Corso:Algebra IV
I1/Esercizi/Campi intermedi

1. $H_1 = \{1, x, x^2, x^3\}$; $H_1' \supseteq \mathbb{Q}(i)$, inoltre $|\mathbb{Q}(i) : \mathbb{Q}| = 2$ e per il teorema fondamentale di Galois

$$2 = |G : H_1| = |H_1' : G'|$$

e quindi $H_1' = \mathbb{Q}(i)$.

2. $H_2 = \{1, x^2, y, x^2y\}$; considero $\xi \in M$ e per prima cosa impongo $\xi^{x^2} = \xi$.

$$\xi = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3$$

e tenendo conto che $i^{x^2} = i$ e $\alpha^{x^2} = -\alpha$:

$$\xi^{x^2} = a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3 + a_4 i - a_5 i\alpha + a_6 i\alpha^2 - a_7\alpha^3 i$$

e imponendo l'uguaglianza segue che $a_1 = a_3 = a_5 = a_7 = 0$, e quindi gli elementi fissati da x^2 sono della forma

$$\xi_1 = a_0 + a_2\alpha^2 + a_4 i + a_6\alpha^2 i,\ a_i \in \mathbb{Q} \forall i$$

Ora, impongo che gli elementi trovati vengano fissati anche da y :

$$\xi_1^y = a_0 + a_2\alpha^2 - a_4 i - a_6\alpha^2 i$$

allora, imponendo l'uguaglianza, $a_4 = a_6 = 0$.

$$H_2'' = \{a_0 + a_2\alpha^2,\ a_0, a_2 \in \mathbb{Q}\} = \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2})$$

3. $H_3 = \{1, x^2, xy, x^3y\}$; considero un generico elemento fissato da x^2 , della forma

$$\xi_1 = a_0 + a_2\alpha + a_4 i + a_6 i\alpha$$
$$\xi_1^{xy} = a_0 - a_2\alpha^2 - a_4 i + a_6\alpha^2 i$$

Imponendo l'uguaglianza

$$a_2 = a_4 = 0$$

quindi,

$$H_3' = \{a_0 + a_6\alpha^2 i\} = \mathbb{Q}(i\sqrt{2})$$

4. $H_4 = \{1, y\}$; $H_4' = \mathbb{Q}(\alpha)$, infatti y fissa α , $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 2$, $2 = |G : H_4| = |H_4' : \mathbb{Q}|$ quindi $H_4' = \mathbb{Q}(\alpha)'$.

5. $H_5 = \{1, x^2\}$; siccome gli elementi fissati da x^2 sono già stati calcolati prima, segue che

$$H_5' = \{a_0 + a_2\alpha^2 + a_4 i + a_6\alpha^2 i,\ a_i \in \mathbb{Q} \forall i\}$$

e in particolare se pongo $a_2 = a_6 = 0$, ottengo $\mathbb{Q}(i) \subset H_5'$ .Anche α^2 è fissato da x^2 ; osservo allora che $|\mathbb{Q}(\alpha^2, i) : \mathbb{Q}| = 4$, inoltre $4 = |G : H_5| = |H_5' : \mathbb{Q}|$ quindi $H_5' = \mathbb{Q}(\alpha^2, i)$.

6. $H_6 = \{1, xy\}$; calcolo gli elementi fissati da xy , tenendo conto che $i^{xy} = -i$, e $\alpha^{xy} = -\alpha i$:

$$\xi = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3$$

$$\longrightarrow \xi^{xy} = a_0 - a_1\alpha i - a_2\alpha^2 + a_3\alpha^3 i - a_4 i - a_5\alpha + a_6 i\alpha^2 + a_7\alpha^3$$

Imponendo l'uguaglianza

$$\begin{cases} a_1 = -a_5, \\ a_2 = 0 \\ a_3 = a_7 \\ a_4 = 0 \end{cases}$$

da cui segue che

$$H_6' = \{a_0 + a_1(\alpha - i\alpha) + a_3(\alpha^3 + i\alpha^3) + a_6 i\alpha^2,\ a_i \in \mathbb{Q}\}$$

