Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 27-05-2020

Esercizio sul gruppo di Galois di $X^n - 2$

$n > 1$, $\alpha := \sqrt[n]{2} \in \mathbb{R}_{>0}$, $\omega := e^{(2\pi i)/n} \in \mathbb{C}$, $G := \mathrm{G}_{\mathbb{Q}}(X^n - 2)$.

1. $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \omega)$ campo di spezzamento di $X^n - 2$.
2. n primo $\implies$ $\#G = n\varphi(n) = n(n-1)$.
3. $n = 4$ o 6 $\implies$ $\#G = n\varphi(n)$.
4. $n = 8$ $\implies$ $\#G < n\varphi(n)$.
5. $\#G = n\varphi(n)$ $\implies$ $G \cong C_n \rtimes_\theta \mathbb{Z}/n\mathbb{Z}^*$ con $\theta \colon \mathbb{Z}/n\mathbb{Z}^* \to \mathrm{Aut}(C_n)$ isomorfismo.

Esercizio sul gruppo di Galois di $X^n - 2$

$n > 1$, $\alpha := \sqrt[n]{2} \in \mathbb{R}_{>0}$, $\omega := e^{(2\pi i)/n} \in \mathbb{C}$, $G := \mathrm{G}_{\mathbb{Q}}(X^n - 2)$.

1. $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \omega)$ campo di spezzamento di $X^n - 2$.
2. n primo $\implies$ $\#G = n\varphi(n) = n(n-1)$.
3. $n = 4$ o 6 $\implies$ $\#G = n\varphi(n)$.
4. $n = 8$ $\implies$ $\#G < n\varphi(n)$.
5. $\#G = n\varphi(n)$ $\implies$ $G \cong C_n \rtimes_\theta \mathbb{Z}/n\mathbb{Z}^*$ con $\theta\colon \mathbb{Z}/n\mathbb{Z}^* \to \mathrm{Aut}(C_n)$ isomorfismo.

1. Le radici in $\mathbb{C}$ di $X^n - 2$ sono $\alpha\omega^j$ per $j = 0, \ldots, n-1$ $\implies$ il campo di spezzamento in $\mathbb{C}$ di $X^n - 2$ su $\mathbb{Q}$ è $L := \mathbb{Q}(\alpha\omega^j \,:\, j = 0, \ldots, n-1) = \mathbb{Q}(\alpha, \omega)$.
2. $\mathbb{Q} \subseteq L$ di Galois, $G = \mathrm{G}_{\mathbb{Q}}(L)$ $\implies$ $\#G = [L : \mathbb{Q}]$.
   $X^n - 2$ irriducibile per Eisenstein $\implies$ $\mathrm{m}_{\alpha,\mathbb{Q}} = X^n - 2$ $\implies$ $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(X^n - 2) = n$.
   $\mathrm{m}_{\omega,\mathbb{Q}} = \Phi_n$ $\implies$ $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n) = n - 1$.
   $\mathrm{mcd}(n, n-1) = 1$ $\implies$ $[L : \mathbb{Q}] = n(n-1)$.

