Corso:Algebra IV I1/Teoria di Galois/Esempio di studio di estensione

1 Determinazione del grado dell'estensione

Sia $\omega = \cos(2\pi/5) + i\sin(2\pi/5)$, e studio l'estensione $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$. Ora ω è una radice quinta dell'unità, e quindi è radice del polinomio $x^5 - 1$, che è un polinomio in $\mathbb{Q}[x]$, e quindi ω è algebrico su $\mathbb{Q}$.

Osservo che $x^5 - 1$ si può fattorizzare come

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) = (x-1)\phi_5(x)$$

dove $\phi_5(x)$ è un polinomio a coefficienti razionali. Siccome $\omega \neq 1$, ω è radice di $\phi_5(x)$, cioè $\phi_5(\omega) = 0$.

Vogliamo provare che $\phi_5(x)$ è proprio il polinomio minimo di ω su $\mathbb{Q}$.

Osservazione 2.7

Osservo che dato un anello A commutativo unitario, e dati due elementi $a, b \in A$, posso considerare l'omomorfismo (di valutazione) $\phi : A[x] \to A[x]$ tale che $x \mapsto ax + b$ e $c \mapsto c$ per ogni $c \in A$.

Se $f(x)$ è un polinomio in $A[x]$, allora

$$(f(x))^\phi = f(ax + b)$$

Se a è invertibile nell'anello A , allora ϕ è un isomorfismo, con inverso l'omomorfismo (di valutazione) $\phi^{-1} : A[x] \to A[x]$ tale che $x \mapsto a^{-1}x - a^{-1}b$, e $c \mapsto c$, $\forall c \in A$.

In particolare, se F è un campo, preso $a \neq 0$ segue che $\phi : F[x] \to F[x]$ tale che $x \mapsto ax + b$ e $c \mapsto c$, $\forall c \in F$ è un isomorfismo, e quindi un polinomio $f(x) \in F[x]$ è irriducibile in $F[x]$ se e solo se lo è $f(x)^\phi = f(ax + b)$, con $a, b \in F$, $a \neq 0$.

In base all'osservazione precedente, mostrare che $\phi_5(x)$ è irriducibile su $\mathbb{Q}$ equivale a mostrare che $\phi_5(x + 1)$ è irriducibile su $\mathbb{Q}$.

$$\phi_5(x) = x^4 + x^3 + x^2 + x + 1 = \frac{x^5 - 1}{x - 1}$$

$$\phi_5(x+1) = \frac{(x+1)^5 - 1}{x + 1 - 1} = \frac{(x+1)^5 - 1}{x}$$

$$= 1/x \sum_{k=1}^{5} \binom{5}{k} x^k$$

(infatti $\binom{5}{0} = 1$ e si elide con il -1 già presente)

$$= \sum_{k=1}^{5} \binom{5}{k} x^{k-1}$$

$$= x^4 + \binom{5}{4} x^3 + \binom{5}{3} x^2 + \binom{5}{2} x + \binom{5}{1}$$

e per $p = 5$ posso applicare Eisenstein ($p = 5 \mid \binom{5}{k}$, per $k = 1, \ldots, 4$, non divide il coefficiente direttivo e p^2 non divide il termine noto), e quindi $\phi_5(x+1)$ è irriducibile sopra $\mathbb{Q}$, e lo è anche $\phi_5(x)$.

Osservazione 2.8

Più in generale se p è un numero primo, si ha che $x^p - 1 = (x-1) * (x^{p-1} + x^{p-2} + \cdots + x + 1)$. Chiamo $\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, questo polinomio è irriducibile su $\mathbb{Q}$ per argomenti analoghi a quelli precedenti.

Infatti, come prima

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

$$= 1/x * \sum_{k=1}^{p} \binom{p}{k} x^k = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}$$

e $p \mid \binom{p}{k}$ per $k = 1, \ldots, p-1$, per il criterio di Eisenstein $\phi_p(x+1)$ è irriducibile su $\mathbb{Q}$.

Tornando a $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$, abbiamo mostrato che $\phi_5(x)$ è il polinomio minimo di ω . In particolare, $\mathbb{Q}(\omega)$ contiene tutti (e soli) gli elementi della forma $a + b\omega + c\omega^2 + d\omega^3$, $a, b, c, d \in \mathbb{Q}$, tali che ω è radice di $\phi_5(x)$.

Segue che $|\mathbb{Q}(\omega) : \mathbb{Q}| = 4$. Di più, $\mathbb{Q}(\omega)$ è il campo di spezzamento di $\phi_5(x)$ sopra $\mathbb{Q}$, perché $\omega \in \mathbb{Q}(\omega)$ implica che $\omega^2, \omega^3, \omega^4 \in \mathbb{Q}(\omega)$ e quindi $\mathbb{Q}(\omega)$ contiene tutte le radici di $\phi_5(x)$.