Mostro che $H_6' = \mathbb{Q}(\alpha - i\alpha)$ infatti, calcolando le potenze di $\alpha - i\alpha$ ottengo:

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

$$(\alpha - i\alpha)^3 = -2i\alpha^2(\alpha - i\alpha) = -2i\alpha^3 - 2\alpha^3 = -2(i\alpha^3 + \alpha^3)$$

$$(\alpha - i\alpha)^4 = (-2i\alpha^2)^2 = -4\alpha^4 = -8$$

cioè $\alpha - i\alpha$ ha come polinomio minimo $x^4 + 8$. Quindi posso porre $\beta = \alpha - i\alpha$, e scrivere

$$H_6' = \{a_0 + a_1\beta + a_6\beta^2 + a_3\beta^3,\ a_i \in \mathbb{Q}\} = \mathbb{Q}(\beta).$$

7. $H_7 = \{1, x^2y\}$; tenendo conto che $i^{x^2y} = -i$ e $\alpha^{x^2y} = -\alpha$, e preso un generico elemento $\xi \in M$

$$\xi = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3,\ a_i \in \mathbb{Q}$$

$$\xi^{xy} = a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3 - a_4 i + a_5 i\alpha - a_6 i\alpha^2 + a_7 i\alpha^3$$

Imponendo l'uguaglianza si ha $a_1 = a_3 = a_4 = a_6 = 0$, quindi

$$H_7' = \{a_0 + a_2\alpha^2 + a_5 i\alpha + a_7 i\alpha^2,\ a_i \in \mathbb{Q}\}$$

e calcolando le potenze di $i\alpha$:

$$(i\alpha)^2 = \alpha^2,\ (i\alpha)^3 = -i\alpha^3,\ (i\alpha)^4 = \alpha^2 = 2$$

quindi $i\alpha$ ha come polinomio minimo $x^4 - 2$, $H_7' = \mathbb{Q}(i\alpha)$ e $H_7' \supseteq \mathbb{Q}$ ha grado 4.

8. $H_8 = \{1, x^3y\}$; $i^{x^3y} = -i$, $\alpha^{x^3y} = i\alpha$. Dato $\xi \in M$ della forma

$$\xi = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3$$

$$\xi^{x^3y} = a_0 + a_1\alpha i - a_2\alpha^2 - a_3 i\alpha^3 - a_4 i + a_5\alpha + a_6 i\alpha^2 - a_7\alpha^3$$

e imponendo l'uguaglianza:

$$\begin{cases} a_1 = a_5 \\ a_2 = 0 \\ a_3 = -a_7 \\ a_4 = 0 \end{cases}$$

quindi

$$H_8' = \{a_0 + a_1(\alpha + i\alpha) + a_3(\alpha^3 + i\alpha^3) + a_6 i\alpha^2,\ a_i \in \mathbb{Q} \forall i\} = \mathbb{Q}(\alpha + i\alpha)$$

infatti

$$(\alpha + i\alpha)^2 = \alpha^2 + 2i\alpha^2 - \alpha^2 = 2i\alpha^2$$

$$(\alpha + i\alpha)^3 = 2i\alpha^3 - 2\alpha^3$$

$$(\alpha + i\alpha)^4 = (2i\alpha^2)^2 = -4\alpha^4 = -8$$

cioè $\alpha + i\alpha$ ha polinomio minimo $x^4 + 8$ e quindi $H_8' \supseteq \mathbb{Q}$ ha grado 4.

* *

Esercizio 7.4

Calcolare $\phi_n(x)$ per $n = 1 \ldots, 20$.

