Università Cattolica del Sacro Cuore

Sede di Brescia

Facoltà di Scienze Matematiche, Fisiche e Naturali

CORSO DI ISTITUZIONI DI ALGEBRA SUPERIORE I

prof. Clara Franchi

Esercizi svolti

raccolti da Elena Rossi

Anno Accademico 2009-2010

Esercizi

1. Si determinino il polinomio minimo di $\sqrt[3]{5}$ su $\mathbb{Q}$, il grado dell'estensione $\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}$ e una sua base.

Svolgimento.
Il polinomio $x^3 - 5$ ha come radici $\sqrt[3]{5}$, $\omega\sqrt[3]{5}$, $\omega^2\sqrt[3]{5}$ con $\omega = e^{\frac{2}{3}\pi i} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.
Il polinomio minimo di $\sqrt[3]{5}$ è proprio $x^3 - 5$: infatti è monico, irriducibile in $\mathbb{Q}[x]$ per il Criterio di Eisenstein, con $p = 5$, e ammette $\sqrt[3]{5}$ come radice.
Per il Teorema di Struttura delle estensioni semplici:

$$|\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}| = \deg(x^3 - 5) = 3$$

e quindi $\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}$ è un'estensione algebrica di grado 3.
Una sua base è : $\mathcal{B} = \{1, \sqrt[3]{5}, \sqrt[3]{25}\}$
e $\mathbb{Q}(\sqrt[3]{5}) = \{a + b\sqrt[3]{5} + c\sqrt[3]{25} | a, b, c \in \mathbb{Q}\}$. $\square$

2. Dimostrare che $\mathbb{Q}(1 + \sqrt{3}) = \mathbb{Q}(\sqrt{3})$

Svolgimento.
Si ha che $1 + \sqrt{3} \in \mathbb{Q}(\sqrt{3})$ perchè $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} | a, b \in \mathbb{Q}\}$.
Inoltre $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$. Ne segue: $\mathbb{Q}(1 + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3})$.
Viceversa $\sqrt{3} = (1 + \sqrt{3}) - 1 \in \mathbb{Q}(1 + \sqrt{3})$ e $\mathbb{Q} \subseteq \mathbb{Q}(1 + \sqrt{3})$.
Allora $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(1 + \sqrt{3})$. $\square$

Osservazione: per ogni $\alpha \in \mathbb{Q}$, $\mathbb{Q}(\alpha) = \mathbb{Q}$: infatti $\mathbb{Q}(\alpha)$ è il piú piccolo campo contenente $\mathbb{Q}$ ed α, e quindi è $\mathbb{Q}$.

3. Provare che $\mathbb{Q}(\sqrt{6}, \sqrt{7}) = \mathbb{Q}(\sqrt{6} - \sqrt{7})$

Svolgimento.
$(\supseteq)$ $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{6}, \sqrt{7})$. Inoltre $\sqrt{6} - \sqrt{7} \in \mathbb{Q}(\sqrt{6}, \sqrt{7})$ perchè è ottenuto da due elementi di $\mathbb{Q}(\sqrt{6}, \sqrt{7})$ mediante un'operazione di campo.

Allora $\mathbb{Q}(\sqrt{6}-\sqrt{7}) \subseteq \mathbb{Q}(\sqrt{6},\sqrt{7})$.
$(\subseteq)$ Sia $u := \sqrt{6}-\sqrt{7}$. Allora: $u+\sqrt{7}=\sqrt{6}$. Eleviamo al quadrato:

$$(u+\sqrt{7})^2 = (\sqrt{6})^2 \Longrightarrow u^2+2u\sqrt{7}+7=6 \Longrightarrow$$

$$2u\sqrt{7} = -u^2-1 \Longrightarrow \sqrt{7} = \frac{-u^2-1}{2u} \in \mathbb{Q}(u) = \mathbb{Q}(\sqrt{6}-\sqrt{7}).$$

Allora si ha anche $\sqrt{6} = u+\sqrt{7} \in \mathbb{Q}(u)$. Ovviamente $\mathbb{Q} \subseteq \mathbb{Q}(u)$. Quindi $\mathbb{Q}(\sqrt{6},\sqrt{7}) \subseteq \mathbb{Q}(\sqrt{6}-\sqrt{7})$. $\square$

4. Determinare il grado di $\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}$ e il polinomio minimo di $\sqrt[3]{2}+i$ su $\mathbb{Q}$. Dimostrare che $\mathbb{Q}(\sqrt[3]{2}, i) = \mathbb{Q}(\sqrt[3]{2}+i)$.

Svolgimento.
Per la formula dei gradi:

$$|\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}| = |\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[3]{2})||\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}|$$

$$\begin{tikzcd} \mathbb{Q}(\sqrt[3]{2}, i) \arrow[d, no head] \\ \mathbb{Q}(\sqrt[3]{2}) \arrow[d, no head] \\ \mathbb{Q} \end{tikzcd}$$

- $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ perchè $\min_{\mathbb{Q},\sqrt[3]{2}}(x) = x^3-2$ (il polinomio è irriducibile per il Criterio di Eisenstein e ammette $\sqrt[3]{2}$ come radice).

- $|\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[3]{2})| =?$
  Cerchiamo il polinomio minimo $\min_{\mathbb{Q}(\sqrt[3]{2}),i}(x)$.
  Sicuramente x^2+1 è irriducibile in $\mathbb{Q}[x]$. Esso è irriducibile anche in $\mathbb{Q}(\sqrt[3]{2})[x]$: infatti, se non lo fosse, sarebbe il prodotto di due fattori di primo grado, cioè

  $$x^2+1 = (x-x_1)(x-x_2) = (x-i)(x+i)$$

  da cui seguirebbe $i \in \mathbb{Q}(\sqrt[3]{2})$, il che è assurdo perchè $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.
  Allora $\min_{\mathbb{Q}(\sqrt[3]{2}),i}(x) = x^2+1$ e quindi $|\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[3]{2})| = 2$.

Ne segue $|\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}| = 3 \cdot 2 = 6$.

Proviamo che $\mathbb{Q}(\sqrt[3]{2}, i) = \mathbb{Q}(\sqrt[3]{2} + i)$

($\supseteq$) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, i)$. Inoltre $\sqrt[3]{2} + i \in \mathbb{Q}(\sqrt[3]{2}, i)$ perchè è ottenuto da due elementi di $\mathbb{Q}(\sqrt[3]{2}, i)$ mediante un'operazione di campo.

Allora $\mathbb{Q}(\sqrt[3]{2} + i) \subseteq \mathbb{Q}(\sqrt[3]{2}, i)$.

($\subseteq$) Sia $u := \sqrt[3]{2} + i$. Allora: $u - i = \sqrt[3]{2}$. Eleviamo al cubo:

$$(u - i)^3 = (\sqrt[3]{2})^3 \Longrightarrow u^3 - 3u^2 i - 3u + i = 2 \Longrightarrow$$

$$i(3u^2 - 1) = u^3 - 3u - 2 \Longrightarrow i = \frac{u^3 - 3u - 2}{3u^2 - 1} \in \mathbb{Q}(u) = \mathbb{Q}(\sqrt[3]{2} + i).$$

Allora si ha anche $\sqrt[3]{2} = u - i \in \mathbb{Q}(u)$. Ovviamente $\mathbb{Q} \subseteq \mathbb{Q}(u)$. Quindi $\mathbb{Q}(\sqrt[3]{2}, i) \subseteq \mathbb{Q}(u) = \mathbb{Q}(\sqrt[3]{2} + i)$.

Sappiamo che $\deg(\min_{\mathbb{Q}, \sqrt[3]{2}+i}(x)) = |\mathbb{Q}(\sqrt[3]{2} + 1) : \mathbb{Q}| = 6$. Sia $u := \sqrt[3]{2} + i$. Per quanto visto prima abbiamo $u^3 - 3u - 2 = (3u^2 - 1)i$. Eleviamo al quadrato:

$$u^6 + 9u^2 + 4 - 6u^4 - 4u^3 + 12u = -(9u^4 - 6u^2 + 1)$$

$$u^6 + 3u^4 - 4u^3 + 3u^2 + 12u + 5 = 0$$

Poniamo $p(x) = x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5$, allora $p(u) = 0$.

Il polinomio minimo è monico, divide $p(x)$ ed ha grado 6: allora $p(x) = \min_{\mathbb{Q}, \sqrt[3]{2}+i}(x)$.

$\square$

5. Provare che $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

Svolgimento.

$|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ perchè $\min_{\mathbb{Q}, \sqrt[3]{2}}(x) = x^3 - 2$.

$|\mathbb{Q}(\sqrt{2} : \mathbb{Q}| = 2$ perchè $\min_{\mathbb{Q}, \sqrt{2}}(x) = x^2 - 2$.

Se fosse $\sqrt{2} \in \mathbb{Q}(\sqrt[3]{2})$ si dovrebbe avere $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| \big| |\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}|$: assurdo. $\square$

6. Siano $K \leq L \leq M$ e $[M : K] < \infty$. Mostrare che:

1. se $|M : K| = |L : K| \Rightarrow M = L$;

2. se $|M : L| = |M : K| \Rightarrow L = K$.

Svolgimento.

Per la formula dei gradi: $|M : K| = |M : L||L : K|$

1. Se $|M : K| = |L : K|$, semplificando abbiamo $|M : L| = 1$.
   Allora $\exists v \in M, v \neq 0$ tale che $\{v\}$ è base per M su L. Quindi $M = Lv$. Dato che M è un campo, v è invertibile e $L = Mv^{-1}$. Quindi L è un ideale non nullo di M. Poichè gli ideali di un campo sono solo $\{0_M\}$ e M si ha che $L = M$.

2. Se $|M : L| = |M : K|$, semplificando abbiamo $|L : K| = 1 \Longrightarrow L = K$.

$\square$

7. Siano $K \leq L_1, L_2 \leq M$. Supponiamo $|L_i : K| = n_i, i = 1, 2$. Provare che:

1. $|L_1 \cap L_2 : K|$ divide $(n_1, n_2) = d$.

2. $| < L_1, L_2 >: L_i| \leq n_j$ con $i \neq j$.

3. se $(n_1, n_2) = 1$, allora $L_1 \cap L_2 = K$ e $| < L_1, L_2 >: K| = n_1 n_2$.

Svolgimento.

1. Poniamo $|L_1 \cap L_2 : K| = m$.
   $|L_1 : K| = |L_1 : L_1 \cap L_2||L_1 \cap L_2 : K| \Longrightarrow m|n_1$
   $|L_2 : K| = |L_2 : L_1 \cap L_2||L_1 \cap L_2 : K| \Longrightarrow m|n_2$
   Per la definizione di MCD: $m|n_1$ e $m|n_2 \Longrightarrow m|d$.

2. Vogliamo dimostrare che $| < L_1, L_2 >: L_1| \leq n_2$. Poniamo $R =< L_1, L_2 >$.
   Poichè $|L_2 : K| = n_2$ si ha che $L_2 = K(\alpha_1, \ldots, \alpha_r)$ per qualche $\alpha_i \in L_2$, $i = 1, \ldots, r$. Allora $R = L_1(\alpha_1, \ldots, \alpha_r)$ (R è il piú piccolo campo contenente L_1 e L_2.)

Procediamo per induzione su r.

Se $r=1$: $L_2 = K(\alpha_1)$ e $R = L_1(\alpha_1)$. Si ha che $|R : L_1| = \deg(\min{}_{L_1,\alpha_1}(x))$, $|L_2 : K| = \deg(\min{}_{K,\alpha_1}(x))$. Sappiamo che $\min{}_{K,\alpha_1}(x)$ è un polinomio a coefficienti in $K \subseteq L_1$ che si annulla in α_1. Allora $\min{}_{L_1,\alpha_1}(x) | \min{}_{K,\alpha_1}(x)$ e quindi $\deg(\min{}_{L_1,\alpha_1}(x)) \leq \deg(\min{}_{K,\alpha_1}(x)) = n_2$.

Sia ora $r > 1$. L'ipotesi induttiva è : $|L_1(\alpha_1, \ldots, \alpha_{r-1}) : L_1| \leq |K(\alpha_1, \ldots, \alpha_{r-1}) : K|$

Si ha che $R = L_1(\alpha_1, \ldots, \alpha_r) = L_1(\alpha_1, \ldots, \alpha_{r-1})(\alpha_r)$. Ripetendo il ragionamento fatto si ha $\deg(\min{}_{L_1(\alpha_1,\ldots,\alpha_{r-1}),\alpha_r}(x)) \leq \deg(\min{}_{K(\alpha_1,\ldots,\alpha_{r-1}),\alpha_r}(x))$.

