, in ultima analisi, che aggiungendo come prima radice α_3 troviamo $\mathbb{Q}(\alpha_3)$ di grado 3 su $\mathbb{Q}$ con le restanti due radici che non appartengono a $\mathbb{Q}(\alpha_3)$ come nei due precedenti casi.

Quindi nell'estensione $E/\mathbb{Q}$ abbiamo trovato 3 campi intermedi distinti di grado 3 su $\mathbb{Q}$; e cioè $\mathbb{Q}(\alpha_1), \mathbb{Q}(\alpha_2)$ e $\mathbb{Q}(\alpha_3)$.

Studiamo ora il gruppo di Galois$(E/\mathbb{Q})$ che indicheremo semplicemente con G, il quale agisce transitivamente sulle radici di $x^3 - 5$.

Poichè il polinomio ha grado 3, G sarà un sottogruppo del gruppo S_3 delle permutazioni su tre elementi, d'altra parte essendo $|G| = [E : \mathbb{Q}] = |S_3| = 6$ si ha

$$G = S_3.$$

Ricordiamo che S_3 ha tre sottogruppi non banali di ordine 2 : $H_1 =< (23) >$, $H_2 =< (13) >$ e $H_3 =< (12) >$ tali che $(S_3 : H_i) = 3 \ \forall i = 1, 2, 3$; si ha che $H_i \not\lhd S_3$ $\forall i = 1, 2, 3$.
Inoltre, in S_3 abbiamo un unico sottogruppo di ordine 3 che indicheremo con $H =< (123) >$ il quale risulta avere indice 2 ed è quindi $\lhd S_3$.
Soffermiamoci ora su quanto appena detto; abbiamo, infatti, osservato che $G = S_3$. Da un teorema enunciato precedentemente (teorema 2.6), sappiamo che $G = S_3$ implica che Δ non ha una radice quadrata in $\mathbb{Q}$. Proviamolo.
Nelle notazioni della proposizione 2.5, se $f = x^3 - 5$ si ha $p = 0$ e $q = -5$.
Calcoliamo, ora, il discriminante:

$$\Delta = -4p^3 - 27q^2 = -27 \cdot 25 = -675$$

Abbiamo quindi effettivamente dimostrato che Δ non ha una radice quadrata in $\mathbb{Q}$ poichè -675 non è un quadrato in $\mathbb{Q}$.
Torniamo ora al nostro gruppo di Galois G e osserviamo che se $\sigma \in G$ allora questo sarà individuato da $\sigma(\alpha_i)$ $\forall i = 1, 2, 3$; infatti essendo $G = S_3$ ne segue che fissata comunque una permutazione delle radici, esiste un automorfismo di E che permuta le radici in quel modo.
Vediamo meglio come agiscono gli elementi di G; abbiamo $G = \{id, \sigma_1, \sigma_2, \sigma_3, \phi, \phi^2\}$ dove:

$$\begin{aligned} (2\,3) = \sigma_1 : \quad & E \longrightarrow E \\ & \alpha_1 \mapsto \alpha_1 \\ & \alpha_2 \mapsto \alpha_3 \\ & \alpha_3 \mapsto \alpha_2 \end{aligned}$$

$$\begin{aligned} (1\,3) = \sigma_2 : \quad & E \longrightarrow E \\ & \alpha_1 \mapsto \alpha_3 \\ & \alpha_2 \mapsto \alpha_2 \\ & \alpha_3 \mapsto \alpha_1 \end{aligned}$$

$$\begin{aligned} (1\,2) = \sigma_3 : \quad & E \longrightarrow E \\ & \alpha_1 \mapsto \alpha_2 \\ & \alpha_2 \mapsto \alpha_1 \\ & \alpha_3 \mapsto \alpha_3 \end{aligned}$$

$$(1\,2\,3) = \phi: \quad \begin{aligned} E &\longrightarrow E \\ \alpha_1 &\mapsto \alpha_2 \\ \alpha_2 &\mapsto \alpha_3 \\ \alpha_3 &\mapsto \alpha_1 \end{aligned}$$

Utilizzando le notazioni precedentemente introdotte possiamo concludere che

$$H_i =< \sigma_i > \quad \forall i = 1,2,3, \quad H =< \phi > .$$

Analizziamo in modo più approfondito H_1.
Iniziamo con il creare una base del nostro campo di spezzamento. Da quanto dimostrato precedentemente abbiamo che $E = \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1)(\alpha_2)$, dal teorema della torre sappiamo che una base per E è data da $\{1, \alpha_1, \alpha_1^2\} \cdot \{1, \alpha_2\} = \{1, \alpha_1, \alpha_1^2, \alpha_2, \alpha_1\alpha_2, \alpha_1^2\alpha_2\}$.
Vediamo ora come agisce σ_1 su tali elementi:

$$\sigma_1: \quad \begin{aligned} E &\longrightarrow E \\ 1 &\mapsto 1 \\ \alpha_1 &\mapsto \alpha_1 \\ \alpha_1^2 &\mapsto \alpha_1^2 \\ \alpha_2 &\mapsto \alpha_3 \\ \alpha_1\alpha_2 &\mapsto \alpha_1\alpha_3 \\ \alpha_1^2\alpha_2 &\mapsto \alpha_1^2\alpha_3 \end{aligned}$$

Tale automorfismo deve mandare la radice α_3 in α_2; proviamo che ciò è verificato.
Possiamo scrivere α_3 come:

$$\alpha_3 = \sqrt[3]{5}\frac{-1 - i\sqrt{3}}{2} = \frac{\sqrt[3]{25}(-1 - i\sqrt{3})}{2\sqrt[3]{5}} = \frac{\alpha_2^2}{\alpha_1}$$

Ora:

$$\sigma_1(\alpha_3) = \sigma_1(\frac{\alpha_2^2}{\alpha_1}) = \frac{\alpha_3^2}{\alpha_1} = \frac{\sqrt[3]{25}(-1 + i\sqrt{3})}{2\sqrt[3]{5}} = \sqrt[3]{5}\frac{-1 + i\sqrt{3}}{2} = \alpha_2$$

Osservando l'automorfismo preso in esame possiamo notare che gli elementi della base fissata di $\mathbb{Q}(\alpha_1)(\alpha_2)$ vengono mandati in $\{1, \alpha_1, \alpha_1^2, \alpha_3, \alpha_1\alpha_3, \alpha_1^2\alpha_3\}$ e queste sono proprio le componenti della base $\{1, \alpha_1, \alpha_1^2\} \cdot \{1, \alpha_3\}$ di $\mathbb{Q}(\alpha_1)(\alpha_3) = E$.
Vediamo ora chi è il campo fisso di H_1.

Si ha:
$H_1^* = \{a \in E | \sigma(a) = a \quad \forall \sigma \in H_1\} = \{a \in E | id(a) = a, \sigma_1(a) = a\} =$
$= \{a \in E | \sigma_1(a) = a\}$.
Il generico elemento di E si scrive in modo unico come

$a_1 + a_2\alpha_1 + a_3\alpha_1^2 + a_4\alpha_2 + a_5\alpha_1\alpha_2 + a_6\alpha_1^2\alpha_2$, con $a_i \in \mathbb{Q}$; risulta:

$\sigma_1(a_1+a_2\alpha_1+a_3\alpha_1^2+a_4\alpha_2+a_5\alpha_1\alpha_2+a_6\alpha_1^2\alpha_2) = a_1+a_2\alpha_1+a_3\alpha_1^2+a_4\alpha_3+a_5\alpha_1\alpha_3+a_6\alpha_1^2\alpha_3$.