Per calcoli precedenti sappiamo che

$$\phi_1(x) = x - 1$$

$$\phi_2(x) = x + 1$$

$$\phi_4(x) = x^2 + 1$$

$$\phi_6(x) = x^2 - x + 1$$

$$\phi_8(x) = x^4 + 1$$

Inoltre, ricordiamo che in generale, per p primo

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

quindi conosciamo anche $\phi_3(x)$, $\phi_5(x)$, $\phi_7(x)$, $\phi_{11}(x)$, $\phi_{13}(x)$, $\phi_{17}(x)$, $\phi_{19}(x)$.

Calcoliamo i polinomi rimanenti:

1. $\phi_9 = \frac{x^9-1}{\phi_1(x)*\phi_3(x)}$ e $\phi_1(x) * \phi_3(x) = x^3 - 1$, quindi

$$\phi_9(x) = \frac{x^9 - 1}{x^3 - 1}$$

Aggiungendo e togliendo x^6 al numeratore:

$$\phi_9(x) = \frac{x^9 - x^6 + x^6 - 1}{x^3 - 1}$$

$$\phi_9(x) = \frac{x^6(x^3 - 1) + (x^3 + 1)(x^3 - 1)}{x^3 - 1}$$

$$\phi_9(x) = \frac{(x^6 + x^3 + 1)(x^3 - 1)}{x^3 - 1}$$

$$\phi_9(x) = x^6 + x^3 + 1$$

2. $\phi_{10}(x) = \frac{x^{10}-1}{\phi_1(x)*\phi_2(x)*\phi_5(x)}$

$$= \frac{x^{10} - 1}{(x^5 - 1)\phi_2(x)}$$

$$= \frac{(x^5 - 1)(x^5 + 1)}{(x^5 - 1)\phi_2(x)}$$

$$= \frac{x^5 + 1}{x + 1}$$

Eseguo la divisione:

$$\frac{x^5 + 1}{x + 1} =$$

$$q_1 = x^4,\ r_1 = x^5 + 1 - x^4(x + 1) = -x^4 + 1$$

$$q_2 = -x^3,\ r_2 = -x^4 + 1 + x^3(x + 1) = x^3 + 1$$

$$q_3 = x^2,\ r_3 = x^3 + 1 - x^2(x + 1) = -x^2 + 1$$

$$q_4 = -x,\ r_4 = -x^2 + 1 + x(x + 1) = x + 1$$

$$q_5 = 1$$

Complessivamente,

$$x^5 + 1 = (x + 1) * (x^4 - x^3 + x^2 - x + 1)$$

quindi

$$\phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

3. $\phi_{12}(x) = \frac{x^{12}-1}{\phi_1(x)*\phi_2(x)*\phi_3(x)*\phi_4(x)*\phi_6(x)}$

$$= \frac{(x^6 + 1)(x^6 - 1)}{\phi_4(x) * (x^6 - 1)}$$

$$= \frac{x^6 + 1}{x^2 + 1}$$

Eseguo la divisione

$$\frac{x^6+1}{x^2+1} =$$

$$q_1 = x^4,\ r_1 = x^6 + 1 - x^4(x^2+1) = -x^4 + 1$$

$$q_2 = -x^2,\ r_2 = -x^4 + 1 + x^2(x^2+1) = x^2 + 1$$

$$q_3 = 1,\ r_3 = 0$$

Quindi

$$x^6 + 1 = (x^4 - x^2 + 1) * (x^2 + 1)$$

$$\longrightarrow \phi_{12}(x) = x^4 - x^2 + 1$$

4. $\phi_{14} = \frac{x^{14}-1}{\phi_1(x)*\phi_2(x)*\phi_7(x)}$

$$= \frac{x^7+1}{\phi_2(x)}$$

$$= \frac{x^7+1}{x+1}$$

e questa divisione è simile a quella per il calcolo di $\phi_{10}(x)$, quindi

$$\phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$

5. $\phi_{15}(x) = \frac{x^{15}-1}{\phi_1(x)*\phi_3(x)*\phi_5(x)}$ e $\phi_1(x)*\phi_5(x) = x^5-1$, mentre $\phi_3(x) = x^2+x+1$, quindi