Dimostrazione di 3, 4 e 5

3. $\varphi(4) = \varphi(6) = 2 \implies [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n) = 2 \implies$
   $n = \mathrm{mcm}(n, 2) \mid [L : \mathbb{Q}] \leq 2n \implies [L : \mathbb{Q}] = 2n = n\varphi(n)$
   (altrimenti $[L : \mathbb{Q}] = n \implies \omega \in L = \mathbb{Q}(\alpha) \subset \mathbb{R}$, assurdo).
4. $\omega = \sqrt{2}(1+i)/2$, $\omega^2 = i \implies \sqrt{2}\omega = 1 + i = 1 + \omega^2 \implies \omega$
   radice di $X^2 - \sqrt{2}X + 1 \in \mathbb{Q}(\alpha)[X]$ (perché $\sqrt{2} = \alpha^4$) $\implies$
   $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2 \cdot 8 = 16 < 32 = 8\varphi(8)$.
5. $H := \mathrm{G}_{\mathbb{Q}(\alpha)}(L) < G$ tale che $\#H = \#G/[\mathbb{Q}(\alpha) : \mathbb{Q}] = \varphi(n)$,
   $H' := \mathrm{G}_{\mathbb{Q}(\omega)}(L) \triangleleft G$ (perché $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ normale) tale che
   $\#H' = \#G/[\mathbb{Q}(\omega) : \mathbb{Q}] = n$ e $H \cap H' = \{1\} \implies$
   $\#(HH') = n\varphi(n) = \#G \implies G = HH' \implies G = H' \rtimes H$.
   $H' = \{\sigma_{\bar{j}} : \bar{j} \in \mathbb{Z}/n\mathbb{Z}\}$ con $\sigma_{\bar{j}}(\alpha) = \alpha\omega^j$ (e $\sigma_{\bar{j}}(\omega) = \omega$) $\implies$
   $\sigma_{\bar{j}} = \sigma_{\bar{1}}^j \ \forall \bar{j} \in \mathbb{Z}/n\mathbb{Z} \implies H' = \langle \sigma_{\bar{1}} \rangle \cong C_n$.
   $H \cong G/H' \cong \mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong \mathbb{Z}/n\mathbb{Z}^* \implies G \cong C_n \rtimes_\theta \mathbb{Z}/n\mathbb{Z}^*$
   con $\theta \colon \mathbb{Z}/n\mathbb{Z}^* \to \mathrm{Aut}(C_n) \cong \mathbb{Z}/n\mathbb{Z}^*$ omomorfismo iniettivo
   (quindi isomorfismo) perché $\tau \in H \implies \exists\, \bar{l} \in \mathbb{Z}/n\mathbb{Z}^*$ tale che
   $\tau(\omega) = \omega^l$ (e $\tau(\alpha) = \alpha$) $\implies \tau\sigma_{\bar{1}}\tau^{-1} = \sigma_{\bar{l}} = \sigma_{\bar{1}} \iff \tau = 1$

Esercizio sui gruppi di Galois di polinomi biquadratici

Determinare campo di spezzamento $\mathbb{Q} \subseteq L$ e gruppo di Galois G di f su $\mathbb{Q}$ nei seguenti casi:

1. $f = X^4 - 4X^2 + 2$;
2. $f = X^4 - 4X^2 - 2$.

Esercizio sui gruppi di Galois di polinomi biquadratici

Determinare campo di spezzamento $\mathbb{Q} \subseteq L$ e gruppo di Galois G di f su $\mathbb{Q}$ nei seguenti casi:

1. $f = X^4 - 4X^2 + 2$;
2. $f = X^4 - 4X^2 - 2$.

1. f irriducibile per Eisenstein.
   $f(X) = g(X^2)$ con $g(Y) := Y^2 - 4Y + 2$ che ha radici $2 \pm \sqrt{2} \in \mathbb{R}_{>0} \implies$ le radici di f sono $\pm\alpha, \pm\beta$ con $\alpha := \sqrt{2+\sqrt{2}}, \beta := \sqrt{2-\sqrt{2}} \in \mathbb{R}_{>0} \implies L = \mathbb{Q}(\alpha, \beta)$.
   $\alpha^2 - 2 = \sqrt{2} = \alpha\beta \implies \beta = (\alpha^2 - 2)/\alpha \in \mathbb{Q}(\alpha) \implies$
   $L = \mathbb{Q}(\alpha) \implies \#G = [L : \mathbb{Q}] = \deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = \deg(f) = 4$.
   $\exists \sigma \in G = \mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ tale che $\sigma(\alpha) = \beta$ (perché β radice di $\mathrm{m}_{\alpha,\mathbb{Q}} = f$) $\implies$