Quindi $\mathbb{Q}(\alpha_1) \subseteq H_1^*$. Poichè $|H_1| = 2$ la corrispondenza di Galois ci dice che $[E : H_1^*] = 2$ e quindi $[H_1^* : \mathbb{Q}] = 3$ per il teorema della torre; da cui $\mathbb{Q}(\alpha_1) = H_1^*$.
Questo stesso ragionamento può essere fatto, in modo analogo, anche per H_2 e H_3; in conclusione si ottiene

$$H_i^* = \mathbb{Q}(\alpha_i) \quad \forall i = 1, 2, 3.$$

Si osservi che $H_i \not\lhd G$ e corrispondentemente $\mathbb{Q}(\alpha_i)$ non è un estensione normale di $\mathbb{Q}$ come già dimostrato precedentemente.

Studiamo, infine, H.
Vediamo meglio come agisce la ϕ.

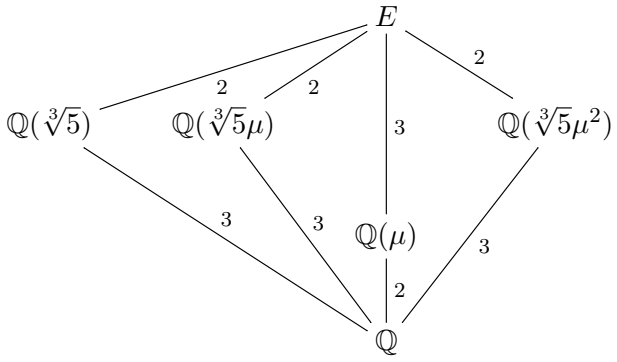
$$\begin{aligned} \phi: \quad E = \mathbb{Q}(\alpha_1)(\alpha_2) &\longrightarrow E = \mathbb{Q}(\alpha_2)(\alpha_3) \\ 1 &\mapsto 1 \\ \alpha_1 &\mapsto \alpha_2 \\ \alpha_1^2 &\mapsto \alpha_2^2 \\ \alpha_2 &\mapsto \alpha_3 \\ \alpha_1\alpha_2 &\mapsto \alpha_2\alpha_3 \\ \alpha_1^2\alpha_2 &\mapsto \alpha_2^2\alpha_3 \end{aligned}$$

Osserviamo che $\alpha_1^2\alpha_2 = \sqrt[3]{25} \cdot \sqrt[3]{5}\mu = 5\mu$ e analogamente $\alpha_2^2\alpha_3 = \sqrt[3]{25}\mu^2 \cdot \sqrt[3]{5}\mu^2 = 5\mu$; quindi $\phi(5\mu) = 5\phi(\mu) = 5\mu$ e da questo possiamo dedurre che $\phi(\mu) = \mu$. É possibile vedere che μ ha grado 2 su $\mathbb{Q}$ in quanto il polinomio minimo di μ è $x^2 + x + 1$, quindi $\mathbb{Q}(\mu)$ risulta essere un' estensione normale poichè di grado 2.
Si ha:
$H^* = \{a \in E | \sigma(a) = a \quad \forall \sigma \in H\} = \{a \in E | \phi(a) = a\}$; infatti $H = \{id, \phi, \phi^2\}$ e se $\phi(a) = a$ allora $\phi^2(a) = \phi(\phi(a)) = \phi(a) = a$.
Quindi, poichè $\phi(\mu) = \mu$, si ha $\mathbb{Q}(\mu) \subseteq H^*$. Poichè $|H| = 3$, la corrispondenza di Galois ci dice che $[E : H^*] = 3$ e quindi $[H^* : \mathbb{Q}] = 2$ per il teorema della torre, da cui:

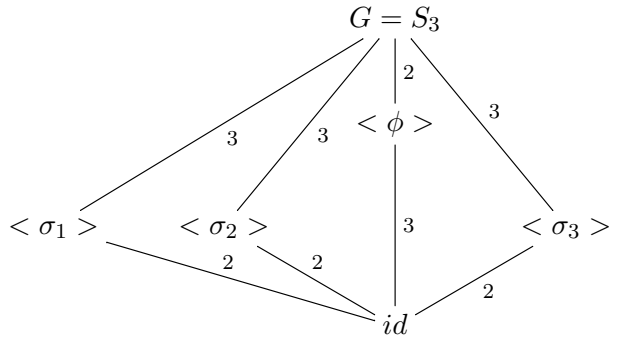
$$H^* = \mathbb{Q}(\mu).$$

Concludiamo il nostro studio osservando che H_1 e H_2 sono sottogruppi coniugati.
Infatti $(12)(23)(12) = (13)$, cioè $\sigma_3 H_1 \sigma_3^{-1} = H_2$. Allora la corrispondenza di Galois ci dice che le due estensioni corrispondenti sono anch'esse coniugate; infatti l'automorfismo σ_3 è tale che $\sigma_3(\mathbb{Q}(\alpha_1)) = \mathbb{Q}(\alpha_2)$, cioè $\sigma_3(H_1^*) = H_2^*$.

Concludiamo il nostro studio mostrando graficamente la corrispondenza trovata.



dove il numero accanto all'estensione denota il grado.



dove il numero accanto all'inclusione denota l'indice del sottogruppo piccolo nel sottogruppo grande.

4.2 Esempio 2: un polinomio cubico razionale con tre radici in $\mathbb{R} \setminus \mathbb{Q}$

Sia $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$.
Il polinomio f ha tre radici reali, infatti la funzione

$$\begin{aligned} \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\mapsto x^3 - 3x + 1 \end{aligned}$$

cambia segno tra -2 e 0, tra 0 e 1, e tra 1 e 2, dunque ha tre zeri reali di cui due > 0 e uno < 0.
Sia α una qualsiasi di queste radici, e proviamo che $\alpha \notin \mathbb{Q}$.
Se fosse $\alpha = \frac{a}{b}$ con $a, b \in \mathbb{Z}$, $(a, b) = 1, b > 0$, si avrebbe

$$\begin{aligned} &\frac{a^3}{b^3} - 3\frac{a}{b} + 1 = 0 \\ &a^3 - 3ab^2 + b^3 = 0 \\ &a^3 = b^2(3a - b) \text{ da cui } \quad b|a^3 \Rightarrow b = 1 \end{aligned}$$

Allora $a^3 - 3a + 1 = 0$ da cui $a(a^2 - 3) = -1$, quindi $a = \pm 1$ e $a^2 - 3 = \mp 1$, il che non è possibile.
Quindi il polinomio f, di terzo grado e senza radici in $\mathbb{Q}$, è irriducibile su $\mathbb{Q}$.