$$= \frac{x^{15}-1}{(x^2+x+1)(x^5-1)}$$

Eseguo la divisione:

$$\frac{x^{15}-1}{x^5-1} =$$

$$q_1 = x^{10},\ r_1 = x^{15} - 1 - x^{10}(x^5-1) = x^{10} - 1$$

$$q_2 = x^5,\ r_2 = x^{10} - 1 - x^5(x^5-1) = x^5 - 1$$

$$q_3 = 1,\ r_3 = 0$$

quindi

$$x^{15} - 1 = (x^{10} + x^5 + 1)(x^5 - 1)$$

$$\longrightarrow \phi_{15}(x) = \frac{x^{10}+x^5+1}{x^2+x+1}$$

Ora eseguo la divisione:

$$\frac{x^{10}+x^5+1}{x^2+x+1} =$$

$$q_1 = x^8,\ r_1 = x^{10} + x^5 + 1 - x^8(x^2+x+1) = -x^9 - x^8 + x^5 + 1$$

$$q_2 = -x^7,\ r_2 = -x^9 - x^8 + x^5 + 1 + x^7(x^2+x+1) = x^7 + x^5 + 1$$

$$q_3 = x^5,\ r_3 = x^7 + x^5 + 1 - x^5(x^2+x+1) = -x^6 + 1$$

$$q_4 = -x^4,\ r_4 = -x^6 + 1 + x^4(x^2+x+1) = x^5 + x^4 + 1$$

$$q_5 = x^3,\ r_5 = x^5 + x^4 + 1 - x^3(x^2+x+1) = -x^3 + 1$$

$$q_6 = -x,\ r_6 = -x^3 + 1 + x(x^2+x+1) = x^2 + x + 1$$

$$q_7 = 1,\ r_7 = 0$$

Quindi

$$x^{10} + x^5 + 1 = (x^2 + x + 1)(x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)$$

$$\longrightarrow \phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

6. $\phi_{16}(x) = \frac{x^{16}-1}{[\phi_1(x)*\phi_2(x)*\phi_4(x)]*\phi_8(x)}$ Il termine tra parentesi quadra è $x^4 - 1$, e uso l'espressione di $\phi_8(x)$:

$$= \frac{(x^8 + 1)(x^4 + 1)(x^4 - 1)}{(x^4 - 1)(x^4 + 1)}$$

$$= x^8 + 1$$

7. $\phi_{18}(x) = \frac{(x^9-1)*(x^9+1)}{\phi_1(x)*\phi_2(x)*\phi_3(x)*\phi_6(x)*\phi_9(x)}$

$$= \frac{(x^9 - 1) * (x^9 + 1)}{[\phi_1(x) * \phi_3(x) * \phi_9(x)] * \phi_2(x) * \phi_6(x)}$$

$$= \frac{x^9 + 1}{(x^2 - x + 1)(x + 1)}$$

Eseguo la divisione:

$$\frac{x^9 + 1}{x^2 - x + 1} =$$

$$q_1 = x^7,\ r_1 = x^9 + 1 - x^7(x^2 - x + 1) = x^8 - x^7 + 1$$

$$q_2 = x^6,\ r_2 = x^8 - x^7 + 1 - x^6(x^2 - x + 1) = -x^6 + 1$$

$$q_3 = -x^4,\ r_3 = -x^6 + 1 + x^4(x^2 - x + 1) = -x^5 + x^4 + 1$$

$$q_4 = -x^3,\ r_4 = -x^5 + x^4 + 1 + x^3(x^2 - x + 1) = x^3 + 1$$

$$q_5 = x,\ r_5 = x^3 + 1 - x(x^2 - x + 1) = x^2 - x + 1$$

$$q_6 = 1,\ r_6 = 0$$

quindi

$$x^9 + 1 = (x^2 - x + 1)(x^7 + x^6 - x^4 - x^3 + x + 1)$$

$$\phi_{18}(x) = \frac{x^7 + x^6 - x^4 - x^3 + x + 1}{x + 1}$$

$$\phi_{18}(x) = \frac{x^6(x + 1) - x^3(x + 1) + x + 1}{x + 1}$$

$$\phi_{18}(x) = \frac{(x^6 - x^3 + 1)(x + 1)}{x + 1}$$

$$\phi_{18}(x) = x^6 - x^3 + 1$$

8. $\phi_{20}(x) = \frac{(x^{10}-1)(x^{10}+1)}{\phi_1(x)*\phi_2(x)*\phi_4(x)*\phi_5(x)*\phi_{10}(x)}$

$$\phi_{20}(x) = \frac{(x^{10}-1)(x^{10}+1)}{\phi_2(x)*\phi_4(x)*\phi_{10}(x)}$$

e $\phi_4(x) = x^2+1$, e $\phi_{10}(x) = \frac{x^5+1}{x+1}$, allora

$$= \frac{(x^5+1)(x^{10}+1)}{(x^5+1)/(x+1)*(x+1)*(x^2+1)}$$

$$= \frac{x^{10}+1}{x^2+1}$$

$$= x^8 - x^6 + x^4 - x^2 + 1$$

(il risultato si ottiene facendo la sostituzione $y = x^2$, infatti abbiamo già eseguito la divisione $\frac{y^5+1}{y+1}$)

* *

Esercizio 7.5

Siano p, q primi distinti. Esprimere $\phi_{pq}(x)$ in termini di $\phi_p(x)$.

Per il primo lemma, siccome gli unici divisori del prodotto pq sono $1, p, q, pq$, si ha

$$\phi_{pq}(x) = \frac{x^{pq}-1}{\phi_1(x)*\phi_p(x)*\phi_q(x)}$$

$$\phi_{pq}(x) = \frac{x^{pq}-1}{\phi_p(x)*(x^q-1)}$$

Moltiplico e divido per $\phi_1(x) = x-1$:

$$\phi_{pq}(x) = \frac{(x^{pq}-1)(x-1)}{(x-1)*\phi_p(x)*(x^q-1)}$$

$$\phi_{pq}(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1)*(x^q-1)}$$

$$\phi_{pq}(x) = \frac{((x^q)^p-1)(x-1)}{(x^p-1)*(x^q-1)}$$

$$\phi_{pq}(x) = \frac{(x^q)^p-1}{x^q-1} * \frac{x-1}{x^p-1}$$

$$= \frac{\phi_p(x^q)}{\phi_p(x)}$$

* *

Esercizio 7.6

Determinare le radici seste dell'unità su F_5 .

Trovare le radici seste dell'unità in F_5 equivale a trovare il campo di spezzamento del polinomio $f(x) = x^6 - 1$ su F_5 .

Osservo che gli elementi 1 e 4 in F_5 sono radici seste dell'unità, in particolare $x + 4 = x - 1 \mid f(x)$ e $x + 1 \mid f(x)$, e si ha

$$f(x) = x^6 - 1 = (x^3 + 1)(x^3 - 1) = (x + 1)(x^2 - x + 1)(x - 1)(x^2 + x + 1)$$

Pongo $g(x) = x^2 + x + 1$ e $h(x) = x^2 - x + 1$.