Per la formula dei gradi si ha:

$$\begin{aligned}
|R : L_1| &= |L_1(\alpha_1, \ldots, \alpha_r) : L_1(\alpha_1, \ldots, \alpha_{r-1})||L_1(\alpha_1, \ldots, \alpha_{r-1}) : L_1| \leq \\
&\leq \deg(\min{}_{L_1(\alpha_1,\ldots,\alpha_{r-1}),\alpha_r}(x))|K(\alpha_1, \ldots, \alpha_{r-1}) : K| \leq \\
&\leq \deg(\min{}_{K(\alpha_1,\ldots,\alpha_{r-1}),\alpha_r}(x))|K(\alpha_1, \ldots, \alpha_{r-1}) : K| = \\
&= |K(\alpha_1, \ldots, \alpha_r) : K(\alpha_1, \ldots, \alpha_{r-1})||K(\alpha_1, \ldots, \alpha_{r-1}) : K| = \\
&= |K(\alpha_1, \ldots, \alpha_r) : K| = |L_2 : K| = n_2.
\end{aligned}$$

3. Per il punto (1) : $|L_1 \cap L_2 : K| \big| (n_1, n_2) = 1 \Longrightarrow L_1 \cap L_2 = K$.

   $x = |< L_1, L_2 >: K| = |< L_1, L_2 >: L_i||L_i : K|$ e quindi $n_i | x$ per $i = 1, 2$.

   MCD$(n_1, n_2) = 1 \Longrightarrow n_1 n_2 | x \Longrightarrow x \geq n_1 n_2$.

   Inoltre per il punto (2) abbiamo che:

   $x = |< L_1, L_2 >: K| = |< L_1, L_2 >: L_2||L_2 : K| \leq n_1 n_2$

   Allora $x = n_1 n_2$.

$\square$

8. Sia $L : K$ un'estensione, $|L : K| = p$ primo. Dimostrare che se H è un campo intermedio tra K e L ($K \leq H \leq L$) allora o $H = K$ o $H = L$.

Svolgimento.

$p = |L : K| = |L : H||H : K| = ab$

Poichè $p \in \mathbb{Z}$ è primo i suoi unici divisori positivi sono 1 e p. Quindi si ha:

$$a = 1 \Longrightarrow |L : H| = 1 \Longrightarrow H = L$$

oppure

$$b = 1 \Longrightarrow |H : K| = 1 \Longrightarrow H = K.$$

$\square$

9. Sia $\alpha \in \mathbb{C}$ tale che $\min_{\mathbb{Q},\alpha}(x) = x^2 + x + 1$. Mostrare che $\alpha^2 - 1 \neq 0$. Scrivere l'elemento $\frac{\alpha^2+1}{\alpha^2-1} \in \mathbb{Q}(\alpha)$ nella forma $a + b\alpha$, con $a, b \in \mathbb{Q}$.

Svolgimento.

Si ha che $\alpha^2 + \alpha + 1 = 0$. Se per assurdo fosse $\alpha^2 - 1 = 0 \Longrightarrow \alpha^2 = 1 \Longrightarrow \alpha = \pm 1$

Allora si avrebbe

$$\alpha^2 + \alpha + 1 = \begin{cases} 3 & \text{se } \alpha = +1 \\ 1 & \text{se } \alpha = -1 \end{cases} \quad \Longrightarrow \quad \neq 0.$$

Quindi necessariamente $\alpha^2 - 1 \neq 0$.

$\mathbb{Q}(\alpha)$ è un'estensione semplice e $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 2$, base $\{1, \alpha\}$.

$\alpha^2 = -\alpha - 1$

$$\frac{\alpha^2 + 1}{\alpha^2 - 1} = \frac{-\alpha - 1 + 1}{-\alpha - 1 - 1} = \frac{-\alpha}{-\alpha - 2} = \alpha(\alpha + 2)^{-1}$$

Per calcolare $(\alpha + 2)^{-1}$ dividiamo $x^2 + x + 1$ per $x + 2$: otteniamo

$$x^2 + x + 1 = (x + 2)(x - 1) + 3.$$

Sostituiamo α: $\quad 0 = (\alpha + 2)(\alpha - 1) + 3 \quad \Longrightarrow \quad -3 = (\alpha + 2)(\alpha - 1)$

Dividiamo per -3:

$$\frac{(\alpha + 2)(\alpha - 1)}{-3} = 1 \qquad \Rightarrow \qquad (\alpha + 2)^{-1} = \frac{(1 - \alpha)}{3}$$

Allora otteniamo:

$$\frac{\alpha^2 + 1}{\alpha^2 - 1} = \alpha(\alpha + 2)^{-1} = \alpha\frac{(1 - \alpha)}{3} = \frac{(\alpha - \alpha^2)}{3} = \frac{(\alpha + \alpha + 1)}{3} = \frac{1}{3} + \frac{2}{3}\alpha.$$

$\square$

10. Sia $u = 2i + \sqrt[3]{5} \in \mathbb{C}$.

1. Si verifichi che $i \in \mathbb{Q}(u)$ e si concluda che $\mathbb{Q}(u) = \mathbb{Q}(\sqrt[3]{5}, i)$.

2. Calcolare $|\mathbb{Q}(u) : \mathbb{Q}|$, $|\mathbb{Q}(u) : \mathbb{Q}(\sqrt[3]{5})|$, $|\mathbb{Q}(u) : \mathbb{Q}(i)|$.

3. Determinare i polinomi minimi $\min_{\mathbb{Q}(\sqrt[3]{5}),u}(x)$ e $\min_{\mathbb{Q}(i),u}(x)$.

Svolgimento.

1. $u = 2i + \sqrt[3]{5} \quad \Rightarrow u - 2i = \sqrt[3]{5} \quad \Rightarrow (u-2i)^3 = 5$
   $\Rightarrow u^3 - 6iu^2 - 12u + 8i = 5 \quad \Rightarrow i(8 - 6u^2) = 5 + 12u - u^3 \quad \Rightarrow$
   $$i = \frac{5 + 12u - u^3}{8 - 6u^2} \in \mathbb{Q}.$$
   $\sqrt[3]{5} = u - 2i \in \mathbb{Q}(u)$. Quindi $\mathbb{Q}(\sqrt[3]{5}, i) \subseteq \mathbb{Q}(u)$.
   Viceversa $\mathbb{Q}(u) \subseteq \mathbb{Q}(\sqrt[3]{5}, i)$ perchè $u \in \mathbb{Q}(\sqrt[3]{5}, i)$.
   Dunque $\mathbb{Q}(\sqrt[3]{5}, i) = \mathbb{Q}(u)$.

2. Poichè $\min_{\mathbb{Q},\sqrt[3]{5}}(x) = x^3 - 5$, si ha che $|\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}| = 3$.
   Poichè $\min_{\mathbb{Q},i}(x) = x^2 + 1$, si ha che $|\mathbb{Q}(i) : \mathbb{Q}| = 2$.
   Poichè $\mathrm{MCD}(2,3) = 1$ per l'esercizio (7.3) si ha che $\mathbb{Q}(\sqrt[3]{5}) \cap \mathbb{Q}(i) = \mathbb{Q}$ e, poichè $\mathbb{Q}(u) = \mathbb{Q}(\sqrt[3]{5}, i)$, $|\mathbb{Q}(u) : \mathbb{Q}| = 6$.

3. $u = 2i + \sqrt[3]{5} \quad \Rightarrow u - \sqrt[3]{5} = 2i \quad \Rightarrow (u - \sqrt[3]{5})^2 = -4 \quad \Rightarrow$
   $u^2 - 2u\sqrt[3]{5} + \sqrt[3]{25} = -4$
   Sia $p(x) = x^2 - 2x\sqrt[3]{5} + \sqrt[3]{25} + 4$: $p(x) \in \mathbb{Q}(\sqrt[3]{5})[x]$, è monico e si annulla in u.
   Per la formula dei gradi si ha che $|\mathbb{Q}(u) : \mathbb{Q}(\sqrt[3]{5})| = 2 = \deg(\min_{\mathbb{Q}(\sqrt[3]{5}),u}(x))$.
   Quindi $p(x)$ è irriducibile in $\mathbb{Q}(\sqrt[3]{5})[x]$. Allora:
   $$\min_{\mathbb{Q}(\sqrt[3]{5}),u}(x) = p(x) = x^2 - 2x\sqrt[3]{5} + \sqrt[3]{25} + 4.$$
   Dal punto 1. sappiamo che $u^3 - 6iu^2 - 12u + 8i = 5$. Sia
   $$p(x) = x^3 - 6ix^2 - 12x + 8i - 5.$$

$p(x) \in \mathbb{Q}(i)$, è monico e si annulla in u. Per la formula dei gradi si ha che $3 = |\mathbb{Q}(u) : \mathbb{Q}(i)| = \deg(\min_{\mathbb{Q}(i),u}(x))$ e quindi $p(x)$ è irriducibile in $\mathbb{Q}(i)[x]$. Allora:

$$\min_{\mathbb{Q}(i),u} = p(x) = x^3 - 6ix^2 - 12x + 8i - 5.$$

$\square$

11. Calcolare $\min_{\mathbb{Q},\sqrt{2}+\sqrt{5}}(x)$.

Svolgimento.
Sia $u = \sqrt{2} + \sqrt{5} \quad \Rightarrow u^2 = (\sqrt{2} + \sqrt{5})^2 = 2 + 5 + 2\sqrt{10} \quad \Rightarrow$
$u^2 - 7 = 2\sqrt{10} \quad \Rightarrow u^4 - 14u^2 + 49 = 40 \quad \Rightarrow u^4 - 14u^2 + 9 = 0.$
Poniamo

$$p(x) = x^4 - 14x^2 + 9$$

$p(x) \in \mathbb{Q}[x]$, è monico e si annulla su $u = \sqrt{2} + \sqrt{5}$. Verifichiamo che $p(x)$ non ha radici in $\mathbb{Q}$ e quindi non ha fattori di primo grado.
Poniamo $t = x^2$. Allora $t_{1,2} = 7 \pm \sqrt{40} = 7 \pm 2\sqrt{10}$.
Quindi $x_{1,2,3,4} = \pm\sqrt{7 \pm 2\sqrt{10}} \notin \mathbb{Q}$.
Verifichiamo che $p(x)$ non è decomponibile in fattori di secondo grado. Siano $a, b, c, d \in \mathbb{Q}$ tali che:

$$\begin{aligned} x^4 - 14x^2 + 9 &= (x^2 + ax + b)(x^2 + cx + d) = \\ &= x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd \end{aligned}$$

$$\begin{cases} a + c = 0 \\ b + ac + d = -14 \\ ad + bc = 0 \\ bd = 9 \end{cases} \quad \Rightarrow \quad \begin{cases} c = -a \\ b + d - a^2 = 14 \\ a(d - b) = 0 \\ bd = 9 \end{cases}$$

Per il Lemma di Gauss, un polinomio monico a coefficienti interi è irriducibile in $\mathbb{Q}[x]$ se e solo se lo è in $\mathbb{Z}[x]$. Quindi possiamo assumere che $a, b, c, d \in \mathbb{Z}$. Allora:

- se $a = 0$, abbiamo

$$\begin{cases} c = 0 \\ b + d = -14 \\ bd = 9 \end{cases} \quad \Rightarrow \quad \begin{array}{l} d = -b - 14 \\ b^2 + 14b + 9 = 0 \end{array}$$

  Quindi $b_{1,2} = -7 \pm \sqrt{40} \notin \mathbb{Z}$: contraddizione.

- se $b-d=0$, abbiamo

$$\begin{cases} b=d \\ c=-a \\ b^2=9 \\ 2b-a^2=-14 \end{cases} \Rightarrow \begin{cases} b=\pm 3 \\ d=\pm 3 \\ a^2=14+2b=\begin{cases} 14+6=20 & \text{se } b=3 \\ 14-6=8 & \text{se } b=-3 \end{cases} \end{cases}$$

  Quindi $a \notin \mathbb{Z}$: contraddizione.

Allora $p(x)$ è irriducibile in $\mathbb{Q}[x]$: è il polinomio minimo

$$\min{}_{\mathbb{Q},\sqrt{2}+\sqrt{5}}(x)=x^4-14x^2+9.$$

Osservazione: le radici del polinomio x^4-14x^2+9 sono

$$\pm(\sqrt{2}\pm\sqrt{5})=\pm\sqrt{7\pm 2\sqrt{10}}$$

Infatti: $7\pm 2\sqrt{10}=2+5\pm 2\sqrt{10}=(\sqrt{2}\pm\sqrt{5})^2$

$\square$

12. Scrivere gli elementi di $\operatorname{Gal}(\mathbb{Q}(\sqrt{2}+\sqrt{5}):\mathbb{Q})$.

Svolgimento.

