Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 03-06-2020

Esercizio sui campi

K campo perfetto, $0 \neq f \in K[X]$ tale che $\mathrm{G}_K(f) \cong C_6$.

1. $\deg(f) \geq 5$.
2. f irriducibile $\implies$ $\deg(f) = 6$.
3. Fornire un esempio con f irriducibile.
4. Fornire un esempio con $\deg(f) = 5$.
5. $\exists\, g \in K[X]$ tale che $\deg(g) = 5$ e g ha lo stesso campo di spezzamento di f su K.

Esercizio sui campi

K campo perfetto, $0 \neq f \in K[X]$ tale che $\mathrm{G}_K(f) \cong C_6$.

1. $\deg(f) \geq 5$.
2. f irriducibile $\implies$ $\deg(f) = 6$.
3. Fornire un esempio con f irriducibile.
4. Fornire un esempio con $\deg(f) = 5$.
5. $\exists\, g \in K[X]$ tale che $\deg(g) = 5$ e g ha lo stesso campo di spezzamento di f su K.

1. Per assurdo $\deg(f) \leq 4 \implies C_6 \cong \mathrm{G}_K(f) \cong G < S_4$, assurdo perché S_4 non contiene elementi di ordine 6.
2. $K \subseteq L$ campo di spezzamento di $f \implies K \subseteq L$ di Galois $\implies [L : K] = \#\mathrm{G}_K(L) = \#\mathrm{G}_K(f) = 6$; f irriducibile $\implies \deg(f) \mid [L : K] = 6 \implies \deg(f) = 6$ per il punto 1.
3. $K = \mathbb{Q}$, $f = \Phi_7 = (X^7 - 1)/(X - 1) = X^6 + \cdots + 1$ irriducibile e tale che $\mathrm{G}_{\mathbb{Q}}(f) \cong \mathbb{Z}/7\mathbb{Z}^* \cong C_6$ (perché 7 è primo).

Dimostrazione di 4 e 5

4. Basta prendere $K = \mathbb{F}_q$ (con q potenza positiva di un numero primo) e $f = f_1 f_2$ con f_1 e f_2 irriducibili in $\mathbb{F}_q[X]$, $\deg(f_1) = 2$ e $\deg(f_2) = 3$ (perché $\mathrm{G}_{\mathbb{F}_q}(f) \cong C_d$ con $d = \mathrm{mcd}(2,3) = 6$). Per esempio $K = \mathbb{F}_2$, $f_1 = X^2 + X + 1$ e $f_2 = X^3 + X + 1$ (irriducibili perché di gradi 2 e 3 e senza radici in $\mathbb{F}_2$) $\implies$ $f = X^5 + X^4 + 1$.
5. $\mathrm{G}_K(f) = \langle \sigma \rangle \implies K_1 := L^{\langle \sigma^2 \rangle}$ e $K_2 := L^{\langle \sigma^3 \rangle}$ tali che $K \subseteq K_i$ normali per $i = 1, 2$ (perché $\mathrm{G}_{K_i}(L) \triangleleft \mathrm{G}_K(L) = \mathrm{G}_K(f)$);
$[K_1 : K] = [\langle \sigma \rangle : \langle \sigma^2 \rangle] = 6/3 = 2$ e
$[K_2 : K] = [\langle \sigma \rangle : \langle \sigma^3 \rangle] = 6/2 = 3$.
$\alpha_i \in K_i \setminus K \implies K(\alpha_i) = K_i$ (perché $[K_i : K]$ primo) $\implies$
$[K(\alpha_1, \alpha_2) : K] = 2 \cdot 3 = 6$ (perché $[K(\alpha_1) : K] = 2$ e $[K(\alpha_2) : K] = 3$ coprimi) $\implies K(\alpha_1, \alpha_2) = L$.
$g_i := \mathrm{m}_{\alpha_i, K}$ si spezza su K_i (perché $K \subseteq K_i$ normale) e $\deg(g_i) = [K(\alpha_i) : K] \implies \deg(g_1) = 2$ e $\deg(g_2) = 3 \implies$ $g := g_1 g_2$ tale che $\deg(g) = 5$ e $K \subseteq L = K(\alpha_1, \alpha_2)$ campo di spezzamento di g.

Esercizio sui campi

$f := X^4 - X - 1$.

1. Determinare $\mathrm{G}_{\mathbb{F}_2}(f)$.
2. f è irriducibile in $\mathbb{Q}[X]$.
3. Indicando con α e β radici (complesse) distinte di f, trovare $g \in \mathbb{Q}(\alpha)[X]$ monico tale che $\deg(g) = 3$ e $g(\beta) = 0$.
4. $(\alpha + \beta)^2$ è radice di $h := X^3 + 4X - 1$.
5. $\mathrm{G}_{\mathbb{Q}}(h) \cong S_3$.
6. $\mathrm{G}_{\mathbb{Q}}(f) \cong S_4$.

Esercizio sui campi

$f := X^4 - X - 1$.

1. Determinare $\mathrm{G}_{\mathbb{F}_2}(f)$.
2. f è irriducibile in $\mathbb{Q}[X]$.
3. Indicando con α e β radici (complesse) distinte di f, trovare $g \in \mathbb{Q}(\alpha)[X]$ monico tale che $\deg(g) = 3$ e $g(\beta) = 0$.
4. $(\alpha + \beta)^2$ è radice di $h := X^3 + 4X - 1$.
5. $\mathrm{G}_{\mathbb{Q}}(h) \cong S_3$.
6. $\mathrm{G}_{\mathbb{Q}}(f) \cong S_4$.