Considero $K_0 = \frac{F_5[x]}{(x^2+x+1)} = F_5(\alpha)$ con α radice di $g(x)$, cioè $\alpha^2 = 4\alpha + 4$.

$$K_0 = \{a + b\alpha,\ a, b \in F_5,\ \alpha^2 = 4\alpha + 4\}$$

Verifico se K_0 contiene radici di $h(x)$, cioè, preso un elemento $a + b\alpha \in K_0$, verifico se soddisfa l'equazione $h(a + b\alpha) = 0$.

$$(a + b\alpha)^2 - a - b\alpha + 1 = 0$$
$$a^2 + 2ab\alpha + b^2\alpha^2 - a - b\alpha + 1 = 0$$

e siccome $\alpha^2 = 4\alpha + 4$,

$$a^2 + 1 + 2ab\alpha + b^2(4\alpha + 4) - a - b\alpha + 1 = 0$$
$$a^2 + 1 + 2ab\alpha + 4b^2\alpha + 4b^2 - a - b\alpha + 1 = 0$$
$$(2ab + 4b^2 - b)\alpha + 4b^2 - a + 2 + a^2 = 0$$

e quest'equazione è soddisfatta se

$$\begin{cases} a^2 + 4b^2 + 4a + 1 = 0 \\ 2ab + 4b^2 + 4b = 0 \end{cases}$$

Osservo che $a = 0, b = -1$, è una soluzione, quindi $-\alpha \in K_0$ è radice di $h(x)$. Allora K_0 è campo di spezzamento per $f(x)$.

Determino l'altra radice di $g(x)$ eseguendo la divisione:

$$\frac{x^2 + x + 1}{x - \alpha} =$$
$$q_1 = x,\ r_1 = x^2 + x + 1 - x(x - \alpha) = (1 + \alpha)x + 1$$
$$q_2 = 1 + \alpha,\ r_2 = (1 + \alpha)x + 1 - (1 + \alpha)(x - \alpha) = \alpha^2 + \alpha + 1 = 0$$

quindi $x^2 + x + 1 = (x - \alpha)(x - 1 - \alpha)$, cioè l'altra radice di $g(x)$ è $1 + \alpha$.

Analogamente si verifica che l'altra radice di $h(x)$ è $-1 - \alpha$.

Procedimento alternativo: si possono trovare le radici dei due polinomi $g(x), h(x)$ con la formula risolutiva per le equazioni di secondo grado.

Concludo che le radici seste dell'unità sono

$$\{1,\, -1,\, \alpha, -\alpha,\, \alpha+1,\, -\alpha-1\}$$

Si ha che $\varphi(6) = 2$, quindi ci sono due radici primitive seste. Osservo che

$$\alpha^2 = -\alpha - 1$$
$$\alpha^3 = \alpha * (-\alpha - 1) = -\alpha^2 - \alpha = \alpha + 1 - \alpha = 1 \;\longrightarrow o(\alpha) = 3$$
$$(-\alpha)^2 = -1 - \alpha$$
$$(-\alpha)^3 = (-1-\alpha) * (-\alpha) = \alpha + \alpha^2 = -1$$
$$(-1)^2 = 1 \;\longrightarrow o(\alpha) = 2 * 3 = 6$$
$$(\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = \alpha$$
$$\alpha^3 = 1, \;\longrightarrow, o(\alpha) = 6$$

Quindi in particolare, le radici primitive seste sono $-\alpha, \alpha + 1$.

* *

Esercizio 7.7

Sia $\omega \in \mathbb{C}$ radice primitiva p -esima dell'unità, cioè $\omega = \cos(2\pi/p) + i\sin(2\pi/p)$ e considero $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$. Calcolare traccia e norma, $t(\omega)$ e $n(\omega)$, di ω in $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$.

Per le osservazioni precedenti sappiamo che $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong U_p$ e quindi è un gruppo ciclico di ordine $p-1$, chiamo i suoi elementi $\{g_1, g_2, \ldots, g_{p-1}\}$.

Gli elementi di $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$ sono determinati dalla loro azione su ω , e sono tali che $\omega \mapsto \omega^i$ per $i = 1, \ldots, p-1$, in particolare sia g_i tale che $\omega \mapsto \omega^i$.