Per l'esercizio precedente sappiamo che

$$\min{}_{\mathbb{Q},\sqrt{2}+\sqrt{5}}(x)=x^4-14x^2+9$$

e le sue radici sono $\pm(\sqrt{2}\pm\sqrt{5})$.
Una base di $\mathbb{Q}(\sqrt{2}+\sqrt{5}):\mathbb{Q}$ come $\mathbb{Q}$-spazio vettoriale è :

$$1, \sqrt{2}+\sqrt{5}, (\sqrt{2}+\sqrt{5})^2, (\sqrt{2}+\sqrt{5})^3$$

Quindi

$$\mathbb{Q}(\sqrt{2}+\sqrt{5})=\{a+b(\sqrt{2}+\sqrt{5})+c(\sqrt{2}+\sqrt{5})^2+d(\sqrt{2}+\sqrt{5})^3 | a,b,c,d\in\mathbb{Q}\}$$

Gli elementi di $\operatorname{Gal}(\mathbb{Q}(\sqrt{2}+\sqrt{5}):\mathbb{Q})$ sono completamente determinati dall'azione sugli elementi della base. Allora sia $\sigma\in\operatorname{Gal}(\mathbb{Q}(\sqrt{2}+\sqrt{5}):\mathbb{Q})$:

$$\begin{array}{l} \sigma(1)=1 \\ \sigma(\sqrt{2}+\sqrt{5})=\text{radice di } x^4-14x^2+9 \\ \sigma((\sqrt{2}+\sqrt{5})^2)=[\sigma(\sqrt{2}+\sqrt{5})]^2 \\ \sigma((\sqrt{2}+\sqrt{5})^3)=[\sigma(\sqrt{2}+\sqrt{5})]^3 \end{array}$$

Allora σ è completamente determinato da $\sigma(\sqrt{2}+\sqrt{5})$. Nel nostro caso, tutte le scelte per $\sigma(\sqrt{2}+\sqrt{5})$ nell'insieme delle radici del polinomio minimo x^4-14x^2+9 vanno bene. [1]

Allora:

$$\begin{aligned}
&\sigma_1(\sqrt{2}+\sqrt{5}) = \sqrt{2}+\sqrt{5} \quad \Longrightarrow \quad \sigma_1 = \mathrm{Id}_{Q(\sqrt{2}+\sqrt{5})}\\
&\sigma_2(\sqrt{2}+\sqrt{5}) = -(\sqrt{2}+\sqrt{5})\\
&\sigma_3(\sqrt{2}+\sqrt{5}) = \sqrt{2}-\sqrt{5}\\
&\sigma_4(\sqrt{2}+\sqrt{5}) = -\sqrt{2}+\sqrt{5}.
\end{aligned}$$

□

13. Riferendosi all'esercizio precedente (12), scrivere la matrice di σ_3 rispetto alla base $\{1, u, u^2, u^3\}$, con $u = \sqrt{2}+\sqrt{5}$.

Svolgimento.

La matrice ha sulle colonne le immagini degli elementi della base, scritte rispetto alla base fissata:

$$\left(\ \sigma_3(1) \ \middle| \ \sigma_3(\sqrt{2}+\sqrt{5}) \ \middle| \ \sigma_3((\sqrt{2}+\sqrt{5})^2) \ \middle| \ \sigma_3((\sqrt{2}+\sqrt{5})^3) \ \right) \in \mathrm{Mat}_4(\mathbb{Q})$$

Ovviamente $\sigma_3(1) = 1$.

Per come è stata definita σ_3: $\sigma_3(\sqrt{2}+\sqrt{5}) = \sqrt{2}-\sqrt{5}$

$$\begin{aligned}
\sqrt{2}-\sqrt{5} &= a + b(\sqrt{2}+\sqrt{5}) + c(\sqrt{2}+\sqrt{5})^2 + d(\sqrt{2}+\sqrt{5})^3 =\\
&= a + b(\sqrt{2}+\sqrt{5}) + c(7+2\sqrt{10}) + d(17\sqrt{2}+11\sqrt{5}) =\\
&= (a+7c) + (b+11d)\sqrt{2} + (b+11d)\sqrt{5} + 2c\sqrt{10}
\end{aligned}$$

$$\begin{cases} a+7c=0\\ b+17d=1\\ b+11d=-1\\ 2c=0 \end{cases} \quad \Longrightarrow \quad \begin{cases} c=0\\ a=0\\ b=1-17d\\ 1-17d+11d+1=0 \end{cases} \quad \Longrightarrow \quad \begin{cases} a=0\\ b=-\frac{14}{3}\\ c=0\\ d=\frac{1}{3} \end{cases}$$

[1] Se non stessimo considerando il polinomio minimo, ma, ad esempio, $(x^2-2)(x^2+1)$, potremmo mandare $\sqrt{2}$ solo in $\pm\sqrt{2}$.

Allora:

$$\sigma_3(\sqrt{2}+\sqrt{5}) = -\frac{14}{3}(\sqrt{2}+\sqrt{5}) + \frac{1}{3}(\sqrt{2}+\sqrt{5})^3$$

Consideriamo: $\sigma_3((\sqrt{2}+\sqrt{5})^2) = (\sqrt{2}-\sqrt{5})^2 = 7-2\sqrt{10}$

$$\begin{cases} a+7c=7 \\ b+17d=0 \\ b+11d=0 \\ 2c=-2 \end{cases} \implies \begin{cases} c=-1 \\ a=14 \\ b=-11d \\ 6d=0 \end{cases} \implies \begin{cases} a=14 \\ b=0 \\ c=-1 \\ d=0 \end{cases}$$

Allora:

$$\sigma_3((\sqrt{2}+\sqrt{5})^2) = 14-(\sqrt{2}+\sqrt{5})^2$$

Consideriamo: $\sigma_3((\sqrt{2}+\sqrt{5})^3) = (\sqrt{2}-\sqrt{5})^3 = 17\sqrt{2}-11\sqrt{5}$

$$\begin{cases} a+7c=0 \\ b+17d=17 \\ b+11d=-11 \\ 2c=0 \end{cases} \implies \begin{cases} c=0 \\ a=0 \\ b=-11-11d \\ -11-11d+17d=17 \end{cases} \implies \begin{cases} a=0 \\ b=-\frac{187}{3} \\ c=0 \\ d=\frac{14}{3} \end{cases}$$

Allora:

$$\sigma_3((\sqrt{2}+\sqrt{5})^3) = -\frac{187}{3}(\sqrt{2}+\sqrt{5}) + \frac{14}{3}\sqrt{2}+\sqrt{5})^3$$

Quindi:

$$\begin{pmatrix} 1 & 0 & 14 & 0 \\ 0 & -\frac{14}{3} & 0 & -\frac{187}{3} \\ 0 & 0 & -1 & 0 \\ 0 & \frac{1}{3} & 0 & \frac{14}{3} \end{pmatrix}$$

□

14. Sia $\alpha = \sqrt{2+\sqrt{2}} \in \mathbb{R}$.

1. Determinare min $_{\mathbb{Q},\alpha}(x)$ e min $_{\mathbb{Q}(\sqrt{2}),\alpha}(x)$.

2. Scrivere una $\mathbb{Q}$-base per $\mathbb{Q}(\alpha)$.

3. Dire se $\mathbb{Q}(\alpha)$ è estensione di Galois di $\mathbb{Q}$.

4. Descrivere gli elementi del gruppo Gal $(\mathbb{Q}(\alpha) : \mathbb{Q})$ e verificare che Gal $(\mathbb{Q}(\alpha) : \mathbb{Q})$ è ciclico.

Svolgimento.

1. $\alpha = \sqrt{2+\sqrt{2}} \quad \Longrightarrow \quad \alpha^2 = 2+\sqrt{2} \quad \Longrightarrow \quad \alpha^2 - 2 = \sqrt{2} \quad \Longrightarrow$
   $(\alpha^2-2)^2 = 2 \quad \Longrightarrow \quad \alpha^4 - 4\alpha^2 + 4 = 2 \quad \Longrightarrow \quad \alpha^4 - 4\alpha^2 + 2 = 0$
   $p(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$ è monico e si annulla su α. Per il criterio di Eisenstein (con p=2) $p(x)$ è irriducibile su $\mathbb{Q}$.
   Allora $\min_{\mathbb{Q},\alpha}(x) = x^4 - 4x^2 + 2$.
   Per determinare $\min_{\mathbb{Q}(\sqrt{2}),\alpha}(x)$ guardiamo ai passaggi effettuati per trovare $p(x)$. In particolare sappiamo che $\alpha^2 - 2 = \sqrt{2}$.
   Il polinomio $x^2 - 2 - \sqrt{2}$ appartiene a $\mathbb{Q}(\sqrt{2})[x]$, è monico e si annulla su α.
   Inoltre sappiamo che
   $$4 = \deg(\min_{\mathbb{Q},\alpha}(x)) = |\mathbb{Q}(\alpha) : \mathbb{Q}| = |\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}) : \mathbb{Q}|$$
   e $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$. Quindi $2 = |\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})| = \deg(\min_{\mathbb{Q}(\sqrt{2}),\alpha}(x))$, Pertanto $\min_{\mathbb{Q}(\sqrt{2}),\alpha}(x) = x^2 - 2 - \sqrt{2}$.

2. Per il punto precedente sappiamo che
   $$|\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$$
   Quindi una $\mathbb{Q}$- base per $\mathbb{Q}(\alpha)$ è $\mathcal{B} = \{1, \alpha, \alpha^2, \alpha^3\}$.

3. Sappiamo che $\mathbb{Q}(\alpha)$ è estensione di Galois di $\mathbb{Q}$ se e solo se $\mathbb{Q}(\alpha)$ è campo di spezzamento di un polinomio separabile.
   Sia $f(x) = x^4 - 4x^2 + 2$. $\mathbb{Q}(\alpha)$ è l'estensione che otteniamo aggiungendo a $\mathbb{Q}$ una radice del polinoio f. $\mathbb{Q}(\alpha)$ è campo di spezzamento di f se tutte le radici di f sono contenute in $\mathbb{Q}(\alpha)$.
   Radici di f: $\pm\sqrt{2\pm\sqrt{2}}$
   Allora si ha che:
   $$\alpha = \sqrt{2+\sqrt{2}} \in \mathbb{Q}(\alpha)$$
   $$-\alpha = -\sqrt{2+\sqrt{2}} \in \mathbb{Q}(\alpha)$$

Consideriamo ora $\sqrt{2-\sqrt{2}}$:

$$\sqrt{2-\sqrt{2}} = \frac{\sqrt{2-\sqrt{2}}\cdot\sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2}}} = \frac{\sqrt{4-2}}{\sqrt{2+\sqrt{2}}} = \frac{\sqrt{2}}{\alpha} = \frac{\alpha^2-2}{\alpha}$$

Allora $\sqrt{2-\sqrt{2}} = \frac{\alpha^2-2}{\alpha} \in \mathbb{Q}(\alpha)$, e quindi anche $-\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\alpha)$.
Poichè tutte le radici di f stanno in $\in \mathbb{Q}(\alpha)$, questo è il campo di spezzamento del polinomio f su $\mathbb{Q}$.
Infine f è separabile, perchè è irriducibile su $\mathbb{Q}$ e tutte le sue radici sono distinte.
Si conclude che $\in \mathbb{Q}(\alpha)$ è estensione di Galois di $\mathbb{Q}$.