$$\sigma^2(\alpha) = \sigma(\beta) = \sigma\left(\frac{\alpha^2 - 2}{\alpha}\right) = \frac{\beta^2 - 2}{\beta} = \frac{-\sqrt{2}}{\beta} = -\alpha$$

$$\implies \sigma^2 \neq \mathrm{id}_L \implies G \cong C_4.$$

Dimostrazione di 2

f irriducibile per Eisenstein.
$f(X) = g(X^2)$ con $g(Y) := Y^2 - 4Y - 2$ che ha radici
$2 \pm \sqrt{6} \in \mathbb{R} \implies$ le radici di f sono $\pm\alpha, \pm\beta i$ con
$\alpha := \sqrt{\sqrt{6}+2}, \beta := \sqrt{\sqrt{6}-2} \in \mathbb{R}_{>0} \implies L = \mathbb{Q}(\alpha, \beta i)$.
$\alpha\beta = \sqrt{2} \implies \alpha\beta i = \sqrt{2} i \implies L = \mathbb{Q}(\alpha, \sqrt{2} i)$.
$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = \deg(f) = 4$,
$[\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}] = \deg(\mathrm{m}_{\sqrt{2}i,\mathbb{Q}}) = 2$ (perché $\mathrm{m}_{\sqrt{2}i,\mathbb{Q}} = X^2 + 2$) $\implies$

$$\mathrm{mcm}(4, 2) = 4 \mid \#G = [\mathbb{Q}(\alpha, \sqrt{2}i) : \mathbb{Q}] \leq 4 \cdot 2 = 8$$

e non può essere $[\mathbb{Q}(\alpha, \sqrt{2}i) : \mathbb{Q}] = 4$ (perché $\sqrt{2}i \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$)
$\implies \#G = 8$.
$G \cong G' < S_4 \implies G \cong D_4$.

Esercizio sui quadrati in $\mathbb{F}_p$

p primo dispari.

1. $\mathbb{F}_p^*$ contiene un elemento di ordine 4 $\iff$ $p \equiv 1 \mod 4$.
2. $\overline{-1}$ è un quadrato in $\mathbb{F}_p$ $\iff$ $p \equiv 1 \mod 4$.
3. ω radice ottava primitiva dell'unità (in un'estensione di $\mathbb{F}_p$), $\alpha := \omega + \omega^{-1} \implies \alpha^2 = \bar{2}$.
4. $\alpha^p = \begin{cases} \alpha & \text{se } p \equiv \pm 1 \mod 8 \\ -\alpha & \text{se } p \equiv \pm 3 \mod 8. \end{cases}$
5. $\bar{2}$ è un quadrato in $\mathbb{F}_p$ $\iff$ $p \equiv \pm 1 \mod 8$.
6. $X^4 + 1$ è irriducibile in $\mathbb{Q}[X]$ ma non in $\mathbb{F}_p[X]$.

Esercizio sui quadrati in $\mathbb{F}_p$

p primo dispari.

1. $\mathbb{F}_p^*$ contiene un elemento di ordine 4 $\iff$ $p \equiv 1 \mod 4$.
2. $\overline{-1}$ è un quadrato in $\mathbb{F}_p$ $\iff$ $p \equiv 1 \mod 4$.
3. ω radice ottava primitiva dell'unità (in un'estensione di $\mathbb{F}_p$), $\alpha := \omega + \omega^{-1}$ $\implies$ $\alpha^2 = \bar{2}$.
4. $$\alpha^p = \begin{cases} \alpha & \text{se } p \equiv \pm 1 \mod 8 \\ -\alpha & \text{se } p \equiv \pm 3 \mod 8. \end{cases}$$
5. $\bar{2}$ è un quadrato in $\mathbb{F}_p$ $\iff$ $p \equiv \pm 1 \mod 8$.
6. $X^4 + 1$ è irriducibile in $\mathbb{Q}[X]$ ma non in $\mathbb{F}_p[X]$.