CALCOLO DELLA TRACCIA: Per definizione

$$t(\omega) = \omega^{g_1} + \omega^{g_2} + \cdots + \omega^{g_n}$$
$$= \sum_{i=1}^{p-1} \omega^i = \omega + \omega^2 + \cdots + \omega^{p-1}$$

e in particolare, $t(\omega) + 1 = \phi_p(\omega)$, e siccome ω è radice del polinomio ciclotomico, $\phi_p(\omega) = 0$ quindi $t(\omega) = -1$.

CALCOLO DELLA NORMA:

$$n(\omega) = \prod_{i=1}^{p-1} \omega^{g_i} = \prod_{i=1}^{p-1} \omega^i$$
$$= \omega^{\sum_{i=1}^{p-1} i} = \omega^{p(p-1)/2} = (1)^{(p-1)/2} = 1$$

* *

Esercizio 7.8

Sia $\alpha = \sqrt{2 + \sqrt{2}}$.

1. Calcolare il polinomio minimo $f(x)$ di α su $\mathbb{Q}$.
2. Sia M campo di spezzamento di $f(x)$ su $\mathbb{Q}$, mostrare che $\mathcal{G}(M/\mathbb{Q})$ è ciclico di ordine 4.
3. Determinare la corrispondenza di Galois tra campi intermedi e sottogruppi.

1. POLINOMIO MINIMO: Osservo che

$$\alpha^2 = 2 + \sqrt{2} \longrightarrow \alpha^2 - 2 = \sqrt{2}$$

ed elevando al quadrato l'ultima identità si ha:

$$\alpha^4 + 4 - 4\alpha^2 = 2, \longrightarrow \alpha^4 - 4\alpha^2 + 2 = 0$$

cioè α è radice del polinomio $f(x) = x^4 - 4x^2 + 2$. $f(x)$ è monico, e **mostro che è irriducibile**. Pongo $x^2 = t$ e risolvo l'equazione

$$t^2 - 4t + 2 = 0$$

$$t_{1,2} = \frac{4 \pm \sqrt{8}}{2}$$

$$t_{1,2} = \frac{4 \pm 2\sqrt{2}}{2}$$

$$t_{1,2} = 2 \pm \sqrt{2}$$

quindi $f(x)$ si fattorizza nel modo seguente:

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

quindi $f(x)$ non ammette una fattorizzazione in $\mathbb{Q}[x]$ ed è irriducibile in $\mathbb{Q}[x]$, quindi è il polinomio minimo di α su $\mathbb{Q}$ (potevo anche usare il Criterio di Eisenstein).

2. GRUPPO DI GALOIS: Pongo $\alpha = \sqrt{2 + \sqrt{2}}$ e $\beta = \sqrt{2 - \sqrt{2}}$, allora le radici di $f(x)$ sono $\pm\alpha$ e $\pm\beta$. gr(f(x)) = $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$, siccome dobbiamo mostrare che $\mathcal{G}(M/\mathbb{Q})$ è ciclico di ordine 4, **mostriamo che** $M = \mathbb{Q}(\alpha)$ **, equivalentemente che** $\beta \in \mathbb{Q}(\alpha)$. Moltiplico e divido β per $\sqrt{2 + \sqrt{2}}$:

$$\beta = \sqrt{2 - \sqrt{2}} = \frac{\sqrt{2 - \sqrt{2}} * \sqrt{2 + \sqrt{2}}}{\sqrt{2 + \sqrt{2}}}$$

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

quindi $\beta \in \mathbb{Q}(\alpha)$ e $M = \mathbb{Q}(\alpha)$ .Segue quindi che $4 = |M : \mathbb{Q}| = o(\mathcal{G}(M/\mathbb{Q})$, e $G := \mathcal{G}(M/\mathbb{Q}) = \{g_1, g_2, g_3, g_4\}$. Gli elementi di G sono determinati dalla loro azione su α , e mandano α in una delle radici di $f(x)$; supponiamo che gli elementi di G siano definiti nel seguente modo:

$$\alpha^{g_1} = \alpha,\ \alpha^{g_2} = -\alpha,\ \alpha^{g_3} = \beta,\ \alpha^{g_4} = -\beta.$$