Vogliamo costruire il campo di spezzamento di f come sottocampo di $\mathbb{C}$.
Iniziamo con il calcolare le radici del polinomio mediante le formule di Cardano.
Nelle notazioni di paragrafo 3.2, si ha $p = -3, q = 1$, e
$z_1^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = -\frac{1}{2} + \sqrt{\frac{1}{4} - 1} = -\frac{1}{2} + \frac{i\sqrt{3}}{2} = e^{i\frac{2\pi}{3}}$ e
$z_2^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = -\frac{1}{2} - \frac{i\sqrt{3}}{2} = e^{i\frac{4\pi}{3}}$.
Poniamo $\zeta = e^{i\frac{2}{9}\pi}$
Le tre radici cubiche di $e^{i\frac{2\pi}{3}}$ sono $\zeta = e^{i\frac{2}{9}\pi}, \zeta^4 = e^{i\frac{8}{9}\pi}, \zeta^7 = e^{i\frac{14}{9}\pi}$ e le tre radici cubiche di $e^{i\frac{4\pi}{3}}$ sono $\zeta^2 = e^{i\frac{4}{9}\pi}, \zeta^5 = e^{i\frac{10}{9}\pi}, \zeta^8 = e^{i\frac{16}{9}\pi}$; quindi le coppie (z_1, z_2) tali che $z_1 \cdot z_2 = -\frac{p}{3} = 1$ sono: $(\zeta, \zeta^8), (\zeta^4, \zeta^5)$ e (ζ^7, ζ^2), da cui le radici di f sono:

$\alpha_1 = \zeta + \zeta^8$,
$\alpha_2 = \zeta^4 + \zeta^5$,
$\alpha_3 = \zeta^7 + \zeta^2$

Consideriamo la prima radice α_1. Il suo polinomio minimo su $\mathbb{Q}$ è $x^3 - 3x + 1$ essendo f irriducibile e monico.
Quindi $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1)$ è un'estensione di grado 3, inoltre tale estensione risulta essere normale poichè α_2 e $\alpha_3 \in \mathbb{Q}(\alpha_1)$.
Proviamolo:
$\alpha_3 = \alpha_1^2 - 2$ infatti
$\alpha_1^2 - 2 = \zeta^2 + \zeta^{16} + 2\zeta^9 - 2 = \zeta^2 + \zeta^{16} = \zeta^2 + \zeta^7 = \alpha_3$
$\alpha_2 = \zeta^4 + \zeta^5 = (\zeta^7 + \zeta^2)^2 - 2 = \alpha_3^2 - 2$.
Abbiamo quindi provato che le restanti due radici appartengono a $E = \mathbb{Q}(\alpha_1)$ e quindi che l'estensione è normale; ne viene allora che E è il campo di spezzamento di f cercato; infatti su E f si spezza completamente come:

$$f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Osserviamo, inoltre, che lo stesso ragionamento può essere fatto partendo dalla radice α_2 o dalla radice α_3 poichè $x^3 - 3x + 1$ è il polinomio minimo di tutte le radici.
Di conseguenza, si ottiene che $E = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha_3)$ e

$$[E : \mathbb{Q}] = 3$$

Studiamo ora il gruppo di Galois$(E/\mathbb{Q})$ che indicheremo semplicemente con G.
Poichè il polinomio ha grado 3, G sarà un sottogruppo del gruppo S_3 delle permutazioni su $\{\alpha_1, \alpha_2, \alpha_3\}$; inoltre, poichè $[E : \mathbb{Q}] = 3$ necessariamente $|G| = 3$. Quindi G è l'unico sottogruppo di S_3 di ordine 3, ossia $G = A_3$
Studiamo il discriminante del nostro polinomio:

$$\Delta = -4p^3 - 27 = (-4)(-27) - 27 = 81$$

Quindi Δ è un quadrato in $\mathbb{Q}$, e il teorema 2.6 ci conferma che dovrà valere:

$$G \subseteq A_3.$$

Quindi

$$G = A_3.$$

Torniamo ora al nostro gruppo di Galois G, vi sono quindi tre automorfismi:

$$\begin{aligned} id: \quad & E \longrightarrow E \\ & \alpha_1 \mapsto \alpha_1 \\ & \alpha_2 \mapsto \alpha_2 \\ & \alpha_3 \mapsto \alpha_3 \end{aligned}$$

$$\begin{aligned} (1\,2\,3) = \tau_1: \quad & E \longrightarrow E \\ & \alpha_1 \mapsto \alpha_2 \\ & \alpha_2 \mapsto \alpha_3 \\ & \alpha_3 \mapsto \alpha_1 \end{aligned}$$

$$\begin{aligned} (1\,3\,2) = \tau_2: \quad & E \longrightarrow E \\ & \alpha_1 \mapsto \alpha_3 \\ & \alpha_2 \mapsto \alpha_1 \\ & \alpha_3 \mapsto \alpha_2 \end{aligned}$$

Poichè

$$G =< \tau_1 > \cong \mathbb{Z}_3.$$

G non ha sottogruppi diversi da quelli banali. Concludiamo il nostro studio mostrando graficamente la corrispondenza trovata.

$$\begin{array}{c} E = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha_3) \\ \Big| 3 \\ \mathbb{Q} \end{array}$$

$$\begin{array}{c} G = A_3 \\ \Big| 3 \\ id \end{array}$$

Capitolo 5

La corrispondenza di Galois per polinomi razionali di quarto grado: esempi

5.1 Esempio 3: il polinomio $(x^2-2)(x^2-3)$

Sia $f=(x^2-2)(x^2-3)\in\mathbb{Q}[x]$.
Vogliamo costruire il campo di spezzamento di f come sottocampo di $\mathbb{C}$.
Iniziamo con l'osservare che nel campo dei complessi abbiamo quattro radici:
$(\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3})$.
Denotiamo le quattro radici di f come $\alpha_1=\sqrt{2},\alpha_2=-\sqrt{2},\alpha_3=\sqrt{3},\alpha_4=-\sqrt{3}$.
Consideriamo la prima radice α_1.
Il suo polinomio minimo su $\mathbb{Q}$ è x^2-2, in quanto questo polinomio si annulla in $\sqrt{2}$ e risulta essere irriducibile perchè di 2° grado e senza radici in $\mathbb{Q}$, quindi $\mathbb{Q}\subseteq\mathbb{Q}(\alpha_1)=\mathbb{Q}(\alpha_2)$ è un'estensione di grado 2.
Osserviamo che $\alpha_3\notin\mathbb{Q}(\alpha_1)$, infatti se $\alpha_3\in\mathbb{Q}(\alpha_1)$ allora dovrebbero esistere $a,b\in\mathbb{Q}$ tali che α_3 si potrebbe scrivere come :

$$\alpha_3=a+b\sqrt{2}$$

da cui $(\sqrt{3})^2=(a+b\sqrt{2})^2$ cioè $3=a^2+2b^2+2ab\sqrt{2}$ da cui seguirebbe la razionalità di $\sqrt{2}$.
Quindi non esistono a e b razionali che verificano tale equazione.
Questo ci dice che per costruire il campo di spezzamento dobbiamo aggiungere le altre due radici α_3 e α_4.
Su $\mathbb{Q}(\alpha_1)$ f si spezza come

$$f=(x-\sqrt{2})(x+\sqrt{2})(x^2-3)=(x-\alpha_1)(x-\alpha_2)(x^2-3);$$

considerando $g=x^2-3$ osserviamo che tale polinomio è irriducibile su $\mathbb{Q}(\alpha_1)$ perchè di 2° grado e senza radici in $\mathbb{Q}(\sqrt{2})$ e quindi risulta essere il polinomio minimo di α_3 e α_4.