4. Poichè $\mathbb{Q}(\alpha) : \mathbb{Q}$ è di Galois si ha che:

$$|\operatorname{Gal}(\mathbb{Q}(\alpha):\mathbb{Q})| = |\mathbb{Q}(\alpha):\mathbb{Q}| = 4$$

Gli elementi di $\operatorname{Gal}(\mathbb{Q}(\alpha):\mathbb{Q})$ sono univocamente determinati dalla loro azione su α e sono:

$$\begin{aligned}
&\sigma_1 : \alpha \mapsto \alpha \quad \Longrightarrow \quad \sigma_1 = \mathrm{Id}_{\mathbb{Q}(\alpha)} \\
&\sigma_2 : \alpha \mapsto -\alpha \\
&\sigma_3 : \alpha \mapsto \sqrt{2-\sqrt{2}} = \frac{\alpha^2-2}{\alpha} \\
&\sigma_4 : \alpha \mapsto -\sqrt{2-\sqrt{2}} = \frac{2-\alpha^2}{\alpha}
\end{aligned}$$

Per verificare che $\operatorname{Gal}(\mathbb{Q}(\alpha):\mathbb{Q})$ è ciclico, cerchiamone un generatore, ossia un σ_i di periodo 4.
$\sigma_1 = \mathrm{Id}_{\mathbb{Q}(\alpha)}$ ha periodo 1.
σ_2 ha periodo 2, infatti:

$$\sigma_2^2(\alpha) = \sigma_2(\sigma_2(\alpha)) = \sigma_2(-\alpha) = -\sigma_2(\alpha) = -(-\alpha) = \alpha$$

σ_3 ha periodo 4, infatti:

$$\sigma_3^2(\alpha) = \sigma_3(\sigma_3(\alpha)) = \sigma_3\left(\frac{\alpha^2-2}{\alpha}\right) = \frac{\sigma_3(\alpha)^2-2}{\sigma_3(\alpha)} = \frac{\left(\frac{\alpha^2-2}{\alpha}\right)^2-2}{\frac{\alpha^2-2}{\alpha}} =$$
$$= \frac{\frac{2-2\alpha^2}{\alpha^2}}{\frac{\alpha^2-2}{\alpha}} = \frac{2-2\alpha^2}{\alpha(\alpha^2-2)} = \frac{2-2(2+\sqrt{2})}{\sqrt{2}\sqrt{2+\sqrt{2}}} = \frac{-2-2\sqrt{2}}{\sqrt{2}\sqrt{2+\sqrt{2}}} =$$
$$= -\frac{2(\sqrt{2}+1)}{\sqrt{2}\sqrt{2+\sqrt{2}}} = -\frac{\sqrt{2}+2}{\sqrt{2+\sqrt{2}}} = -\sqrt{2+\sqrt{2}} = -\alpha$$

Quindi $\sigma_3^2 = \sigma_2$.

Invece:

$$\sigma_3^4(\alpha) = \sigma_3^2(\sigma_3^2(\alpha)) = \sigma_2(\sigma_2(\alpha)) = \sigma_2^2(\alpha) = \alpha$$

Possiamo concludere che $\mathrm{Gal}\,(\mathbb{Q}(\alpha):\mathbb{Q}) = \langle\sigma_3\rangle$, e quindi $\mathrm{Gal}\,(\mathbb{Q}(\alpha):\mathbb{Q})$ è ciclico.

$\square$

15. Calcolare il campo di spezzamento Σ di

$$f = (x^2-3)(x^2+2) \in \mathbb{Q}[x].$$

Calcolare $|\Sigma : \mathbb{Q}|$ e deteminare $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$.

Svolgimento.

Le radici di f sono: $\pm\sqrt{3},\ \pm i\sqrt{2}$.

$\Sigma = \mathbb{Q}(\sqrt{3}, -\sqrt{3}, i\sqrt{2}, -i\sqrt{2}) = \mathbb{Q}(\sqrt{3}, i\sqrt{2})$

$|\Sigma : \mathbb{Q}| = |\Sigma : \mathbb{Q}(\sqrt{3})||\mathbb{Q}(\sqrt{3}) : \mathbb{Q}|$

$\Sigma : \mathbb{Q}(\sqrt{3})$ è un'estensione semplice ottenuta aggiungendo $i\sqrt{2}$. Ha grado 2 (perchè $\min_{\mathbb{Q}(\sqrt{3}),\,i\sqrt{2}}(x) = x^2+2$).

$\mathbb{Q}(\sqrt{3}) : \mathbb{Q}$ è un'estensione semplice di grado 2 (perchè $\min_{\mathbb{Q},\sqrt{3}}(x) = x^2-3$).

Allora: $|\Sigma : \mathbb{Q}| = 4$.

Σ è un'estensione di Galois, perchè è campo di spezzamento di un polinomio separabile. Allora: $|\,\mathrm{Gal}\,(\Sigma : \mathbb{Q})| = |\Sigma : \mathbb{Q}| = 4$.

Per determinare gli elementi di $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ procediamo un passo alla volta.

$$
\begin{tikzcd}
\bullet\, \mathbb{Q}(\sqrt{3}, i\sqrt{2}) \arrow[r] \arrow[d, dash] & \bullet\, \mathbb{Q}(\sqrt{3}, i\sqrt{2}) \arrow[d, dash] \\
\bullet\, \mathbb{Q}(\sqrt{3}) \arrow[r] \arrow[d, dash] & \bullet\, \mathbb{Q}(\sqrt{3}) \arrow[d, dash] \\
\bullet\, \mathbb{Q} \arrow[r, "\mathrm{Id}"] & \bullet\, \mathbb{Q}
\end{tikzcd}
$$

Osserviamo che i σ_i sono completamente determinati dalla loro azione su $\sqrt{3}$ e $i\sqrt{2}$. Possiamo estendere l'identitá di $\mathbb{Q}$ ad un automorfismo di $\mathbb{Q}(\sqrt{3})$ in due modi diversi, mandando $\sqrt{3}$ in una delle radici di $\min_{\mathbb{Q},\sqrt{3}}(x) = x^2 - 3$:

$$\tilde{\sigma_1} : \begin{cases} \mathbb{Q}(\sqrt{3}) \to & \mathbb{Q}(\sqrt{3}) \\ \sqrt{3} \mapsto & \sqrt{3} \end{cases} \qquad \text{cioè } \tilde{\sigma_1} = \mathrm{Id}_{\mathbb{Q}(\sqrt{3})}$$

e

$$\tilde{\sigma_2} : \begin{cases} \mathbb{Q}(\sqrt{3}) \to & \mathbb{Q}(\sqrt{3}) \\ \sqrt{3} \mapsto & -\sqrt{3} \end{cases} \qquad \text{e } \tilde{\sigma_2}|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$$

Ora possiamo estendere ognuno dei $\tilde{\sigma_i}$ ad un automorfismo di $\mathbb{Q}(\sqrt{3},\ i\sqrt{2})$ in due modi diversi, mandando $i\sqrt{2}$ in una delle radici di $\min_{\mathbb{Q}(\sqrt{3}),i\sqrt{2}}(x) = x^2 + 2$. Otteniamo in tutto quattro $\mathbb{Q}$-automorfismi di $\mathbb{Q}(\sqrt{3},\ i\sqrt{2})$, cioè :

$$\sigma_1 : \begin{cases} \sqrt{3} \mapsto & \sqrt{3} \\ i\sqrt{2} \mapsto & i\sqrt{2} \end{cases} \qquad \sigma_2 : \begin{cases} \sqrt{3} \mapsto & -\sqrt{3} \\ i\sqrt{2} \mapsto & i\sqrt{2} \end{cases}$$

$$\sigma_3 : \begin{cases} \sqrt{3} \mapsto & \sqrt{3} \\ i\sqrt{2} \mapsto & -i\sqrt{2} \end{cases} \qquad \sigma_4 : \begin{cases} \sqrt{3} \mapsto & -\sqrt{3} \\ i\sqrt{2} \mapsto & -i\sqrt{2} \end{cases}$$

Una base di Σ su $\mathbb{Q}$ è data dal prodotto degli elementi di una base di $\mathbb{Q}(\sqrt{3})$ su $\mathbb{Q}$, cioè $\mathcal{B}_1 = \{1,\ \sqrt{3}\}$, per gli elementi di una base di Σ su $\mathbb{Q}(\sqrt{3})$, cioè $\mathcal{B}_2 = \{1,\ i\sqrt{2}\}$[2]. Quindi una base è :

$$\mathcal{B} = \{1,\ \sqrt{3},\ i\sqrt{2},\ i\sqrt{6}\}.$$

Ogni elemento di $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ è completamente determinato dalla sua azione sugli elementi della base e, poichè si tratta di automorfismi di campo, se $\sigma \in \mathrm{Gal}\,(\Sigma : \mathbb{Q})$

[2]Vedi la dimostrazione del teorema sulla formula dei gradi.

si ha che

$$\sigma(i\sqrt{6}) = \sigma(\sqrt{3} \cdot i\sqrt{2}) = \sigma(\sqrt{3}) \cdot \sigma(i\sqrt{2}).$$

Quindi gli automorfismi σ_i sono completamente determinati dalla loro azione su $\sqrt{3}$ e $i\sqrt{2}$.

Sappiamo che $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ ha ordine 4. Allora puó essere:

$$\mathrm{Gal}\,(\Sigma : \mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \text{oppure} \quad \mathrm{Gal}\,(\Sigma : \mathbb{Q}) \cong \mathbb{Z}_4$$

Nel primo caso tutti gli elementi dovrebbero avere periodo 2, eccetto l'unitá, nel secondo caso il gruppo è ciclico.

Si vede che $\sigma_2^2 = \mathrm{Id}_\Sigma$, $\sigma_3^2 = \mathrm{Id}_\Sigma$, $\sigma_4^2 = \mathrm{Id}_\Sigma$ e quindi tutti gli elementi non identici del gruppo di Galois hanno periodo 2. Pertanto $\mathrm{Gal}\,(\Sigma : \mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Sappiamo che, se $R = \{\pm\sqrt{3}, \pm i\sqrt{2}\}$, allora $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ è isomorfo ad un sottogruppo di $\mathrm{Sym}(R) = \mathrm{S}_4$ e quindi possiamo scrivere i suoi elementi come permutazioni di R. Abbiamo:

$\sigma_1 = \mathrm{Id}$

$\sigma_2 = (\sqrt{3}, -\sqrt{3})$

$\sigma_3 = (i\sqrt{2}, -i\sqrt{2})$

$\sigma_4 = (\sqrt{3}, -\sqrt{3})(i\sqrt{2}, -i\sqrt{2})$

□

16. Sia $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.

1. Determinare il campo di spezzamento Σ di f su $\mathbb{Q}$ e $|\Sigma : \mathbb{Q}|$.

2. Scrivere gli elementi di $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ come permutazioni delle radici di f e dire se il gruppo è transitivo.

3. Descrivere i sottocampi di Σ, specificando quali sono estensione normale di $\mathbb{Q}$.

Svolgimento.

1. Le radici di f sono: $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$ con $\omega = e^{\frac{2\pi}{3}i}$.

   $\Sigma = \mathbb{Q}(\sqrt[3]{2},\, \omega\sqrt[3]{2},\, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2},\, \omega)$.

   $|\Sigma : \mathbb{Q}| = 2 \cdot 3 = 6$

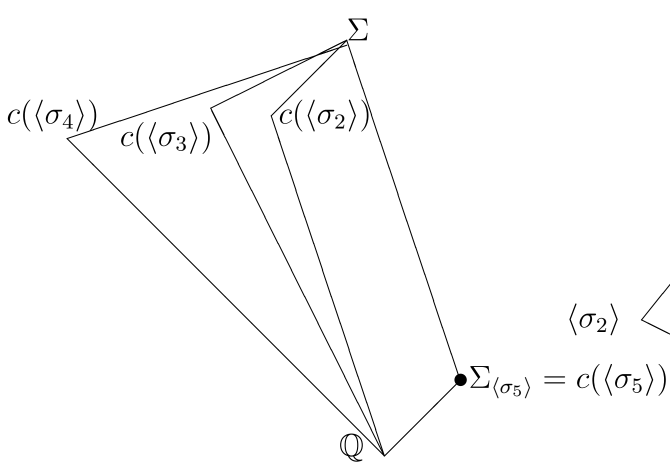
2. $\Sigma : \mathbb{Q}$ è estensione di Galois perchè Σ è campo di spezzamento di f separabile. Quindi $|\,\mathrm{Gal}\,(\Sigma : \mathbb{Q})| = |\Sigma : \mathbb{Q}| = 6$.

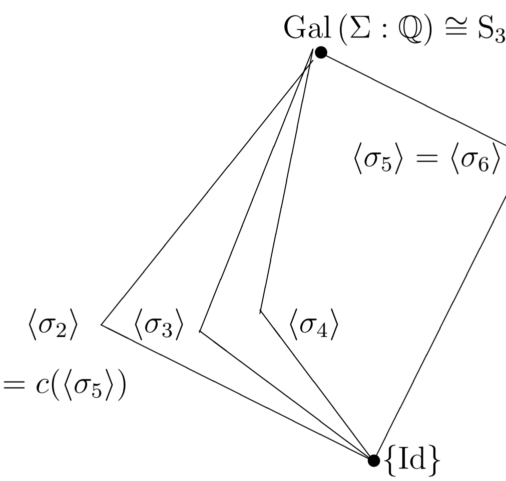
   Sappiamo che $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ è isomorfo ad un sottogruppo di S_3 e poichè $|\mathrm{S}_3| = 6$ si ha che $\mathrm{Gal}\,(\Sigma : \mathbb{Q}) \cong \mathrm{S}_3$.