Per mostrare che G è ciclico, **basta trovare un elemento di ordine 4**. Esplicito le relazioni tra gli elementi di G :#*Per g_2 si ha:

$$\alpha^{g_2^2} = (-\alpha)^{g_2} = \alpha$$

quindi $o(g_2) = 2$. Considero allora g_3 :#*Per g_3 si ha

$$\alpha^{g_3^2} = \beta^{g_3} = (\beta^2 - 2)/\beta$$

e sostituendo l'espressione di β :

$$= \frac{2 - \sqrt{2} - 2}{\sqrt{2 - \sqrt{2}}}$$

$$= \frac{-\sqrt{2}}{\sqrt{2 - \sqrt{2}}}$$

moltiplico e divido per $\sqrt{2 + \sqrt{2}}$:

$$= \frac{-\sqrt{2} * \sqrt{2 + \sqrt{2}}}{\sqrt{2 - \sqrt{2}} * \sqrt{2 + \sqrt{2}}}$$

$$= \frac{-\sqrt{2} * \sqrt{2 + \sqrt{2}}}{\sqrt{2}}$$

$$= -\sqrt{2 + \sqrt{2}} = -\alpha$$

quindi $\alpha^{g_3^2} = \alpha^{g_2}$, e $g_3^2 = g_2$. Allora g_3 non ha ordine 2 e quindi ha necessariamente ordine 4, cioè G è ciclico generato da g_3 , e pongo $g := g_3$, e si ha $g_2 = g^2$.#*Si verifica anche che $g_4 = g^3$, infatti

$$\alpha^{g^3} = \beta^{g^2} = (-\alpha)^g = -\beta$$

quindi $\alpha^{g^3} = \alpha^{g_4}$ e $g_4 = g^3$ .Concludo che $G = \{1, g, g^2, g^3\}$ con $\alpha^g = \beta$ .L'estensione $M \supseteq \mathbb{Q}$ è normale perché M è campo di spezzamento su $\mathbb{Q}$ di $f(x)$ e siamo in caratteristica 0.

3. CORRISPONDENZA DI GALOIS: L'unico sottogruppo proprio di G è $H = \{1, g^2\}$, e determino il corrispondente campo intermedio $H' = \text{Fix(H)}$. Basta determinare gli elementi di M fissati da g^2 . Essendo M campo di spezzamento di $f(x)$ si ha

$$M = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3,\ a_i \in \mathbb{Q},\ \forall i, \alpha^4 = 4\alpha^2 - 2\}$$

Dato $\xi \in M$, siccome g^2 è tale che $\alpha \mapsto -\alpha$, si ha

$$\xi^{g^2} = a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3$$

e $\xi^{g^2} = \xi$ se e solo se $a_1 = a_3 = 0$. Si ha quindi

$$H' = \{a_0 + a_2\alpha^2,\ a_i \in \mathbb{Q},\ \forall i\} = \mathbb{Q}(\alpha^2)$$

Diagramma dei campi: $\mathbb{Q}(\alpha) \supseteq \mathbb{Q}(\alpha^2) \supseteq \mathbb{Q}$ (i tre campi sono uniti da un segmento)Diagramma dei sottogruppi: $1 \leq H \leq G$

* *

Esercizio 7.9

Determinare il gruppo di Galois $\mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$ dove ω è una radice sedicesima dell'unità.

1 Fonti per testo e immagini; autori; licenze

1.1 Testo

- **Corso:Algebra IV I1/Esercizi/Campi intermedi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Esercizi/Campi_intermedi?oldid=48841 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio

1.2 Immagini

1.3 Licenza dell'opera