1. f irriducibile in $\mathbb{F}_2[X]$ (perché senza radici in $\mathbb{F}_2$ e non divisibile per $X^2 + X + 1$, l'unico polinomio irriducibile di grado 2) $\implies$ $\mathrm{G}_{\mathbb{F}_2}(f) \cong C_4$.
2. f irriducibile in $\mathbb{F}_2[X]$ $\implies$ f irriducibile in $\mathbb{Z}[X]$ e in $\mathbb{Q}[X]$.
3. $f(\alpha) = 0$ $\implies$ $(X - \alpha) \mid f$ in $\mathbb{Q}(\alpha)[X]$ $\implies$ $\exists!\, g \in \mathbb{Q}(\alpha)[X]$ tale che $f = (X - \alpha)g$ $\implies$ $0 = f(\beta) = (\beta - \alpha)g(\beta)$ $\implies$ $g(\beta) = 0$ perché $\alpha \neq \beta$. Facendo la divisione con resto di f per $X - \alpha$ si trova $g = X^3 + \alpha X^2 + \alpha^2 X + \alpha^3 - 1$.

Dimostrazione di 4

$0 = g(\beta) = \beta^3 + \alpha\beta^2 + \alpha^2\beta + \alpha^3 - 1$ (per il punto 3) $\Longrightarrow$
$\beta^3 = 1 - \alpha\beta^2 - \alpha^2\beta - \alpha^3 \Longrightarrow$

$$(\alpha+\beta)^3 = \alpha^3 + 3\alpha^2\beta + 3\alpha\beta^2 + \beta^3 =$$
$$\alpha^3 + 3\alpha^2\beta + 3\alpha\beta^2 + 1 - \alpha\beta^2 - \alpha^2\beta - \alpha^3 = 2\alpha^2\beta + 2\alpha\beta^2 + 1$$

$\Longrightarrow$ $\gamma := (\alpha+\beta)^2$ tale che

$$\gamma^3 - 1 = (\alpha+\beta)^6 - 1 = [(\alpha+\beta)^3 - 1][(\alpha+\beta)^3 + 1] =$$
$$(2\alpha^2\beta + 2\alpha\beta^2)(2\alpha^2\beta + 2\alpha\beta^2 + 2) = 4\alpha\beta(\alpha+\beta)(\alpha^2\beta + \alpha\beta^2 + 1).$$

Tenendo conto che $0 = f(\alpha) = \alpha^4 - \alpha - 1$, e quindi $\alpha^4 = \alpha + 1$,

$$\alpha\beta(\alpha^2\beta + \alpha\beta^2 + 1) = \alpha^3\beta^2 + \alpha^2\beta^3 + \alpha\beta =$$
$$\alpha^3\beta^2 + \alpha^2 - \alpha^3\beta^2 - \alpha^4\beta - \alpha^5 + \alpha\beta = \alpha^2 - \alpha\beta - \beta - \alpha^2 - \alpha + \alpha\beta = -\alpha - \beta,$$

per cui $\gamma^3 - 1 = -4\gamma$, cioè $h(\gamma) = 0$.

Dimostrazione di 5 e 6

5. h senza radici in $\mathbb{Q}$ (perché $h(1) = 4 \neq 0$, $h(-1) = -6 \neq 0$) $\implies$ h irriducibile in $\mathbb{Q}[X]$; $\Delta(f) = -4 \cdot 4^3 - 27(-1)^2 < 0$ non è un quadrato in $\mathbb{Q}$ $\implies$ $\mathrm{G}_{\mathbb{Q}}(h) \cong S_3$.
6. $\mathbb{Q} \subseteq L (\subset \mathbb{C})$ campo di spezzamento di f.
   $h((\alpha+\beta)^2) = 0$ (per il punto 4), h irriducibile (come visto nel punto 5) e monico $\implies$ $h = \mathrm{m}_{(\alpha+\beta)^2,\mathbb{Q}}$ $\implies$ h si spezza su L (perché $\mathbb{Q} \subseteq L$ normale e $(\alpha+\beta)^2 \in L$) $\implies$ $\exists\, \mathbb{Q} \subseteq L'$ campo di spezzamento di h tale che $L' \subseteq L$.
   $\mathbb{Q} \subseteq L'$ normale $\implies$ $\mathrm{G}_{L'}(L) \triangleleft G := \mathrm{G}_{\mathbb{Q}}(L) = \mathrm{G}_{\mathbb{Q}}(f)$ e $G/\mathrm{G}_{L'}(L) \cong \mathrm{G}_{\mathbb{Q}}(L') = \mathrm{G}_{\mathbb{Q}}(h) \cong S_3$ (per il punto 5) $\implies$ $6 = \#S_3 \mid \#G$.
   f irriducibile (per il punto 2) $\implies$ $4 = \deg(f) \mid [L : \mathbb{Q}] = \#G$ $\implies$ $\mathrm{mcm}(6,4) = 12 \mid \#G$.
   $G \cong G' < S_4$ $\implies$ $G \cong A_4$ o S_4 e non può essere A_4 perché $\nexists\, H \triangleleft A_4$ tale che $A_4/H \cong S_3$.