$\sigma_1 = \mathrm{Id}$	$\sigma_4 = (\omega\sqrt[3]{2},\, \omega^2\sqrt[3]{2})$
$\sigma_2 = (\sqrt[3]{2},\, \omega\sqrt[3]{2})$	$\sigma_5 = (\sqrt[3]{2},\, \omega\sqrt[3]{2},\, \omega^2\sqrt[3]{2})$
$\sigma_3 = (\sqrt[3]{2},\, \omega^2\sqrt[3]{2})$	$\sigma_6 = (\sqrt[3]{2},\, \omega^2\sqrt[3]{2},\, \omega\sqrt[3]{2}) = \sigma_5^2$

   $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ è transitivo perchè S_3 è transitivo.

3. Applichiamo il teorema di corrispondenza di Galois:





   $\langle\sigma_2\rangle = \{\mathrm{Id},\, \sigma_2\}$ $\quad$ $\langle\sigma_3\rangle = \{\mathrm{Id},\, \sigma_3\}$

   $\langle\sigma_4\rangle = \{\mathrm{Id},\, \sigma_4\}$ $\quad$ $\langle\sigma_5\rangle = \{\mathrm{Id},\, \sigma_5,\, \sigma_6\} = \langle\sigma_6\rangle$

   L'unico sottogruppo normale di $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ è $\langle\sigma_5\rangle$.

   Ad ogni sottogruppo corrisponde un sottocampo. L'unico campo che è estensione normale di $\mathbb{Q}$ è $c(\langle\sigma_5\rangle)$.

   $\Sigma = \mathbb{Q}(\sqrt[3]{2},\, \omega)$

- $c(\langle\sigma_2\rangle) = \Sigma_{\langle\sigma_2\rangle} \overset{\text{def}}{=} \{\alpha \in \Sigma \,|\, \alpha^\sigma = \alpha,\ \forall \sigma \in \langle\sigma_2\rangle\} = \{\alpha \in \Sigma \,|\, \alpha^{\sigma_2} = \alpha\}$
  Sicuramente $\omega^2\sqrt[3]{2} \in c(\langle\sigma_2\rangle)$ e $\mathbb{Q} \subseteq c(\langle\sigma_2\rangle)$, quindi $\mathbb{Q}(\omega^2\sqrt[3]{2}) \subseteq c(\langle\sigma_2\rangle)$.
  Per quanto riguarda i gradi:
  $$\begin{array}{l} |c(\langle\sigma_2\rangle) : \mathbb{Q}| = 3 \\ |\mathbb{Q}(\omega^2\sqrt[3]{2}) : \mathbb{Q}| = 3 \end{array} \qquad \Longrightarrow \qquad \mathbb{Q}(\omega^2\sqrt[3]{2}) = c(\langle\sigma_2\rangle)$$
- $c(\langle\sigma_3\rangle) = \Sigma_{\langle\sigma_3\rangle} = \{\alpha \in \Sigma \,|\, \alpha^{\sigma_3} = \alpha\}$
  $\mathbb{Q}(\omega\sqrt[3]{2}) \subseteq c(\langle\sigma_3\rangle)$ e poichè sono entrambe estensioni di grado 3 su $\mathbb{Q}$, ne segue che $\mathbb{Q}(\omega\sqrt[3]{2}) = c(\langle\sigma_3\rangle)$.
- Allo stesso modo si ha che $c(\langle\sigma_4\rangle) = \mathbb{Q}(\sqrt[3]{2})$.
- $c(\langle\sigma_5\rangle) = \Sigma_{\langle\sigma_5\rangle} = \{\alpha \in \Sigma \,|\, \alpha^\sigma = \alpha,\ \forall \sigma \in \langle\sigma_5\rangle\} = \{\alpha \in \Sigma \,|\, \alpha^{\sigma_5} = \alpha\}$
  (Tutti gli elementi fissati da σ_5 sono fissati anche da σ_5^2)
  $$\omega^{\sigma_5} = \left(\frac{\omega\sqrt[3]{2}}{\sqrt[3]{2}}\right)^{\sigma_5} = \frac{\omega^2\sqrt[3]{2}}{\omega\sqrt[3]{2}} = \omega \quad \Longrightarrow \quad \omega \in c(\langle\sigma_5\rangle)$$
  $\mathbb{Q}(\omega) \subseteq c(\langle\sigma_5\rangle)$ e le estensioni hanno entrambe grado 2 su $\mathbb{Q}$, quindi $\mathbb{Q}(\omega) = c(\langle\sigma_5\rangle)$.

$\square$

17. Sia $f(x) = x^4 - 2x^2 - 15 \in \mathbb{Q}[x]$.

1. Determinare Σ e $|\Sigma : \mathbb{Q}|$.
2. Dire a quale gruppo è isomorfo $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$.
3. Descrivere i sottocampi di Σ.

Svolgimento.

1. $f(x) = (x^2 - 5)(x^2 + 3)$
   Le radici di f sono: $\pm\sqrt{5}$, $\pm i\sqrt{3}$.
   $\Sigma = \mathbb{Q}(\sqrt{5}, i\sqrt{3})$.

$\min_{\mathbb{Q}(\sqrt{5}),\, i\sqrt{3}}(x) = x^2 + 3 \qquad\qquad \min_{\mathbb{Q},\,\sqrt{5}}(x) = x^2 - 5.$

$|\Sigma : \mathbb{Q}| = |\mathbb{Q}(\sqrt{5},\, i\sqrt{3}) : \mathbb{Q}(\sqrt{5})||\mathbb{Q}(\sqrt{5}.\mathbb{Q}| = 4$

2. Gli elementi di $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ sono:

$$\sigma_1 : \begin{cases} \sqrt{5} \mapsto & \sqrt{5} \\ i\sqrt{3} \mapsto & i\sqrt{3} \end{cases} \qquad \sigma_2 : \begin{cases} \sqrt{5} \mapsto & -\sqrt{5} \\ i\sqrt{3} \mapsto & i\sqrt{3} \end{cases}$$

$$\sigma_3 : \begin{cases} \sqrt{5} \mapsto & -\sqrt{5} \\ i\sqrt{3} \mapsto & -i\sqrt{3} \end{cases} \qquad \sigma_4 : \begin{cases} \sqrt{5} \mapsto & \sqrt{5} \\ i\sqrt{3} \mapsto & -i\sqrt{3} \end{cases}$$

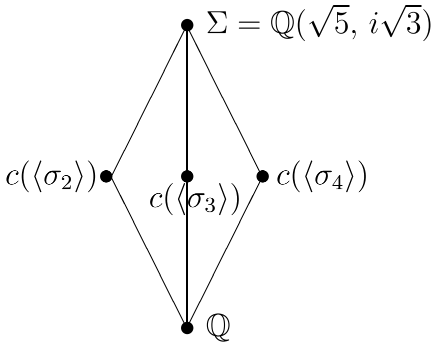
Σ è estensione di Galois di $\mathbb{Q}$, quindi $|\,\mathrm{Gal}\,(\Sigma : \mathbb{Q})| = |\Sigma : \mathbb{Q}| = 4$.

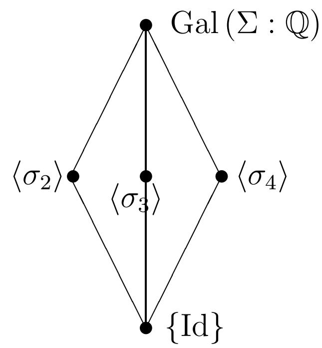
Allora puó essere:

$$\mathrm{Gal}\,(\Sigma : \mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad \text{oppure} \quad \mathrm{Gal}\,(\Sigma : \mathbb{Q}) \cong \mathbb{Z}_4$$

Si vede che $\sigma_2^2 = \mathrm{Id}_\Sigma$, $\sigma_3^2 = \mathrm{Id}_\Sigma$, $\sigma_4^2 = \mathrm{Id}_\Sigma$ e quindi ogni elemento non identico ha periodo 2. Allora $\mathrm{Gal}\,(\Sigma : \mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

3. Applichiamo il teorema di corrispondenza di Galois:





$\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ è un gruppo abeliano (perchè ha ordine $4 = 2^2$), quindi tutti i suoi sottogruppi sono normali. Per il teorema di corrispondenza di Galois, tutte le estensioni intermedie sono normali.

- $c(\langle\sigma_2\rangle) = \mathbb{Q}(i\sqrt{3})$
- $c(\langle\sigma_3\rangle) = \mathbb{Q}(i\sqrt{15})$ infatti:
  $\sigma_3(i\sqrt{15}) = \sigma_3(\sqrt{5} \cdot i\sqrt{3}) = \sigma_3(\sqrt{5})\sigma_3(i\sqrt{3}) = (-\sqrt{5})(-i\sqrt{3}) = i\sqrt{15}$
  Allora $i\sqrt{15} \in c(\langle\sigma_3\rangle)$, $\mathbb{Q} \subseteq c(\langle\sigma_3\rangle) \implies \mathbb{Q}(i\sqrt{15}) \subseteq c(\langle\sigma_3\rangle)$
  $|c(\langle\sigma_3\rangle) : \mathbb{Q}| = |\mathbb{Q}(i\sqrt{15}) : \mathbb{Q}| = 2$, quindi $\mathbb{Q}(i\sqrt{15}) = c(\langle\sigma_3\rangle)$

- $c(\langle\sigma_4\rangle) = \mathbb{Q}(\sqrt{5})$

$\square$

18. Sia $p(x) = x^2 + ax + 1 \in \mathbb{Z}_3[x]$. Per quali valori di a il polinomio ha tutte le radici distinte?

Svolgimento.

$(p(x), p'(x)) \in \mathbb{Z}_3 \quad \Longleftrightarrow \quad p(x)$ ha tutte le radici distinte.

$p'(x) = 2x + a$

$$\begin{array}{ccc|cc} x^2 & +ax & +1 & 2x & +a \\ \cline{4-5} -x^2 & -2ax & & 2x & +a \\ \cline{1-3} // & +2ax & +1 & & \\ & -2ax & -a^2 & & \\ \cline{2-3} & // & 1-a^2 & & \end{array}$$

$1 - a^2 = (p(x), p'(x)) \quad \Longleftrightarrow \quad 1 - a^2 \neq 0 \quad \Longleftrightarrow \quad a^2 \neq 1 \quad \Longleftrightarrow \quad a = 0$

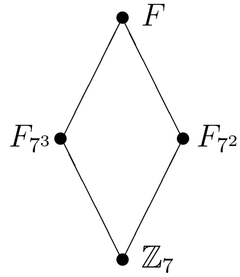
Quindi $p(x)$ ha radici distinte se e solo se $a = 0$. $\square$

19. Descrivere il reticolo dei sottocampi di F campo di ordine $|F| = 7^6$. F possiede un sottocampo di ordine 7^4?

Svolgimento.

$|F| = 7^6$ quindi F è un campo di caratteristica 7, il suo sottocampo fondamentale è $\mathbb{Z}_7$ e $|F : \mathbb{Z}_7| = 6$.

F ha uno e un solo sottocampo di ordine 7^m per ogni m divisore di 6. Quindi F non possiede un sottocampo di ordine 4, perchè $4 \nmid 6$.



$\square$

20. Calcolare $\Phi_8(x)$ e fattorizzarlo in irriducibili in $\mathbb{Q}[x]$ e $\mathbb{Z}_{41}[x]$.

Svolgimento.

$$x^8 - 1 = \prod_{d|8} \Phi_d(x) = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)$$

$$\Phi_8(x) = \frac{x^8-1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)} = \frac{(x^4-1)(x^4+1)}{\Phi_1(x)\Phi_2(x)\Phi_4(x)} = \frac{(x^4-1)(x^4+1)}{x^4-1} = x^4+1$$

In $\mathbb{Q}[x]$, $\Phi_8(x)$ è irriducibile per il teorema di Gauss.

In $\mathbb{Z}_{41}[x]$: 41 è un primo, quindi $\mathbb{Z}_{41}$ è un campo. Ci chiediamo se $\Phi_8(x)$ ha una radice in $\mathbb{Z}_{41}$. Poichè $[0]_{41}$ sicuramente non è una radice di $\Phi_8(x)$, tale radice dovrebbe appartenere a $\mathbb{Z}_{41}^*$, gruppo moltiplicativo. Inoltre, essendo una radice primitiva ottava dell'unitá, dovrebbe avere periodo moltiplicativo 8.