1. $\mathbb{F}_p^*$ è ciclico di ordine $p-1$, dunque contiene un elemento di ordine 4 $\iff$ $4 \mid (p-1)$.
2. Per il punto 1 basta dimostrare che $\overline{-1}$ è un quadrato in $\mathbb{F}_p$ $\iff$ $\mathbb{F}_p^*$ contiene un elemento di ordine 4.
   $\overline{-1} = a^2$ per qualche $a \in \mathbb{F}_p$ $\implies$ $a \in \mathbb{F}_p^*$, $a^4 = \bar{1}$, $a^2 \neq \bar{1}$ $\implies$ $\operatorname{ord}(a) = 4$. Viceversa, $a \in \mathbb{F}_p^*$ tale che $\operatorname{ord}(a) = 4$ $\implies$ $a^2 = \overline{-1}$ perché $a^2 \neq \bar{1}$ e $(a^2)^2 = \bar{1}$.

Dimostrazione di 3, 4, 5 e 6

3. ω radice di $X^8 - 1 = (X^4 - 1)(X^4 + 1)$ e $\omega^4 \neq \bar{1} \implies \omega$ radice di $X^4 + 1 \implies \alpha^2 = \omega^2 + 2\omega\omega^{-1} + \omega^{-2} = \bar{2}$ perché $\omega^2 + \omega^{-2} = \omega^{-2}(\omega^4 + \bar{1}) = \bar{0}$.
4. $\alpha^p = (\omega + \omega^{-1})^p = \omega^p + \omega^{-p} = \omega^i + \omega^{-i}$ se $p \equiv i \mod 8$.
   $i = 1 \implies \alpha^p = \omega + \omega^{-1} = \alpha$.
   $i = -1 \implies \alpha^p = \omega^{-1} + \omega = \alpha$.
   $i = 3 \implies \alpha^p = \omega^3 + \omega^{-3} = \omega^4(\omega^{-1} + \omega) = -\alpha$.
   $i = -3 \implies \alpha^p = \omega^{-3} + \omega^3 = \omega^4(\omega + \omega^{-1}) = -\alpha$.
5. $\bar{2} = \alpha^2$ (per il punto 3) è un quadrato in $\mathbb{F}_p \iff \alpha \in \mathbb{F}_p \iff \alpha^p = \alpha$ (perché i p elementi di $\mathbb{F}_p$ sono le p radici di $X^p - X$) $\iff p \equiv \pm 1 \mod 8$ (per il punto 4).
6. $X^4 + 1 = \Phi_8$ irriducibile in $\mathbb{Q}[X]$ perché $X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$ in $\mathbb{R}[X]$ e $\sqrt{2} \notin \mathbb{Q}$.
   $X^4 + 1$ non irriducibile in $\mathbb{F}_p[X]$ perché $\mathrm{m}_{\omega,\mathbb{F}_p} \mid (X^4 + 1)$ e $\deg(\mathrm{m}_{\omega,\mathbb{F}_p}) = [\mathbb{F}_p(\omega) : \mathbb{F}_p] \leq 2$ ($p^2 \equiv 1 \mod 8 \implies \omega^{p^2} = \omega \implies \omega \in \mathbb{F}_{p^2}$).

Esercizio sulle estensioni semplici

$K \subseteq L$ estensione.

1. $a, b \in K$ e $\alpha, \beta \in L$ tali che $a \neq b$ e
   $K' := K(\alpha + a\beta) = K(\alpha + b\beta) \implies K' = K(\alpha, \beta)$.
2. $K \subseteq L$ di Galois $\implies$ $K \subseteq L$ semplice.
3. Trovare $\gamma \in L$ tale che $L = K(\gamma)$ quando L è campo di spezzamento di $X^3 - 2$ su $K = \mathbb{Q}$.

Esercizio sulle estensioni semplici

$K \subseteq L$ estensione.