Sia $E = \mathbb{Q}(\alpha_1, \alpha_3) = \mathbb{Q}(\alpha_1, \alpha_4)$; questa risulta essere un'estensione di grado 2 di $\mathbb{Q}(\alpha_1)$.
Inoltre su E f si spezza come $f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$, cioè f si spezza completamente su E, ovvero il campo di spezzamento di f è proprio E.
L'estensione $\mathbb{Q} \subseteq E$ è un'estensione di grado 4, tale affermazione risulta essere immediata considerando il teorema della torre; infatti:
$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$.
In questa costruzione $E = \mathbb{Q}(\alpha_1)(\alpha_3)$ viene evidenziato il campo intermedio $\mathbb{Q}(\alpha_1)$.

Proviamo ora a vedere cosa accade aggiungendo a $\mathbb{Q}$ prima la terza radice α_3.
Il polinomio minimo di α_3 su $\mathbb{Q}$ è $x^2 - 3$ per le stesse motivazioni di prima, ne viene che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_3)$ ha grado 2 ed f sul nuovo campo $\mathbb{Q}(\alpha_3)$ si spezza in questo modo:

$$f = (x - \sqrt{3})(x + \sqrt{3})(x^2 - 2) = (x - \alpha_3)(x - \alpha_4)(x^2 - 2).$$

Consideriamo $h = x^2 - 2$, tale polinomio è irriducibile su $\mathbb{Q}(\alpha_3)$ e, come già visto prima risulta essere il polinomio minimo di α_1 e α_2; $\mathbb{Q}(\alpha_3)(\alpha_1)$ è un'estensione di grado 2 di $\mathbb{Q}(\alpha_3)$ e ovviamente $E = \mathbb{Q}(\alpha_1)(\alpha_3) = \mathbb{Q}(\alpha_3)(\alpha_1)$; ma in questa costruzione viene evidenziato il campo intermedio $\mathbb{Q}(\alpha_3)$.

Studiamo ora il gruppo di Galois$(E/\mathbb{Q})$ che indicheremo semplicemente con G.
Poichè il polinomio ha grado 4, G sarà un sottogruppo del gruppo S_4 delle permutazioni su quattro elementi, d'altra parte la corrispondenza di Galois ci assicura che $|G| = 4$ poichè abbiamo provato che $[E : \mathbb{Q}] = 4$.
Sia $\sigma \in G$; allora $\sigma(\sqrt{2})$ non può essere nè $\sqrt{3}$ nè $-\sqrt{3}$, perchè se ad esempio $\sigma(\sqrt{2}) = \sqrt{3}$, allora $\sigma(2) = \sigma((\sqrt{2})^2) = (\sqrt{3})^2 = 3$ che non è possibile. Quindi per ogni $\sigma \in G$, $\sigma\{\sqrt{2}, -\sqrt{2}\} = \{\sqrt{2}, -\sqrt{2}\}$ e $\sigma\{\sqrt{3}, -\sqrt{3}\} = \{\sqrt{3}, -\sqrt{3}\}$. Ne segue che sono possibili solo gli automorfismi con le seguenti permutazioni delle radici:

$$\begin{aligned} id: \quad & E \longrightarrow E \\ & \alpha_1 \mapsto \alpha_1 \\ & \alpha_2 \mapsto \alpha_2 \\ & \alpha_3 \mapsto \alpha_3 \\ & \alpha_4 \mapsto \alpha_4 \end{aligned}$$

$$\begin{aligned} (1\,2) = \tau_1: \quad & E \longrightarrow E \\ & \alpha_1 \mapsto \alpha_2 \\ & \alpha_2 \mapsto \alpha_1 \\ & \alpha_3 \mapsto \alpha_3 \\ & \alpha_4 \mapsto \alpha_4 \end{aligned}$$

$$(3\,4) = \tau_2 : \quad \begin{aligned} E &\longrightarrow E \\ \alpha_1 &\mapsto \alpha_1 \\ \alpha_2 &\mapsto \alpha_2 \\ \alpha_3 &\mapsto \alpha_4 \\ \alpha_4 &\mapsto \alpha_3 \end{aligned}$$

$$(1\,2)(3\,4) = \tau_3 : \quad \begin{aligned} E &\longrightarrow E \\ \alpha_1 &\mapsto \alpha_2 \\ \alpha_2 &\mapsto \alpha_1 \\ \alpha_3 &\mapsto \alpha_4 \\ \alpha_4 &\mapsto \alpha_3 \end{aligned}$$

Essendo esattamente quattro, questi sono effettivamente gli elementi di G, e non abbiamo bisogno di verificare che τ_1, τ_2, τ_3 siano automorfismi.
Da quanto dimostrato precedentemente abbiamo che $E = \mathbb{Q}(\alpha_1, \alpha_3)$, dal teorema della torre sappiamo che una base per E è data da $\{1, \alpha_1\} \cdot \{1, \alpha_3\} = \{1, \alpha_1, \alpha_3, \alpha_1\alpha_3\}$.
É facile osservare che gli automorfismi τ_1, τ_2 e τ_3 hanno tutti ordine 2, in definitiva, G è un gruppo di quattro elementi di cui tre hanno ordine 2, per cui:

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Osserviamo che $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$, quindi, necessariamente un sottogruppo non banale ha ordine 2; quindi ci sono esattamente tre sottogruppi non banali:
$G_1 =< \tau_1 >$, $G_2 =< \tau_2 >$ e $G_3 =< \tau_3 >$.

Studiamo, ora, questi sottogruppi.
Consideriamo anzitutto G_1.
Ricordiamo come agisce τ_1 sugli elementi della base scelta del campo di spezzamento:

$$\tau_1 : \quad \begin{aligned} E &\longrightarrow E \\ 1 &\mapsto 1 \\ \alpha_1 &\mapsto \alpha_2 \\ \alpha_3 &\mapsto \alpha_3 \\ \alpha_1\alpha_3 &\mapsto \alpha_2\alpha_3 \end{aligned}$$

quindi $\tau_1(a + b\alpha_1 + c\alpha_3 + d\alpha_1\alpha_3) = a + b\alpha_2 + c\alpha_3 + d\alpha_2\alpha_3 \quad \forall a, b, c, d \in \mathbb{Q}$.
Si ha:

$$\begin{aligned} a + b\alpha_2 + c\alpha_3 + d\alpha_2\alpha_3 = & a + b\alpha_1 + c\alpha_3 + d\alpha_1\alpha_3 \\ & \text{se e solo se} \qquad b\alpha_2 + d\alpha_2\alpha_3 = b\alpha_1 + d\alpha_1\alpha_3 \\ & \qquad\qquad\quad\ \ \alpha_2(b + d\alpha_3) = \alpha_1(b + d\alpha_3) \\ & \text{cioè se e solo se} \qquad b = d = 0. \end{aligned}$$

Quindi il campo fisso di G_1 è :
$G_1^* = \{v \in E | h(v) = v \quad \forall h \in G_1\} = \{v \in E | \tau_1(v) = v\} = \mathbb{Q}(\sqrt{3})$.
Per G_2 è possibile ripetere questo stesso ragionamento al fine di ottenere che

$$G_2^* = \mathbb{Q}(\sqrt{2}).$$

Prendiamo in ultima analisi G_3 e vediamo come agisce τ_3 sugli elementi della base scelta:

$$\begin{aligned} \tau_3 : \quad E &\longrightarrow E \\ 1 &\mapsto 1 \\ \alpha_1 &\mapsto \alpha_2 \\ \alpha_3 &\mapsto \alpha_4 \\ \alpha_1\alpha_3 &\mapsto \alpha_2\alpha_4 \end{aligned}$$