$\mathbb{Z}_{41}^*$ è un gruppo ciclico di cardinalitá $|\mathbb{Z}_{41}^*| = 40$, e quindi ha un sottogruppo ciclico di ordine d per ogni d che divide 40. Dal momento che $8|40$, $\mathbb{Z}_{41}^*$ ha un sottogruppo ciclico di ordine 8. Tutti gli elementi di periodo 8 stanno in tale sottogruppo di $\mathbb{Z}_{41}^*$ e sono suoi generatori:essi sono radici di $\Phi_8(x)$.

Se $| < g > | = 8$, $< g >= \{1, g, g^2, g^3, g^4, g^5, g^6, g^7\}$.

I generatori sono le potenze di g coprime con 8, cioè g, g^3, g^5, g^8: sono $\varphi(8) = \varphi(2^3) = 2^2(2-1) = 4$.

Allora $\Phi_8(x)$ ha esattamente 4 radici in $\mathbb{Z}_{41}$, ossia si fattorizza completamente in $\mathbb{Z}_{41}$.

$[3]_{41}$ ha periodo moltiplicativo 8 in $\mathbb{Z}_{41}$, infatti:

$$[3]_{41}^4 = [81]_{41} = [-1]_{41} \text{ quindi } [3]_{41} \text{ non ha periodo 4,}$$

$$[3]_{41}^8 = [-1]_{41}^2 = [1]_{41} \text{ quindi } [3]_{41} \text{ ha periodo 8.}$$

Gli altri elementi di periodo 8 sono: $[3]_{41}^3 = [27]_{41}$, $[3]_{41}^5 = [38]_{41}$, $[3]_{41}^7 = [14]_{41}$

$\Phi_8(x) = (x - [3]_{41})(x - [27]_{41})(x - [38]_{41})(x - [14]_{41})$ in $\mathbb{Z}_{41}[x]$. □

21. Dare una costruzione esplicita del campo F di ordine 9.

Svolgimento.

F è un campo di caratteristica 3, con sottocampo fondamentale $\mathbb{Z}_3$.

$|F : \mathbb{Z}_3| = 2$

$$F = \frac{\mathbb{Z}_3[x]}{< p(x) >} \quad \text{con } p(x) \text{ irriducibile in } \mathbb{Z}_3[x] \text{ e di grado 2}$$

$p(x) = x^2 - a$ è irriducibile in $\mathbb{Z}_3[x]$ se e solo se a non è un quadrato in $\mathbb{Z}_3[x]$

n	n^2
0	0
1	1
2	1

Allora $a = 2$ e $p(x) = x^2 - 2$.

$$F = \frac{\mathbb{Z}_3[x]}{< x^2 - 2 >} = \mathbb{Z}_3(\alpha) \quad \text{dove } \alpha \text{ ha polinomio minimo } x^2 - 2 \text{ su } \mathbb{Z}_3$$

$F = \mathbb{Z}_3(\alpha) = \{x + y\alpha | x, y \in \mathbb{Z}_3\} = \{0,\, 1,\, 2,\, \alpha,\, 2\alpha,\, 1+\alpha,\, 2+\alpha,\, 1+2\alpha,\, 2+2\alpha\}$.

$\square$

22. Sia F un campo di ordine 8. Fattorizzare in irriducibili in $F[x]$ i polinomi $\Phi_7(x)$ e $\Phi_3(x)$.

Dedurre che $\Phi_7(x)$ non è irrriducibile in $\mathbb{Z}_2[x]$.

Svolgimento.

• Un elemento di F è radice di $\Phi_7(x)$ se e solo se ha periodo moltiplicativo 7.

$|F^*| = 7$ e F^* è un gruppo ciclico: i generatori di F^* sono gli elementi di periodo moltiplicativo 7. Poichè 7 è un numero primo, ogni elemento di $F^* \setminus \{1\}$ ha periodo 7 e quindi è uno dei generatori di F^*: sono 6 in tutto.

$\deg(\Phi_7(x)) = \varphi(7) = 6$ quindi $\Phi_7(x)$ si fattorizza completamente in $F[x]$:

$$\Phi_7(x) = (x - a_1)(x - a_2)(x - a_3)(x - a_4)(x - a_5)(x - a_6)$$

con $F = \{0,\, 1,\, a_1,\, a_2,\, a_3,\, a_4,\, a_5,\, a_6\}$.

• Un elemento di F è radice di $\Phi_3(x)$ se e solo se ha periodo moltiplicativo 3.

$|F^*| = 7$ e F^* è un gruppo ciclico. Per il teorema di Lagrange, se c'è un elemento di periodo 3 allora $3 \big| |F^*| = 7$: assurdo. Allora non ci sono elementi di periodo

moltiplicativo 3 in F^*, quindi $\Phi_3(x)$ non ha radici in F e così è irriducibile in $F[x]$.
• $\mathbb{Z}_2$ è il sottocampo primo di F. Supponiamo che $\Phi_7(x)$ sia irriducibile in $\mathbb{Z}_2[x]$. In F troviamo una radice a_1 di $\Phi_7(x)$. Allora:

$$\min_{\mathbb{Z}_2,\, a_1}(x) = \Phi_7(x)$$

Il teorema sulle estensioni semplici dice che: $|\mathbb{Z}_2(a_1) : \mathbb{Z}_2| = \deg(\Phi_7(x)) = 6$.
Così $6 = |\mathbb{Z}_2(a_1) : \mathbb{Z}_2| \big| |F : \mathbb{Z}_2| = 3$: assurdo. $\square$

23. Dimostrare che se F è un campo finito, $f \in F[x]$ irriducibile di grado n, E è un'estensione di F, allora sono equivalenti:

1. f si fattorizza completamente in $E[x]$;
2. f ha una radice in E;
3. $n \big| |E : F|$.

Svolgimento.
(1.⇒2.) Ovvio.
(2.⇒3.) Sia α una radice di f. Allora: $\min_{F,\alpha}(x)|f$.
Poichè f è irriducibile in $F[x]$, f è il polinomio minimo, a meno di un coefficiente. Allora $n = \deg(f) = \deg(\min_{F,\alpha}(x)) = |F(\alpha) : F|$ e per la formula dei gradi:

$$n \big| |E : F|.$$

(3.⇒1.) Supponiamo che $n \big| |E : F|$. Sia $|F| = p^t$. Sia E_1 un campo di spezzamento per f su F. Sia $\bar{\alpha} \in \mathrm{E}_1$ una radice di f. Ripetendo il ragionamento fatto prima si ottiene $|F(\bar{\alpha}) : F| = n$. Quindi $|F(\bar{\alpha})| = |F|^n = p^{nt}$, cioè $F(\bar{\alpha})$ è un campo finito. Anche E è un campo finito: $|E| = |F|^{|E:F|} = |F|^{nr} = p^{nrt}$ dove $nr = |E : F|$.
Per il Teorema di struttura dei campi finiti E contiene un sottocampo di ordine p^{nt} che è isomorfo a $F(\bar{\alpha})$ tramite un isomorfismo che è l'identità su F. Quindi l'elemento corrispondente in E ad $\bar{\alpha}$ è una radice di f.
Inoltre E è estensione di Galois di F, quindi E è estensione normale di F. Allora

E contiene tutte le radici di f (avendone una), e f si fattorizza completamente in $E[x]$. $\square$

24. Determinare il campo di spezzamento Σ su $\mathbb{Q}$ del polinomio $x^5 - 1$.

1. Calcolare $|\Sigma : \mathbb{Q}|$.
2. Determinare $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ e provare che è ciclico.
3. Descrivere i sottocampi di Σ, specificando quale di essi è estensione normale di $\mathbb{Q}$.

Svolgimento.
Le radici di $x^5 - 1$ sono $\omega = e^{\frac{2}{5}\pi i}$, ω^2, ω^3, ω^4, $\omega^5 = 1$.
$\Sigma = \mathbb{Q}(1,\, \omega^2,\, \omega^3,\, \omega^4) = \mathbb{Q}(\omega)$.

1. $|\Sigma : \mathbb{Q}| = \deg\left(\min_{\mathbb{Q},\omega}(x)\right) = \deg\left(\Phi_5(x)\right) = \varphi(5) = 4$.

2. Σ è estensione di Galois di $\mathbb{Q}$, perchè è campo di spezzamento di un polinomio in caratteristica zero. Allora:

$$|\,\mathrm{Gal}\,(\Sigma : \mathbb{Q})| = |\Sigma : \mathbb{Q}| = 4 \quad \text{e} \quad \mathrm{Gal}\,(\Sigma : \mathbb{Q}) \cong \mathrm{U}\left(\frac{\mathbb{Z}}{5Z}\right) = \mathbb{Z}_5^*$$

I $\mathbb{Q}$-automorfismi sono completamente determinati dall'azione sull'elemento ω:

$$\begin{aligned} \sigma_1 :& \omega \mapsto \omega \qquad \sigma_1 = \mathrm{Id}_\Sigma \\ \sigma_2 :& \omega \mapsto \omega^2 \\ \sigma_3 :& \omega \mapsto \omega^3 \\ \sigma_4 :& \omega \mapsto \omega^4 \end{aligned}$$

$\mathrm{Gal}\,(\Sigma : \mathbb{Q}) = \{\mathrm{Id}_\Sigma,\, \sigma_2,\, \sigma_3,\, \sigma_4\} = \langle \sigma_2 \rangle$ infatti:
$\sigma_2^2(\omega) = \sigma_2(\omega^2) = [\sigma_2(\omega)]^2 = (\omega^2)^2 = \omega^4 = \sigma_4(\omega)$
Quindi $\sigma_2^2 \neq \mathrm{Id}_\Sigma$, allora $|\sigma_2| \neq 2$ e poichè siamo in un gruppo di ordine 4 si ha $|\sigma_2| = 4$.

3. Per il teorema di corrispondenza di Galois:

$$\begin{tikzcd}[row sep=large] \Sigma \arrow[d, dash] \\ c(\langle \sigma_2^2 \rangle) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd} \qquad\qquad \begin{tikzcd}[row sep=large] \mathrm{Gal}\,(\Sigma : \mathbb{Q}) = \langle \sigma_2 \rangle \arrow[d, dash] \\ \langle \sigma_2^2 \rangle = \langle \sigma_4 \rangle = \{\mathrm{Id}_\Sigma,\, \sigma_4\} \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

$$c(\langle \sigma_2^2 \rangle) = c(\langle \sigma_4 \rangle) = \{a \in \Sigma | a^\alpha = a,\ \forall \alpha \in \langle \sigma_4 \rangle\} = \{a \in \Sigma | a^{\sigma_4} = a\}$$

$\sigma_4(\omega + \omega^4) = \sigma_4(\omega) + [\sigma_4(\omega)]^4 = \omega^4 + \omega^{16} = \omega^4 + \omega$

Allora $\omega + \omega^4 \in\ c(\langle \sigma_4 \rangle)$, $\mathbb{Q} \subseteq\ c(\langle \sigma_4 \rangle)$, quindi $\mathbb{Q}(\omega + \omega^4) \subseteq\ c(\langle \sigma_4 \rangle)$.

Inoltre $|c(\langle \sigma_4 \rangle) : \mathbb{Q}| = |\,\mathrm{Gal}\,(\Sigma : \mathbb{Q}) : \langle \sigma_4 \rangle| = \frac{4}{2} = 2$

Poichè $\mathbb{Q}(\omega + \omega^4) \neq \mathbb{Q}$ si ha che $\mathbb{Q}(\omega + \omega^4) = c(\langle \sigma_4 \rangle)$.

Σ è estensione normale di $\mathbb{Q}$ perchè è campo di spezzamento di un polinomio.

$\mathbb{Q}$ è estensione normale di $\mathbb{Q}$.

$\mathbb{Q}(\omega + \omega^4)$ è un'estensione normale di $\mathbb{Q}$? Per il teorema di corrispondenza di Galois dobbiamo verificare se $\langle \sigma_4 \rangle$ è un sottogruppo normale di $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$.

$\langle \sigma_2 \rangle$ è ciclico, quindi abeliano, per cui tutti i sottogruppi sono normali:

$$\langle \sigma_4 \rangle \trianglelefteq \langle \sigma_2 \rangle.$$

Allora $c(\langle \sigma_4 \rangle)$ è estensione normale di $\mathbb{Q}$.

$\square$

25. Dimostrare che F è un campo finito allora F non è algebricamente chiuso.

Svolgimento.