1. $a, b \in K$ e $\alpha, \beta \in L$ tali che $a \neq b$ e $K' := K(\alpha + a\beta) = K(\alpha + b\beta) \implies K' = K(\alpha, \beta)$.
2. $K \subseteq L$ di Galois $\implies$ $K \subseteq L$ semplice.
3. Trovare $\gamma \in L$ tale che $L = K(\gamma)$ quando L è campo di spezzamento di $X^3 - 2$ su $K = \mathbb{Q}$.

1. $\alpha + a\beta, \alpha + b\beta \in K' \implies (a-b)\beta = \alpha + a\beta - (\alpha + b\beta) \in K'$ $\implies \beta \in K' \implies \alpha = \alpha + b\beta - b\beta \in K' \implies K' = K(\alpha, \beta)$.
2. Posso supporre K infinito.
   $\alpha \in L$ tale che $[K(\alpha) : K]$ massimo $\implies L = K(\alpha)$:
   per assurdo $\exists\, \beta \in L \setminus K(\alpha) \implies \exists\, a, b \in K$ tali che $a \neq b$ e $K' := K(\alpha + a\beta) = K(\alpha + b\beta)$ (altrimenti ci sarebbero infiniti sottocampi distinti di L della forma $K(\alpha + c\beta)$ al variare di $c \in K$, che corrisponderebbero a infiniti sottogruppi distinti di $\mathrm{G}_K(L)$) $\implies$ per il punto 1 $K' = K(\alpha, \beta)$ e $[K' : K] > [K(\alpha) : K]$ (perché $K(\alpha) \subsetneq K'$), assurdo.

Dimostrazione di 3

- $L = \mathbb{Q}(\alpha, \omega)$ con $\alpha := \sqrt[3]{2} \in \mathbb{R}$ e $\omega := e^{(2\pi i)/3}$.
- $L = \mathbb{Q}(\gamma)$ con $\gamma := \alpha + \omega$: basta dimostrare che $L' \subsetneq L$ sottocampo $\implies \gamma \notin L'$.
- A parte $\mathbb{Q}$, L' può essere solo della forma L^H con H sottogruppo non banale di $\mathrm{G}_{\mathbb{Q}}(L) \cong S_3$, quindi $L' = \mathbb{Q}(\omega)$ (se $\#H = 3$) o $L' = \mathbb{Q}(\alpha\omega^j)$ per $j = 0, 1, 2$ (se $\#H = 2$).
- Chiaramente $\gamma \notin \mathbb{Q}(\omega)$ e $\gamma \notin \mathbb{Q}(\alpha)$ (altrimenti $\mathbb{Q}(\omega) = \mathbb{Q}(\alpha) = L$).
- $\gamma \notin \mathbb{Q}(\alpha\omega)$: una $\mathbb{Q}$-base di $\mathbb{Q}(\alpha\omega)$ è $\{1, \alpha\omega, \alpha^2\omega^2\}$ e una $\mathbb{Q}(\alpha\omega)$-base di L è $\{1, \omega\}$ $\implies$ una $\mathbb{Q}$-base di L è $\{1, \alpha\omega, \alpha^2\omega^2, \omega, \alpha\omega^2, \alpha^2\}$ e rispetto a questa base $\gamma = -\alpha\omega + \omega - \alpha\omega^2$ (tenendo conto che $\omega^2 + \omega + 1 = 0$).
- $\gamma \notin \mathbb{Q}(\alpha\omega^2)$: una $\mathbb{Q}$-base di $\mathbb{Q}(\alpha\omega^2)$ è $\{1, \alpha\omega^2, \alpha^2\omega\}$ e una $\mathbb{Q}(\alpha\omega^2)$-base di L è $\{1, \omega\}$ $\implies$ una $\mathbb{Q}$-base di L è $\{1, \alpha\omega^2, \alpha^2\omega, \omega, \alpha, \alpha^2\omega^2\}$ e rispetto a questa base $\gamma = \omega + \alpha$.