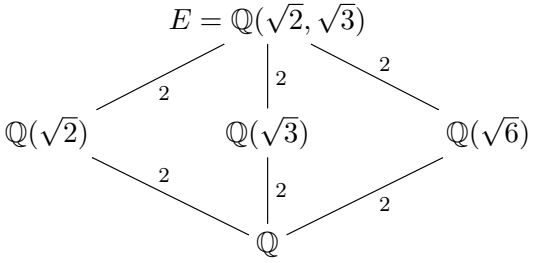
Al fine di studiare il campo fisso di G_3 esaminiamo meglio come lavora τ_3 . Consideriamo un generico elemento in E, questo sarà della forma:
$a + b\alpha_1 + c\alpha_3 + d\alpha_1\alpha_3 = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ con $a, b, c, d \in \mathbb{Q}$
questo verrà mandato da τ_3 in:
$a + b\alpha_2 + c\alpha_4 + d\alpha_2\alpha_4 = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$ con $a, b, c, d \in \mathbb{Q}$
Si ha che:

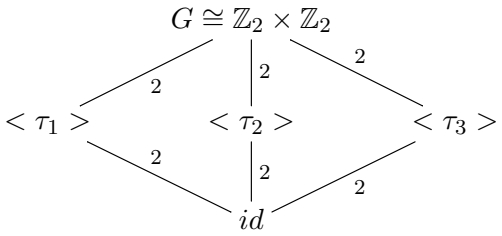
$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} \quad \text{se e solo se } b = c = 0$$

Cioè, τ_3 lascia fissi gli elementi del tipo $a + b\sqrt{6}$ con $a, b \in \mathbb{Q}$, ovvero gli elementi di $\mathbb{Q}(\sqrt{6})$. In conclusione:

$$G_3^* = \mathbb{Q}(\sqrt{6}).$$

Concludiamo il nostro studio mostrando graficamente la corrispondenza trovata.





5.2 Esempio 4: il polinomio $x^4 + 1$

Sia $f = x^4 + 1 \in \mathbb{Q}[x]$.
Vogliamo costruire il campo di spezzamento di f come sottocampo di $\mathbb{C}$.
Iniziamo con l'osservare che nel campo dei complessi abbiamo quattro radici, e precisamente le quattro radici quarte di -1.
Scriviamo -1 in forma trigonometrica:

$$-1 = e^{\pi} i$$

Quindi una fissata radice di f è $\sqrt[4]{e^{\pi i}} = e^{\frac{\pi}{4}i}$. Allora le quattro radici si ottengono moltiplicando tale radici per le radici quarte dell'unità, otteniamo così:
$\alpha_1 = e^{\frac{\pi}{4}i}$
$\alpha_2 = -e^{\frac{\pi}{4}i} = e^{\frac{5}{4}\pi i}$
$\alpha_3 = ie^{\frac{\pi}{4}i} = (e^{\frac{\pi}{2}i})(e^{\frac{\pi}{4}i}) = e^{\frac{3}{4}\pi i}$
$\alpha_4 = -ie^{\frac{\pi}{4}i} = (e^{\frac{3}{2}\pi i})(e^{\frac{\pi}{4}i}) = e^{\frac{7}{4}\pi i}$.
In particolare:
$\alpha_2 = -\alpha_1$ e $\alpha_4 = -\alpha_3$.
Poichè $\alpha_1^2 = \alpha_2^2 = i$ e $\alpha_3^2 = \alpha_4^2 = -i$, si ottiene anche che $\alpha_1^3 = \alpha_3$ e $\alpha_3^3 = \alpha_1$.
Consideriamo la prima radice α_1.
Il suo polinomio minimo su $\mathbb{Q}$ è $x^4 + 1$, infatti α_1 è una radice di $x^4 + 1$ e inoltre tale polinomio risulta essere irriducibile su $\mathbb{Q}$.
Proviamo l'irriducibilità. Si ha:
$x^4 + 1 = p_1 \cdot p_2 \cdot p_3 \cdot p_4, \qquad \text{con} \quad p_i = x - \alpha_i$
Osserviamo che non è possibile scrivere $x^4 + 1$ come prodotto di un polinomio lineare e un polinomio di terzo grado poichè nessuno degli $\alpha_i \in \mathbb{Q}$.
Proviamo, allora, a scrivere il nostro polinomio come prodotto di due polinomi di grado 2.
I casi che si presentano sono i seguenti:

1. $(p_1 \cdot p_2)(p_3 \cdot p_4)$
2. $(p_1 \cdot p_3)(p_2 \cdot p_4)$
3. $(p_1 \cdot p_4)(p_2 \cdot p_3)$

Nessuno dei tre casi dà una fattorizzazione su $\mathbb{Q}$, infatti:
$p_1 \cdot p_2 = (x-\alpha_1)(x-\alpha_2) = x^2 - i$ ma $-i \notin \mathbb{Q}$.
$p_1 \cdot p_3 = (x-\alpha_1)(x-\alpha_3) = (x-e^{\frac{\pi}{4}i})(x-e^{\frac{3\pi}{4}i}) = x^2 - (e^{\frac{\pi}{4}i}+e^{\frac{3\pi}{4}i})x - 1 = x^2 - i\sqrt{2}x - 1$ ma $-i\sqrt{2} \notin \mathbb{Q}$.
$p_1 \cdot p_4 = (x-\alpha_1)(x-\alpha_4) = (x-e^{\frac{\pi}{4}i})(x-e^{\frac{7\pi}{4}i}) = x^2 - (e^{\frac{\pi}{4}i}+e^{\frac{7\pi}{4}i})x + 1 = x^2 - \sqrt{2}x - 1$ ma $-\sqrt{2} \notin \mathbb{Q}$.
In conclusione abbiamo provato che x^4+1 non può essere scomposto neanche come prodotto di due polinomi di secondo grado a coefficienti in $\mathbb{Q}$ e questo prova che il polinomio è irriducibile.
Di conseguenza l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1)$ ha grado 4; osserviamo inoltre che $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$ dato che $\alpha_2 = -\alpha_1$.
Proviamo ora che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1)$ è normale, dobbiamo, quindi, dimostrare che α_3 e $\alpha_4 \in \mathbb{Q}(\alpha_1)$; infatti:
$\alpha_3 = \alpha_1^3$,
$\alpha_4 = -\alpha_3$
In definitiva, abbiamo provato che l'estensione è normale e che $E = \mathbb{Q}(\alpha_1)$ è il campo di spezzamento di f su $\mathbb{Q}$, infatti su $\mathbb{Q}(\alpha_1)$ f si spezza completamente come:

$$f = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4).$$

Possiamo ripetere lo stesso ragionamento partendo dalla radice α_2, o da α_3 oppure da α_4. In definitiva si ottiene che $E = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha_3) = \mathbb{Q}(\alpha_4)$ e inoltre

$$[E : \mathbb{Q}] = 4.$$

Dimostriamo che quanto appena detto è corretto; abbiamo già provato che
$\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$, inoltre $\mathbb{Q}(\alpha_3) = \mathbb{Q}(\alpha_4)$ perchè $\alpha_4 = -\alpha_3$, e $\mathbb{Q}(\alpha_3) \subseteq \mathbb{Q}(\alpha_1)$ perchè $\alpha_3 = \alpha_1^3$.
Affinchè valga l'uguaglianza basta provare che $\alpha_1 \in \mathbb{Q}(\alpha_3)$, che è vero poichè $\alpha_1 = \alpha_3^3$.
Studiamo ora il gruppo di Galois $(E/\mathbb{Q})$ che indicheremo semplicemente con G; abbiamo, grazie alla corrispondenza di Galois, che $|G| = 4$.
Poichè il polinomio ha grado 4, G sarà un sottogruppo del gruppo delle permutazioni su quattro elementi S_4. Per capire meglio come è fatto G studiamo il discriminante di f.