2 Ordine ed elementi del gruppo di Galois G

Come vedremo, **l'estensione** $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$ **è normale**. Se chiamo $G = \mathcal{G}(\mathbb{Q}(\omega)/\mathbb{Q})$, si ha che $o(G) = 4$ per il teorema fondamentale della teoria di Galois.

Sia $g \in G$, allora ω^g è ancora una radice di $\phi_5(x)$. D'altra parte, presa una radice ω^i di $\phi_5(x)$, considero la mappa tale che $H : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega^i)$ che fissa $\mathbb{Q}$ elemento per elemento e manda ω in ω^i . Osservo che $h \in G$, perché $\mathbb{Q}(\omega^i) = \mathbb{Q}(\omega)$, infatti

INCLUSIONE 1: $\omega^i \in \mathbb{Q}(\omega)$ e quindi $\mathbb{Q}(\omega^i) \subseteq \mathbb{Q}(\omega)$;

INCLUSIONE 2: $|\mathbb{Q}(\omega^i) : \mathbb{Q}| = 4$ perché ϕ_5 è polinomio minimo di ogni sua radice. ω^i è invertibile perché i e 5 sono primi tra loro, allora, per opportuni s, t posso scrivere

$$1 = 5s + it, \longrightarrow \omega = \omega^{5s+it} = \omega^{it}$$

cioè $\omega \in \mathbb{Q}(\omega^i)$ e quindi $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\omega^i)$.

Si ha anche che h è invertibile.

Posso scrivere gli elementi di G :

$$G = \{1, g_2, g_3, g_4\},$$

dove $\omega^{g_i} = \omega^i$.

Verifico le relazioni tra gli elementi di G :

$$\omega^{g_2^2} = (\omega^{g_2})^2 = \omega^4 = \omega^{g_4}, \longrightarrow g_2^2 = g_4$$
$$\omega^{g_2^3} = \omega^{g_4 * g_2} = (\omega^4)^{g_2} = (\omega^2)^4$$
$$= \omega^8 = \omega^5 * \omega^3 = \omega^3 = \omega^{g_3}, \longrightarrow g_2^3 = g_3$$

Allora g **è ciclico di ordine 4**, se pongo $g_2 = g$, allora gli elementi di g sono $\{1, g, g^2, g^3\}$.

3 Corrispondenza di Galois

Essendo ciclico di ordine 4, G ha un solo sottogruppo proprio di ordine 2, che è $H = \{1, g^2\}$.

Segue che $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$ **ha un solo campo intermedio** $L = H' = \mathrm{Fix(H)}$ **, e** $|L : \mathbb{Q}| = |G : H| = 2$.

Determiniamo esplicitamente gli elementi di L , per definizione:

$$L = H' = \{a+b\omega+c\omega^2+d\omega^3 \in \mathbb{Q}(\omega)\, t.c.\, (a+b\omega+c\omega^2+d\omega^3)^{g^2} = a+b\omega+c\omega^2+d\omega^3\}$$

Osservo che

$$(a + b\omega + c\omega^2 + d\omega^3)^{g^2}$$
$$= a + b\omega^4 + c(\omega^4)^2 + d(\omega^4)^3$$
$$= a + b\omega^4 + c\omega^3 + d\omega^2$$

siccome ω è radice di $\phi_5(x)$, si ha $\omega^4 = -1 - \omega - \omega^2 - \omega^3$, e sostituendo nell'espressione sopra ottengo

$$= a - b - b\omega - b\omega^2 - b\omega^3 + c\omega^3 + d\omega^2$$

$$= (a-b) - b\omega + (d-b)\omega^2 + (c-b)\omega^3$$

L'insieme $\{1, \omega, \omega^2, \omega^3\}$ è una base per $|\mathbb{Q}(\omega) : \mathbb{Q}|$, quindi chiedere che

$$(a + b\omega + c\omega^2 + d\omega^3)^{g^2} = a + b\omega + c\omega^2 + d\omega^3$$

equivale a chiedere che

$$\begin{cases} a - b = a \\ -b = b \\ d - b = c \\ c - b = d \end{cases}$$

da cui

$$b = 0, d = c$$

quindi L **è il campo intermedio che contiene gli elementi della forma**

$$a + c\omega^2 + c\omega^3 = a + c(\omega^2 + \omega^3),\ a, c \in \mathbb{Q}.$$

Se chiamo $\alpha = \omega^2 + \omega^3$, si ha

$$\alpha^2 = (\omega^2+\omega^3)^2 = \omega^4+\omega^6+2\omega^5 = \omega^4+\omega+2 = -1-\omega-\omega^2-\omega^3+\omega+2 = 1-\omega^2-\omega^3 = 1-\alpha$$

allora $\alpha^2 + \alpha - 1 = 0$, e il polinomio minimo di α è $m(x) = x^2 + x - 1$.

4 Fonti per testo e immagini; autori; licenze

4.1 Testo

- **Corso:Algebra IV I1/Teoria di Galois/Esempio di studio di estensione** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Teoria_di_Galois/Esempio_di_studio_di_estensione?oldid=48506 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio

4.2 Immagini

4.3 Licenza dell'opera