Consideriamo

$$p(x) = \prod_{a \in F} (x - a) + 1\ \in\ F[x]$$

$\forall a \in F : p(a) = 1$ quindi $p(x)$ non ha radici in F, perció F non è algebricamente chiuso. $\square$

26. Sia F un campo con $|F| = 8$. Si dia una costruzione esplicita di F e si trovi un generatore di F^*.

Svolgimento.

Caratteristica di F: 2, sottocampo primo di $F : \mathbb{Z}_2$, $|F : \mathbb{Z}_2| = 3$

$$F = \frac{\mathbb{Z}_2[x]}{\langle f(x) \rangle} \quad \text{con } f \text{ irriducibile di grado 3 in } \mathbb{Z}_2[x]$$

Consideriamo $x^3+x+1 \in \mathbb{Z}_2[x]$: è un polinomio irriducibile in $\mathbb{Z}_2$, perchè ha grado 3 ed è privo di radici in $\mathbb{Z}_2$. Allora:

$$F = \frac{\mathbb{Z}_2[x]}{\langle x^3 + x + 1 \rangle} = \mathbb{Z}_2(\alpha) \quad \text{con } \alpha \text{ radice di } x^3 + x + 1$$

$F = \{a + b\alpha + c\alpha^2 | a, b, c \in \mathbb{Z}_2\} = \{0, 1, \alpha, \alpha^2, 1 + \alpha, 1 + \alpha^2, 1 + \alpha + \alpha^2, \alpha + \alpha^2\}$
Il gruppo moltiplicativo ha ordine $|F^*| = 8 - 1 = 7$, quindi i suoi elementi hanno periodo che divide 7. Allora ogni elemento di $F \setminus \{0, 1\}$ ha periodo moltiplicativo 7 ed è un generatore di F^*:

$$F^* = \langle \alpha \rangle = \langle \alpha^2 \rangle = \langle 1 + \alpha \rangle = \dots$$

$\square$

27. Sia $f(x) = x^4 - 3 \in \mathbb{Q}[x]$.

1. Determinare il campo di spezzamento Σ di f su $\mathbb{Q}$ e calcolare $|\Sigma : \mathbb{Q}|$.

2. Scrivere gli elementi di $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ come permutazioni delle radici di f.

3. Descrivere il reticolo dei sottocampi di Σ.

Svolgimento.

1. Le radici di f sono: $\pm\sqrt[4]{3},\, \pm i\sqrt[4]{3}$
   $\Sigma = \mathbb{Q}(\pm\sqrt[4]{3},\, \pm i\sqrt[4]{3}) = \mathbb{Q}(\sqrt[4]{3}, i)$
   $|\Sigma : \mathbb{Q}| = |\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}(\sqrt[4]{3})||\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}|$
   Risulta $\min_{\mathbb{Q},\sqrt[4]{3}}(x) = x^4 - 3 \in \mathbb{Q}[x]$: è monico, si annulla in $\sqrt[4]{3}$ ed è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisentstein ($p = 3$). Inoltre si ha che $\min_{\mathbb{Q}(\sqrt[4]{3}),i}(x) = x^2 + 1 \in \mathbb{Q}(\sqrt[4]{3})[x]$: è monico, si annulla in i ed è irriducibile in $\mathbb{Q}(\sqrt[4]{3})[x]$ perchè ha grado 2 e le sue radici non sono reali ($\mathbb{Q}(\sqrt[4]{3}) \subset \mathbb{R}$).
   Quindi $|\Sigma : \mathbb{Q}| = 2 \cdot 4 = 8$.

2. Σ è estensione di Galois di $\mathbb{Q}$ perchè campo di spezzamento di un polinomio in caratteristica zero. Allora: $|\operatorname{Gal}(\Sigma : \mathbb{Q})| = |\Sigma : \mathbb{Q}|$.
   Gli elementi di $\operatorname{Gal}(\Sigma : \mathbb{Q})$ sono completamente determinati dalla loro azione su $\sqrt[4]{3}$ e i. Possiamo estendere l'identitá su $\mathbb{Q}$ in quattro modi diversi, mandando $\sqrt[4]{3}$ in una delle radici di $\min_{\mathbb{Q},\sqrt[4]{3}}(x) = x^4 - 3$:

$$\tilde{\sigma}_1 : \sqrt[4]{3} \mapsto \sqrt[4]{3} \qquad \tilde{\sigma}_2 : \sqrt[4]{3} \mapsto -\sqrt[4]{3}$$
$$\tilde{\sigma}_3 : \sqrt[4]{3} \mapsto i\sqrt[4]{3} \qquad \tilde{\sigma}_4 : \sqrt[4]{3} \mapsto -i\sqrt[4]{3}$$

   Ora possiamo estendere ogni $\tilde{\sigma}_i$ ad un automorfismo di $\mathbb{Q}(\sqrt[4]{3},\, i)$ in due modi diversi, mandando i in una delle radici di $\min_{\mathbb{Q}(\sqrt[4]{3}),i}(x) = x^2 + 1$:

$$\sigma_{1,1} : \begin{cases} \sqrt[4]{3} & \mapsto \sqrt[4]{3} \\ i & \mapsto i \end{cases} \qquad \sigma_{1,2} : \begin{cases} \sqrt[4]{3} & \mapsto \sqrt[4]{3} \\ i & \mapsto -i \end{cases}$$

$$\sigma_{2,1} : \begin{cases} \sqrt[4]{3} & \mapsto -\sqrt[4]{3} \\ i & \mapsto i \end{cases} \qquad \sigma_{2,2} : \begin{cases} \sqrt[4]{3} & \mapsto -\sqrt[4]{3} \\ i & \mapsto -i \end{cases}$$

$$\sigma_{3,1} : \begin{cases} \sqrt[4]{3} & \mapsto i\sqrt[4]{3} \\ i & \mapsto i \end{cases} \qquad \sigma_{3,2} : \begin{cases} \sqrt[4]{3} & \mapsto i\sqrt[4]{3} \\ i & \mapsto -i \end{cases}$$

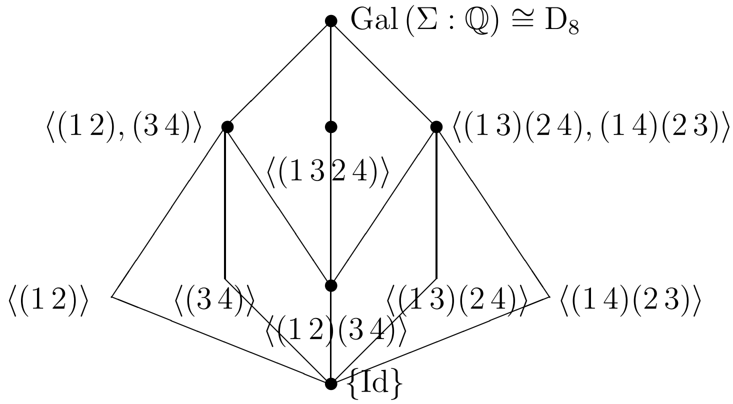
$$\sigma_{4,1} : \begin{cases} \sqrt[4]{3} & \mapsto -i\sqrt[4]{3} \\ i & \mapsto i \end{cases} \qquad \sigma_{4,2} : \begin{cases} \sqrt[4]{3} & \mapsto -i\sqrt[4]{3} \\ i & \mapsto -i \end{cases}$$

   Sia $R = \{\sqrt[4]{3},\, -\sqrt[4]{3},\, i\sqrt[4]{3},\, -i\sqrt[4]{3}\} = \{1, 2, 3, 4\}$. Scriviamo i $\sigma_{i,j}$ come permutazioni delle radici di f:

$$\begin{array}{lcc}
\sigma_{1,1} = \mathrm{Id} & & \\
\sigma_{1,2} = (i\sqrt[4]{3},\ -i\sqrt[4]{3}) & \rightarrow & (3\,4) \\
\sigma_{2,1} = (\sqrt[4]{3},\ -\sqrt[4]{3})(i\sqrt[4]{3},\ -i\sqrt[4]{3}) & \rightarrow & (1\,2)(3\,4) \\
\sigma_{2,2} = (\sqrt[4]{3},\ -\sqrt[4]{3}) & \rightarrow & (1\,2) \\
\sigma_{3,1} = (\sqrt[4]{3},\ i\sqrt[4]{3},\ -\sqrt[4]{3},\ -i\sqrt[4]{3}) & \rightarrow & (1\,3\,2\,4) \\
\sigma_{3,2} = (\sqrt[4]{3},\ i\sqrt[4]{3})(-\sqrt[4]{3},\ -i\sqrt[4]{3}) & \rightarrow & (1\,3)(2\,4) \\
\sigma_{4,1} = (\sqrt[4]{3},\ -i\sqrt[4]{3},\ -\sqrt[4]{3},\ i\sqrt[4]{3}) & \rightarrow & (1\,4\,2\,3) \\
\sigma_{4,2} = (\sqrt[4]{3},\ -i\sqrt[4]{3})(-\sqrt[4]{3},\ i\sqrt[4]{3}) & \rightarrow & (1\,4)(2\,3)
\end{array}$$

$\mathrm{Gal}\,(\Sigma : \mathbb{Q}) \cong \mathrm{D}_8$ gruppo diedrale di ordine 8.

3. Abbiamo che:



Ci sono tre sottogruppo di ordine 4 e cinque sottogruppi di ordine 2 (corrispondenti agli elemnti di periodo due). I sottogruppi normali sono quelli di ordine 4 e $\langle (1\,2)(3\,4) \rangle$.

Per il teorema di corrispondenza di Galois:

$|c(\langle \sigma_{2,2} \rangle) : \mathbb{Q}| = 4$. Sappiamo che $i\sqrt[4]{3} \in c(\langle \sigma_{2,2} \rangle)$ e $\mathbb{Q} \subseteq c(\langle \sigma_{2,2} \rangle)$, quindi $\mathbb{Q}(i\sqrt[4]{3}) \subseteq c(\langle \sigma_{2,2} \rangle)$. Dato che $\min_{\mathbb{Q}, i\sqrt[4]{3}}(x) = x^4 - 3$ si ha $|\mathbb{Q}(i\sqrt[4]{3}) : \mathbb{Q}| = 4$ e dunque:

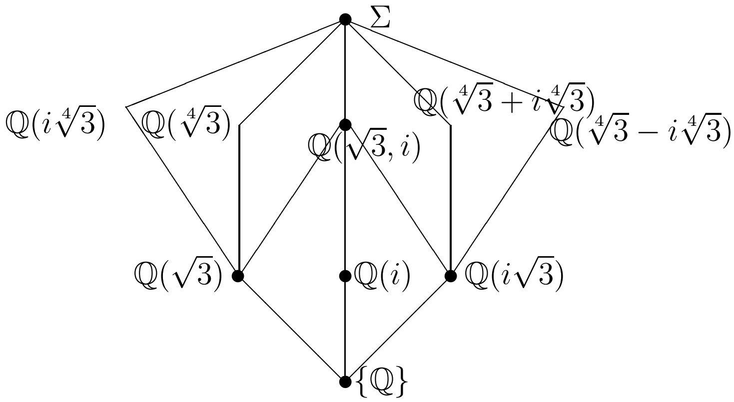
$$\mathbb{Q}(i\sqrt[4]{3}) = c(\langle \sigma_{2,2} \rangle).$$

$|c(\langle \sigma_{1,2} \rangle) : \mathbb{Q}| = 4$. Sappiamo che $\sqrt[4]{3} \in c(\langle \sigma_{1,2} \rangle)$ e $\mathbb{Q} \subseteq c(\langle \sigma_{1,2} \rangle)$, quindi $\mathbb{Q}(\sqrt[4]{3}) \subseteq c(\langle \sigma_{1,2} \rangle)$. Si ha $|\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}| = 4$ e dunque:

$$\mathbb{Q}(\sqrt[4]{3}) = c(\langle \sigma_{1,2} \rangle).$$

$|c(\langle \sigma_{2,1} \rangle) : \mathbb{Q}| = 4$ con $\sigma_{2,1} = (\sqrt[4]{3}, -\sqrt[4]{3})(i\sqrt[4]{3}, -i\sqrt[4]{3})$. Osserviamo che $i \in c(\langle \sigma_{2,1} \rangle)$, $\sqrt{3} \in c(\langle \sigma_{2,1} \rangle)$ e $\mathbb{Q} \subseteq c(\langle \sigma_{2,1} \rangle)$, quindi $\mathbb{Q}(\sqrt{3}, i) \subseteq c(\langle \sigma_{2,1} \rangle)$. Si ha $|\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}| = 4$ e dunque:

$$\mathbb{Q}(\sqrt{3}, i) = c(\langle \sigma_{2,1} \rangle).$$



$|c(\langle \sigma_{3,2} \rangle) : \mathbb{Q}| = 4$. Sappiamo che $\sqrt[4]{3} + i\sqrt[4]{3} \in c(\langle \sigma_{3,2} \rangle)$ e $\mathbb{Q} \subseteq c(\langle \sigma_{3,2} \rangle)$, quindi $\mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3}) \subseteq c(\langle \sigma_{3,2} \rangle)$. Si ha $|\mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3}) : \mathbb{Q}| = 4$ (perchè , se $u = \sqrt[4]{3} + i\sqrt[4]{3}$, si vede che $\min_{\mathbb{Q},u}(x) = x^4 + 12$ e questo è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein con $p = 3$) e dunque:

$$\mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3}) = c(\langle \sigma_{3,2} \rangle).$$

Allo stesso modo si vede che

$$\mathbb{Q}(\sqrt[4]{3} - i\sqrt[4]{3}) = c(\langle \sigma_{4,2} \rangle).$$

I sottocampi che sono estensioni normali di $\mathbb{Q}$ sono i corrispondenti dei sottogruppi normali di $\mathrm{Gal}\,(\Sigma : \mathbb{Q})$ e sono quelli evidenziati col puntino nel disegno. $\square$

28. Sia $|F| = 7^4$. Determinare la caratteristica di F e $|F : F_0|$ con F_0 sottocampo fondamentale di F Descrivere $\mathrm{Aut}(F)$.