$$\Delta = \begin{vmatrix} 4 & \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \\ \lambda_2 & \lambda_3 & \lambda_4 & \lambda_5 \\ \lambda_3 & \lambda_4 & \lambda_5 & \lambda_6 \end{vmatrix}$$

Calcoliamo i valori λ_i, ricordando che $\alpha_1 = -\alpha_2$ e $\alpha_3 = -\alpha_4$, e che $\alpha_i^4 = -1$ per $i = 1, 2, 3, 4$.
$\lambda_1 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$
$\lambda_2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 = e^{\frac{\pi}{2}i} + e^{\frac{5\pi}{2}i} + e^{\frac{3\pi}{2}i} + e^{\frac{7\pi}{2}i} = 2e^{\frac{\pi}{2}i} + 2e^{\frac{3\pi}{2}i} = 0$
$\lambda_3 = \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + \alpha_4^3 = \alpha_1^3 + (-\alpha_1)^3 + \alpha_3^3 + (-\alpha_3)^3 = 0$
$\lambda_4 = \alpha_1^4 + \alpha_2^4 + \alpha_3^4 + \alpha_4^4 = -1 - 1 - 1 - 1 = -4$

$\lambda_5 = \alpha_1^5 + \alpha_2^5 + \alpha_3^5 + \alpha_4^5 = \sum \alpha_i(\alpha_i^4) = -\sum \alpha_i = -\lambda_1 = 0$
$\lambda_6 = \alpha_1^6 + \alpha_2^6 + \alpha_3^6 + \alpha_4^6 = \sum \alpha_i^2(\alpha_i^4) = -\sum \alpha_i^2 = -\lambda_2 = 0.$
Quindi

$$\Delta = \begin{vmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & -4 & 0 \\ 0 & -4 & 0 & 0 \end{vmatrix} = 16^2$$

Abbiamo così dimostrato che il discriminante Δ di f ha una radice quadrata in $\mathbb{Q}$; questo ci permette di dire che :

$$G \subseteq A_4.$$

Dobbiamo quindi trovare tre permutazioni pari delle radici che insieme all'identità diano i quattro automorfismi di G. Proviamo con le permutazioni seguenti:

$$\begin{aligned} id: \quad E &\longrightarrow E \\ \alpha_1 &\mapsto \alpha_1 \\ \alpha_2 &\mapsto \alpha_2 \\ \alpha_3 &\mapsto \alpha_3 \\ \alpha_4 &\mapsto \alpha_4 \end{aligned}$$

$$\begin{aligned} (1\,2)(3\,4) = \sigma: \quad E &\longrightarrow E \\ \alpha_1 &\mapsto \alpha_2 \\ \alpha_2 &\mapsto \alpha_1 \\ \alpha_3 &\mapsto \alpha_4 \\ \alpha_4 &\mapsto \alpha_3 \end{aligned}$$

$$\begin{aligned} (1\,3)(2\,4) = \tau: \quad E &\longrightarrow E \\ \alpha_1 &\mapsto \alpha_3 \\ \alpha_2 &\mapsto \alpha_4 \\ \alpha_3 &\mapsto \alpha_1 \\ \alpha_4 &\mapsto \alpha_2 \end{aligned}$$

$$\begin{aligned} (1\,4)(2\,3) = \phi: \quad E &\longrightarrow E \\ \alpha_1 &\mapsto \alpha_4 \\ \alpha_2 &\mapsto \alpha_3 \\ \alpha_3 &\mapsto \alpha_2 \\ \alpha_4 &\mapsto \alpha_1 \end{aligned}$$

Proviamo effettivamente che σ, τ e ϕ danno degli automorfismi.
Iniziamo con il creare una base del nostro campo di spezzamento. Da quanto dimostrato precedentemente abbiamo che $E = \mathbb{Q}(\alpha_1)$ quindi una base di E è data da $\{1, \alpha_1, \alpha_1^2, \alpha_1^3\}$.
Se σ si estende ad un automorfismo del campo E, σ deve agire così:

$$\begin{aligned} \sigma: \quad E &\longrightarrow E \\ 1 &\mapsto 1 \\ \alpha_1 &\mapsto \alpha_2 \\ \alpha_1^2 &\mapsto \alpha_2^2 \\ \alpha_1^3 &\mapsto \alpha_2^3 \end{aligned}$$

Un generico elemento di E è dato da $a + b\alpha_1 + c\alpha_1^2 + d\alpha_1^3$ con $a, b, c, d \in \mathbb{Q}$.
Osserviamo come agisce σ su tale elemento:

$$\sigma(a + b\alpha_1 + c\alpha_1^2 + d\alpha_1^3) = a + b\alpha_2 + c\alpha_2^2 + d\alpha_2^3 = a - b\alpha_1 + c\alpha_1^2 - d\alpha_1^3 \tag{5.1}$$

Quindi σ è un' applicazione $\mathbb{Q}$-lineare biettiva di E in E.
Ora, proviamo che $\sigma(\beta \cdot \gamma) = \sigma(\beta)\sigma(\gamma)$ con $\beta, \gamma \in E$.
Siano $\beta = a_0 + a_1\alpha_1 + a_2\alpha_1^2 + a_3\alpha_1^3$ e $\gamma = b_0 + b_1\alpha_1 + b_2\alpha_1^2 + b_3\alpha_1^3$ con $a_i, b_i \in \mathbb{Q}$;
si ha:

$$\begin{aligned} \sigma(\beta \cdot \gamma) =& \sigma[(a_0 + a_1\alpha_1 + a_2\alpha_1^2 + a_3\alpha_1^3)(b_0 + b_1\alpha_1 + b_2\alpha_1^2 + b_3\alpha_1^3)] = \\ =& \sigma(a_0b_0 + a_0 + b_1\alpha_1 + a_0b_2\alpha_1^2 + a_0b_3\alpha_1^3 + a_1b_0\alpha_1 + a_1b_1\alpha_1^2 + \\ & a_1b_2\alpha_1^3 - a_1b_3 + a_2b_0\alpha_1^2 + a_2b_1\alpha_1^3 - a_2b_2 - \\ & a_2b_3\alpha_1 + a_3b_0\alpha_1^3 - a_3b_1 - a_3b_2\alpha_1 - a_3b_3\alpha_1^2 = \\ =& \sigma[(a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1) + (a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2)\alpha_1 + \\ & (a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3)\alpha_1^2 + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)\alpha_1^3] = \\ =& (a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1) - (a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2)\alpha_1 + \\ & (a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3)\alpha_1^2 - (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)\alpha_1^3 \end{aligned}$$

Inoltre

$$\begin{aligned} \sigma(\beta)\sigma(\gamma) =& \sigma(a_0 + a_1\alpha_1 + a_2\alpha_1^2 + a_3\alpha_1^3)\sigma(b_0 + b_1\alpha_1 + b_2\alpha_1^2 + b_3\alpha_1^3) = \\ =& (a_0 - a_1\alpha_1 + a_2\alpha_1^2 - a_3\alpha_1^3)(b_0 - b_1\alpha_1 + b_2\alpha_1^2 - b_3\alpha_1^3) = \\ =& a_0b_0 - a_0b_1\alpha_1 + a_0b_2\alpha_1^2 - a_0b_3\alpha_1^3 - a_1b_0\alpha_1 + a_1b_1\alpha_1^2 - a_1b_2\alpha_1^3 - \\ & a_1b_3 + a_2b_0\alpha_1^2 - a_2b_1\alpha_1^3 - a_2b_2 + a_2b_3\alpha_1 - a_3b_0\alpha_1^3 - \\ & a_3b_1 + a_3b_2\alpha_1 - a_3b_3\alpha_1^2 = \\ =& (a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1) - (a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2)\alpha_1 + \\ & (a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3)\alpha_1^2 - (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)\alpha_1^3 \end{aligned}$$

Abbiamo, quindi, dimostrato che σ è un automorfismo.
Inoltre $\sigma(\alpha_2) = \sigma(-\alpha_1) = -\sigma(\alpha_1) = -\alpha_2 = \alpha_1$;
$\alpha_3 = \alpha_1^3$ quindi $\sigma(\alpha_3) = \sigma(\alpha_1^3) = \alpha_2^3 = (-\alpha_1)^3 = -\alpha_1^3 = \alpha_4$;
$\alpha_4 = -\alpha_3$ quindi $\sigma(\alpha_4) = \sigma(-\alpha_3) = -\sigma(\alpha_3) = -\alpha_4 = \alpha_3$.

Facciamo ora lo stesso con τ.
Vediamo come agisce τ, nel caso si estenda ad un automorfismo, sugli elementi della base fissata di E.

$$\begin{aligned} \tau: \quad E &\longrightarrow E \\ 1 &\mapsto 1 \\ \alpha_1 &\mapsto \alpha_3 \\ \alpha_1^2 &\mapsto \alpha_3^2 \\ \alpha_1^3 &\mapsto \alpha_3^3 \end{aligned}$$

Quindi τ su un generico elemento di E deve lavorare in questo modo:

$$\begin{aligned} \tau(a + b\alpha_1 + c\alpha_1^2 + d\alpha_1^3) =& a + b\alpha_3 + c\alpha_3^2 + d\alpha_3^3 = a + b\alpha_1^3 + c\alpha_1^6 + d\alpha_1^9 = \\ =& a + b\alpha_1^3 - c\alpha_1^2 + d\alpha_1 = a + d\alpha_1 - c\alpha_1^2 + b\alpha_1^3 \end{aligned} \tag{5.2}$$

Quindi questa τ è $\mathbb{Q}$-lineare e biettiva.
Ora, proviamo che $\tau(\beta \cdot \gamma) = \tau(\beta)\tau(\gamma)$ con $\beta, \gamma \in E$,
$\beta = a_0 + a_1\alpha_1 + a_2\alpha_1^2 + a_3\alpha_1^3$ e $\gamma = b_0 + b_1\alpha_1 + b_2\alpha_1^2 + b_3\alpha_1^3$ con $a_i, b_i \in \mathbb{Q}$:

$$\begin{aligned} \tau(\beta \cdot \gamma) =& \tau[(a_0 + a_1\alpha_1 + a_2\alpha_1^2 + a_3\alpha_1^3)(b_0 + b_1\alpha_1 + b_2\alpha_1^2 + b_3\alpha_1^3)] = \\ =& \tau[(a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1) + (a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2)\alpha_1 + \\ & (a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3)\alpha_1^2 + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)\alpha_1^3] = \\ =& (a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1) + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)\alpha_1 - \\ & (a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3)\alpha_1^2 + (a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2)\alpha_1^3 \end{aligned}$$

Inoltre

$$\begin{aligned} \tau(\beta)\tau(\gamma) =& \tau(a_0 + a_1\alpha_1 + a_2\alpha_1^2 + a_3\alpha_1^3)\tau(b_0 + b_1\alpha_1 + b_2\alpha_1^2 + b_3\alpha_1^3) = \\ =& (a_0 + a_3\alpha_1 - a_2\alpha_1^2 + a_1\alpha_1^3)(b_0 + b_3\alpha_1 - b_2\alpha_1^2 + b_1\alpha_1^3) = \\ =& a_0b_0 + a_0b_3\alpha_1 - a_0b_2\alpha_1^2 + a_0b_1\alpha_1^3 + a_3b_0\alpha_1 + a_3b_3\alpha_1^2 - a_3b_2\alpha_1^3 - a_3b_1 - \\ & a_2b_0\alpha_1^2 - a_2b_3\alpha_1^3 - a_2b_2 + a_2b_1\alpha_1 + a_1b_0\alpha_1^3 - a_1b_3 + a_1b_2\alpha_1 - a_1b_1\alpha_1^2 = \\ =& (a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1) + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)\alpha_1 - \\ & (a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3)\alpha_1^2 + (a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2)\alpha_1^3 \end{aligned}$$

Abbiamo,quindi, dimostrato che τ è un automorfismo.
Inoltre $\tau(\alpha_2) = \tau(-\alpha_1) = -\tau(\alpha_1) = -\alpha_3 = \alpha_4$;

$\tau(\alpha_3) = \tau(\alpha_1^3) = \alpha_3^3 = \alpha_1$;
$\tau(\alpha_4) = \tau(-\alpha_3) = -\tau(\alpha_3) = -\alpha_1 = \alpha_2$.

Si ha quindi che $\sigma\tau$ è pure un automorfismo di E; e $\sigma\tau$ agisce sulle radici $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ come ϕ.
Abbiamo quindi provato che le quattro permutazioni danno degli automorfismi id, σ, τ, ϕ e poichè $|G| = 4, G = \{id, \sigma, \tau, \phi\}$.
É facile, ora, osservare che gli automorfismi σ, τ e ϕ hanno tutti ordine 2, in definitiva, G è un gruppo di quattro elementi di cui tre hanno ordine 2.
In conclusione:

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Osserviamo che $|G| = 4$, quindi, necessariamente un sottogruppo non banale ha ordine 2; quindi ci sono esattamente tre sottogruppi non banali:
$H_1 =< \sigma >$, $H_2 =< \tau >$ e $H_3 =< \phi >$

Studiamo, ora, questi sottogruppi.
Consideriamo anzitutto H_1.
Da 5.1 vediamo che se $v = a + b\alpha_1 + c\alpha_1^2 + d\alpha_1^3$ è fissato da σ, deve essere $a + b\alpha_1 + c\alpha_1^2 + d\alpha_1^3 = a - b\alpha_1 + c\alpha_1^2 - d\alpha_1^3$ e per l'unicità della scrittura di v come combinazione lineare degli elementi della base scelta, questo equivale a dire che $b = 0, d = 0$.
Cioè, σ lascia fissi gli elementi del tipo $a + c\alpha_1^2 = a + ci$ con $a, c \in \mathbb{Q}$, ovvero gli elementi di $\mathbb{Q}(i)$.
Dopo questa osservazione possiamo facilmente individuare il campo fisso di H_1:
$H_1^* = \{v \in E | h(v) = v \quad \forall h \in H_1\} = \{v \in E | \sigma(v) = v\}$, quindi

$$H_1^* = \mathbb{Q}(i).$$

Osserviamo che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(i)$ ha grado 2 poichè il polinomio minimo di i su $\mathbb{Q}$ è $x^2 + 1$, di conseguenza per il teorema della torre si ottiene che $[E : \mathbb{Q}(i)] = 2$.