Sia $f(x) = x^3 + x + 1 \in \mathbb{Z}_7[x]$. Dimostrare che f è irriducibile in $\mathbb{Z}_7[x]$ e dire se f è irriducibile in $F[x]$.

Svolgimento.

Caratteristica di F: 7, $F_0 = \mathbb{Z}_7$, $|F : \mathbb{Z}_7| = 4$.

$\mathrm{Aut}(F)$ è un gruppo ciclico generato dall'automorfismo di Frobenius $\sigma : x \mapsto x^7$

$\mathrm{Aut}(F) = \langle \sigma \rangle$, $|\sigma| = |F : \mathbb{Z}_7| = 4$ quindi c'è un solo sottogruppo di ordine 2:

$$\begin{tikzcd}
\mathrm{Aut}(F) = \langle \sigma \rangle \arrow[d, dash] \\
\langle \sigma^2 \rangle \arrow[d, dash] \\
\{\mathrm{Id}\}
\end{tikzcd}$$

$f(x) = x^3 + x + 1$ è irriducibile in $\mathbb{Z}_7[x]$ se e solo se non ha radici in $\mathbb{Z}_7$.

$f(0) = 1 \neq 0$	$f(4) = f(-3) = -1 \neq 0$
$f(1) = 3 \neq 0$	$f(5) = f(-2) = -2 \neq 0$
$f(2) = 4 \neq 0$	$f(6) = f(-1) = -1 \neq 0$
$f(3) = 3 \neq 0$	

Quindi $f(x)$ non ha radici in $\mathbb{Z}_7$: $f(x)$ è irriducibile in $\mathbb{Z}_7[x]$.

f è irriducibile in $F[x]$ se e solo se non ha radici in F.

Se $\alpha \in F$ è una radice di $f(x)$ abbiamo:

$\min_{\mathbb{Z}_7,\alpha}(x) = x^3 + x + 1 = f(x)$

$$\begin{tikzcd}
F \ni \alpha \arrow[d, dash] \\
\mathbb{Z}_7(\alpha) \arrow[d, dash] \\
\mathbb{Z}_7
\end{tikzcd}$$

$|\mathbb{Z}_7(\alpha) : \mathbb{Z}_7| = \deg(f) = 3$

$|F : \mathbb{Z}_7| = 4$

Allora dovrebbe essere $3 = |\mathbb{Z}_7(\alpha) : \mathbb{Z}_7| \,\big|\, |F : \mathbb{Z}_7| = 4$: assurdo.

Quindi non ci sono radici di f in F, ossia f è irriducibile in $F[x]$. $\square$

29. Sia $\omega = e^{\frac{2\pi}{6}i}$ e sia Σ il campo di spezzamento del polinomio $x^6 - 2$ su $\mathbb{Q}$.

1. Calcolare Σ e $|\Sigma : \mathbb{Q}|$.

2. Calcolare $|\Sigma : \mathbb{Q}(\omega)|$ e dedurre che $x^6 - 2$ è irriducibile in $\mathbb{Q}(\omega)[x]$.

3. Descrivere $\mathrm{Gal}\,(\Sigma : \mathbb{Q}(\omega))$.

Svolgimento.

1. Radici di $f(x) = x^6 - 2$: $\sqrt[6]{2}$, $\omega\sqrt[6]{2}$, $\omega^2\sqrt[6]{2}$, $\omega^3\sqrt[6]{2} = -\sqrt[6]{2}$, $\omega^4\sqrt[6]{2}$, $\omega^5\sqrt[6]{2}$.
   $\Sigma = \mathbb{Q}(\sqrt[6]{2}, \omega)$
   $|\Sigma : \mathbb{Q}| = |\mathbb{Q}(\sqrt[6]{2}, \omega) : \mathbb{Q}(\sqrt[6]{2})||\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}|$
   Il polinomio minimo di $\sqrt[6]{2}$ su $\mathbb{Q}$ è $x^6 - 2 \in \mathbb{Q}[x]$: è monico, si annulla su $\sqrt[6]{2}$ ed è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein ($p = 2$).
   Il polinomio minimo di ω su $\mathbb{Q}(\sqrt[6]{2})$ è $\min_{\mathbb{Q}(\sqrt[6]{2}),\omega}(x) = \Phi_6(x)$: infatti $\Phi_6(x)$ ha grado
   $$\deg(\Phi_6(x)) = \varphi(6) = \varphi(2) \cdot \varphi(3) = 1 \cdot 2 = 2$$
   e non ha radici reali.
   Allora: $|\Sigma : \mathbb{Q}| = 2 \cdot 6 = 12$.

2. Sappiamo che $|\mathbb{Q}(\omega) : \mathbb{Q}| = \deg(\Phi_6(x)) = 2$. Per la formula dei gradi:
   $$|\Sigma : \mathbb{Q}(\omega)| = |\mathbb{Q}(\sqrt[6]{2}, \omega) : \mathbb{Q}(\omega)| = \frac{|\Sigma : \mathbb{Q}|}{|\mathbb{Q}(\omega) : \mathbb{Q}|} = \frac{12}{2} = 6.$$
   Allora $\deg(\min_{\mathbb{Q}(\omega),\,\sqrt[6]{2}}(x)) = 6$.
   $f(x) = x^6 - 2 \in \mathbb{Q}(\omega)[x]$ è monico, di grado 6 e si annulla su $\sqrt[6]{2}$. Ne segue che $\min_{\mathbb{Q}(\omega),\,\sqrt[6]{2}}(x) | f(x)$, ma poichè sono entrambi monici e di grado 6 essi coincidono: $\min_{\mathbb{Q}(\omega),\,\sqrt[6]{2}}(x) = f(x) = x^6 - 2$, che quindi risulta essere irriducibile in $\mathbb{Q}(\omega)[x]$.

3. Σ è estensione di Galois di $\mathbb{Q}(\omega)$, perchè è campo di spezzamento di un polinomio in caratteristica zero. Allora $|\,\mathrm{Gal}\,(\Sigma : \mathbb{Q}(\omega))| = |\Sigma : \mathbb{Q}(\omega)| = 6$.

Ogni elemento di $\mathrm{Gal}\,(\Sigma : \mathbb{Q}(\omega))$ è completamente determinato dall'azione su $\sqrt[6]{2}$. Possiamo estendere l'identitá su $\mathbb{Q}(\omega)$ in 6 modi diversi, mandando $\sqrt[6]{2}$ in una delle radici di $\min_{\mathbb{Q}(\omega),\ \sqrt[6]{2}}(x) = x^6 - 2$:

$$\sigma_1 = \mathrm{Id}_\Sigma : \sqrt[6]{2} \mapsto \sqrt[6]{2} \qquad \sigma_2 : \sqrt[6]{2} \mapsto \omega\sqrt[6]{2} \qquad \sigma_3 : \sqrt[6]{2} \mapsto \omega^2\sqrt[6]{2}$$

$$\sigma_4 : \sqrt[6]{2} \mapsto \omega^3\sqrt[6]{2} = -\sqrt[6]{2} \qquad \sigma_5 : \sqrt[6]{2} \mapsto \omega^4\sqrt[6]{2} \qquad \sigma_6 : \sqrt[6]{2} \mapsto \omega^5\sqrt[6]{2}$$

Si ha che $\sigma_2^2 = \sigma_3$, $\sigma_2^3 = \sigma_4$, $\sigma_2^4 = \sigma_5$ e $\sigma_2^5 = \sigma_6$. Quindi σ_2 ha periodo 6 e $\mathrm{Gal}\,(\Sigma : \mathbb{Q}(\omega)) = \langle\sigma_2\rangle$ è ciclico. □

30. Sia $f(x) = x^5 + 15x - 3 \in \mathbb{Z}_p[x]$. Determinare i primi p per i quali f non ha radici multiple.

Svolgimento.
$f'(x) = 5x^4 + 15 = 5(x^4 + 3)$
Se $\underline{p = 5}$: $f' = 0 \quad \Rightarrow \quad (f, f') = f \notin \mathbb{Z}_p$, quindi f ha radici multiple.
Se $\underline{p \neq 5}$: $f' \neq 0$.

$$(f, f') \in \mathbb{Z}_p \quad \Longleftrightarrow \quad \left(f, x^4 + 3 = \frac{f'}{5}\right) \in \mathbb{Z}_p$$

Eseguendo la divisione di f per $f'/5$ si ottiene:

$$f = \frac{f'}{5}x + 12x - 3$$

$R(x) = 12x - 3 = 3(4x - 1)$
Se $R(x) = 0$, allora $x^4 + 3 | f$, quindi $(f, f'/5) = f'/5 \notin \mathbb{Z}_p$
Allora se $\underline{p = 3}$: $(f, f'/5) = f'/5 \notin \mathbb{Z}_p$, quindi f ha radici multiple.
Se $\underline{p = 2}$: $R(x) = -3 = 1$, da cui $(f, f'/5) = 1 \in \mathbb{Z}_p$, quindi f non ha radici multiple.
Se $\underline{p \neq 2, 3}$ $R(x) = 12x - 3 \neq 0$. Allora dividiamo $x^4 + 3$ per $12x - 3$. Otteniamo:

$$x^4 + 3 = \frac{12x - 3}{3}\left(\frac{1}{4}x^3 + \frac{1}{16}x^2 + \frac{1}{64}x + \frac{1}{256}\right) + \frac{769}{256}$$

$R'(x) = \frac{769}{256}$.
Se $\underline{p = 769}$ il resto è zero e quindi $(f, f') = 12x - 3 \notin \mathbb{Z}_p$: f ha radici multiple.

Se $\underline{p \neq 769}$: $(f, f') = \frac{769}{256} \in \mathbb{Z}_p$, quindi f non ha radici multiple.
Allora f non ha radici multiple per $p \neq 3, 5, 769$. $\square$

31. Dimostrare che σ è un K-automorfismo di L se e solo se σè un automorfismo di L come campo ed è un automorfismo di L come K-spazio vettoriale.

Svolgimento.
($\Rightarrow$) Supponiamo σ K-automorfismo di L.
Per definizione σ è un automorfismo di L come campo e quindi $\forall \alpha, \beta \in L$:

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$$
$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$$

Vediamo che $\forall\, k \in K, \forall\, a \in L : \sigma(ka) = k\sigma(a)$.
Poichè $k \in K \subseteq L$ e σ è un automorfismo di L: $\sigma(ka) = \sigma(k)\sigma(a)$.
Poichè σ è un K-automorfismo, esso fissa gli elementi di K: $\sigma(k)\sigma(a) = k\sigma(a)$.
Quindi σ è un automorfismo di L come K-spazio vettoriale.
($\Leftarrow$) Verifichiamo che σ è un K-automorfismo di L, ossia che $\forall\, k \in K : \sigma(k) = k$.
Poichè σ è un automorfismo di L come K-spazio vettoriale:

$$\sigma(k) = \sigma(k1_L) = k\sigma(1_L)$$

Poichè σ è un automorfismo di L come campo: $k\sigma(1_L) = k1_L = k$. $\square$