Consideriamo ora H_2.
Si ha:
$H_2^* = \{v \in E | h(v) = v \quad \forall h \in H_2\} = \{v \in E | \tau(v) = v\}$
Ma, per 5.2, se $v = a + b\alpha_1 + c\alpha_1^2 + d\alpha_1^3$,

$$\tau(v) = v \quad \text{se e solo se } c = 0,\ b = d.$$

Cioè, τ lascia fissi gli elementi del tipo $a + b(\alpha_1 + \alpha_3) = a + b(i\sqrt{2})$ con $a, b \in \mathbb{Q}$, ovvero tutti e soli gli elementi di $\mathbb{Q}(i\sqrt{2})$.
In conclusione:

$$H_2^* = \mathbb{Q}(i\sqrt{2}).$$

Osserviamo che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(i\sqrt{2})$ ha grado 2 poichè il polinomio minimo di $i\sqrt{2}$ su $\mathbb{Q}$ è $x^2 + 2$, di conseguenza per il teorema della torre si ottiene che $[E : \mathbb{Q}(i\sqrt{2})] = 2$.

Consideriamo ora H_3.
Vediamo come agisce ϕ sugli elementi della base di E.

$$\begin{aligned} \phi: \quad E &\longrightarrow E \\ 1 &\mapsto 1 \\ \alpha_1 &\mapsto \alpha_4 \\ \alpha_1^2 &\mapsto \alpha_4^2 \\ \alpha_1^3 &\mapsto \alpha_4^3 \end{aligned}$$

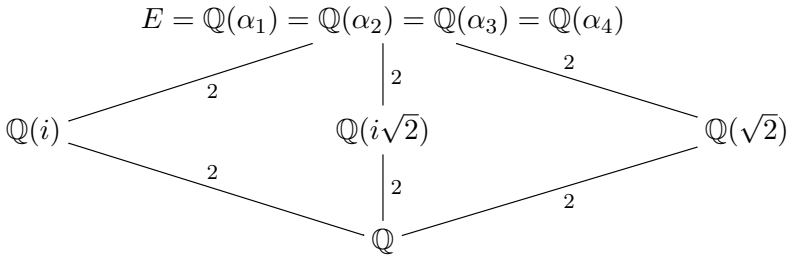
Consideriamo un generico elemento v in $\mathbb{Q}(\alpha_1)$, questo sarà della forma:
$v = a + b\alpha_1 + c\alpha_1^2 + d\alpha_1^3 \quad$ con $a, b, c, d \in \mathbb{Q}$
e verrà mandato da ϕ in:
$\phi(v) = a + b\alpha_4 + c\alpha_4^2 + d\alpha_4^3 = a - d\alpha_1 - c\alpha_1^2 - b\alpha_1^3$.
Dopo questa osservazione possiamo facilmente individuare il campo fisso di H_3:
$H_3^* = \{v \in E | h(v) = v \quad \forall h \in H_3\} = \{v \in E | \phi(v) = v\}$.
Per quanto visto prima, si ha che:

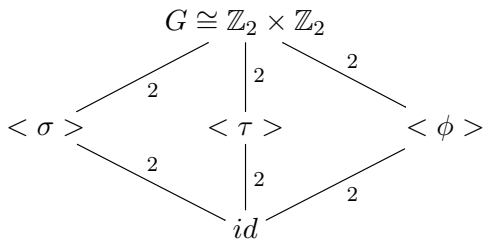
$$\phi(v) = v \quad \text{se e solo se } b = -d,\ c = 0.$$

Cioè, ϕ lascia fissi tutti e soli gli elementi del tipo $a+b\alpha_1-b\alpha_1^3 = a+b(\alpha_1+\alpha_4) = a+b\sqrt{2}$ con $a, b \in \mathbb{Q}$, ovvero gli elementi di $\mathbb{Q}(\sqrt{2})$. In conclusione:

$$H_3^* = \mathbb{Q}(\sqrt{2}).$$

Concludiamo il nostro studio mostrando graficamente la corrispondenza trovata.





Bibliografia

[1] P.M. Cohn: *Algebra, volume 2*, John Wiley & Sons Ltd, 1989

[2] David A. Cox: *Galois Theory*, Wiley-Interscience, 2004

[3] D.J.H Garling: *A Course in Galois Theory*, Cambridge University Press, 1995

[4] M. Idà: *Note del corso di Algebra 2*, Bologna, 2012/13

[5] J.S. Milne: *Fields and Galois Theory*, On-line lecture notes, with exercises, 2014

[6] E. Sernesi: *Geometria 1*, Bollati Boringhieri, 1989

[7] A. Vistoli: *Note di Algebra* ,Bologna, 1993/94

Ringraziamenti

Vorrei ringraziare in primis la mia famiglia senza la quale tutto questo non sarebbe stato possibile.
Mamma e papà siete stati voi che seppur con sacrifici mi avete dato la possibilità di fare questa esperienza, siete stati voi a credere in me sin dall'inizio quando io ancora pensavo che questo giorno potesse mai arrivare, siete stati voi a soffrire con me nelle sconfitte e a gioire nelle vittorie; per tutto questo GRAZIE!
In particolare tu, mamma, sei la madre che ogni figlio vorrebbe avere!!
Poi, vorrei ringraziare Fabrizio, il quale ha vissuto in prima persona la mia esperienza. Grazie perché non mi hai fatto mai perdere d'animo, hai sempre cercato di far emergere il lato positivo delle cose, sei stato sempre con me nei momenti difficili , quando tutte le aspettative, tutti i sogni, sembravano crollare tu eri lì vicino a me ripetendo costantemente la frase ' Io credo in te! '. Grazie perché sei stato la persona che desideravo e desidero tutt'ora avere al mio fianco, il ragazzo con il quale voglio ancora condividere gioie e dolori! TI AMO!
Vorrei, poi, ringraziare i miei amici che seppur lontani fisicamente mi hanno fatto capire di essere vicini a me, ogni giorno, con il cuore! Quindi grazie di cuore a: Francesca, Stefano, Ambra, Cristina, Elena, Federica, Flavia, Giusy, Marta, Sara e Silvia!
VI VOGLIO BENE!
Inoltre, vorrei ringraziare tutte le persone che ho incontrato in questo cammino e che hanno reso ogni giorno migliore!
Infine, ma non per importanza, vorrei ringraziare la professoressa Monica Idà che mi ha seguito durante questi mesi sempre con grande pazienza, insegnandomi che preparazione e competenza non escludono per forza generosità e simpatia. I suoi consigli e la sua estrema disponibilità sono stati i pilastri che hanno reso possibile la realizzazione di questo lavoro.
Grazie di cuore a tutti voi!