Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 26-05-2020

Esercizio sui polinomi con gruppo di Galois S_n

K campo, $0 \neq f \in K[X]$ tale che $\deg(f) = n > 0$ e $\mathrm{G}_K(f) \cong S_n$; α radice di f (in un campo di spezzamento L di f su K).

1. f è irriducibile in $K[X]$.
2. $n > 2 \implies \mathrm{G}_K(K(\alpha)) = \{1\}$.
3. $n > 3 \implies \alpha^n \notin K$.

Esercizio sui polinomi con gruppo di Galois S_n

K campo, $0 \neq f \in K[X]$ tale che $\deg(f) = n > 0$ e $\mathrm{G}_K(f) \cong S_n$; α radice di f (in un campo di spezzamento L di f su K).

1. f è irriducibile in $K[X]$.
2. $n > 2 \implies \mathrm{G}_K(K(\alpha)) = \{1\}$.
3. $n > 3 \implies \alpha^n \notin K$.

1. $\mathrm{G}_K(f) \cong S_n \implies$ le radici $\alpha = \alpha_1 \ldots, \alpha_n \in L$ di f sono distinte e $\forall\, i = 1, \ldots, n\ \exists\, \sigma \in \mathrm{G}_K(f)$ tale che $\sigma(\alpha) = \alpha_i$ $\implies$ α_i radice di $\mathrm{m}_{\alpha,K} \implies f \mid \mathrm{m}_{\alpha,K} \implies f$ irriducibile.
2. $\sigma \in \mathrm{G}_K(K(\alpha)) \implies \exists\, i = 1, \ldots, n$ tale che $\sigma(\alpha) = \alpha_i$, e basta dimostrare $i = 1$. Per assurdo $i = 2 \implies K(\alpha) \subseteq L$ campo di spezzamento di $\prod_{i=3}^{n}(X - \alpha_i) \implies$ $[L : K] = [L : K(\alpha)][K(\alpha) : K] \leq (n-2)!n < n!$, assurdo perché $[L : K] \geq \#\mathrm{G}_K(L) = n!$.
3. Per assurdo $\alpha^n = a \in K \implies$ posso supporre $f = X^n - a$ $\implies$ $L = K(\alpha, \omega)$ con $\langle \omega \rangle = \{\beta \in L : \beta^n = 1\} < L^* \implies$ $[L : K] \leq [K(\alpha) : K][K(\omega) : K] \leq n(n-1) < n!$, assurdo.

Esercizio

$\mathbb{Q} \subseteq L\ (\subset \mathbb{C})$ campo di spezzamento di f di grado 3; $\mathrm{G}_{\mathbb{Q}}(f) \cong S_3$; $\delta \in L$ tale che $\delta^2 = \Delta(f)$; $\alpha \in \mathbb{C}$ tale che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

1. $\mathbb{Q} \subseteq L(\alpha)$ di Galois.
2. $\alpha \in L \implies \alpha \in \mathbb{Q}(\delta)$.
3. $\alpha \notin L \implies \mathrm{G}_{\mathbb{Q}}(L(\alpha)) \cong S_3 \times C_2$.

Esercizio

$\mathbb{Q} \subseteq L\ (\subset \mathbb{C})$ campo di spezzamento di f di grado 3; $\mathrm{G}_{\mathbb{Q}}(f) \cong S_3$; $\delta \in L$ tale che $\delta^2 = \Delta(f)$; $\alpha \in \mathbb{C}$ tale che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

1. $\mathbb{Q} \subseteq L(\alpha)$ di Galois.
2. $\alpha \in L \implies \alpha \in \mathbb{Q}(\delta)$.
3. $\alpha \notin L \implies \mathrm{G}_{\mathbb{Q}}(L(\alpha)) \cong S_3 \times C_2$.

1. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \implies \mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ campo di spezzamento di $g := \mathrm{m}_{\alpha,\mathbb{Q}} \implies \mathbb{Q} \subseteq L(\alpha)$ campo di spezzamento di fg.
2. $\delta \notin \mathbb{Q}$ (perché $\mathrm{G}_{\mathbb{Q}}(f)$ non è isomorfo a un sottogruppo di A_3) e $\delta^2 = \Delta(f) \in \mathbb{Q} \implies [\mathbb{Q}(\delta) : \mathbb{Q}] = 2 = [\mathbb{Q}(\alpha) : \mathbb{Q}] \implies \mathrm{G}_{\mathbb{Q}(\delta)}(L)$ e $\mathrm{G}_{\mathbb{Q}(\alpha)}(L)$ sono due sottogruppi di indice 2 di $\mathrm{G}_{\mathbb{Q}}(L) \cong S_3 \implies \mathrm{G}_{\mathbb{Q}(\delta)}(L) = \mathrm{G}_{\mathbb{Q}(\alpha)}(L) \implies \mathbb{Q}(\delta) = \mathbb{Q}(\alpha)$.
3. $1 < [L(\alpha) : L] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \implies G := \mathrm{G}_{\mathbb{Q}}(L(\alpha))$ tale che $\#G = [L(\alpha) : \mathbb{Q}] = [L(\alpha) : L][L : \mathbb{Q}] = 2 \cdot 6 = 12$. $H := \mathrm{G}_{\mathbb{Q}(\alpha)}(L(\alpha)), H' := \mathrm{G}_L(L(\alpha)) \triangleleft G$ (perché $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ e $\mathbb{Q} \subseteq L$ normali), $H \cap H' = \{1\}$, $\#H = 6$, $\#H' = 2 \implies \#(HH') = \#G \implies G = HH' \implies G = H \times H' \cong S_3 \times C_2$ ($H \cong G/H' \cong \mathrm{G}_{\mathbb{Q}}(L) \cong S_3$).

Esercizio sui campi finiti

Determinare il gruppo di Galois G di $f := X^5 - X + 3$ su $\mathbb{F}_q$ per $q = 2, 3, 4, 5$.

Esercizio sui campi finiti

Determinare il gruppo di Galois G di $f := X^5 - X + 3$ su $\mathbb{F}_q$ per $q = 2, 3, 4, 5$.

In ogni caso $G \cong C_d$ se $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ campo di spezzamento di f, e $d = \mathrm{mcm}(d_1, \ldots, d_r)$ se $f = \prod_{i=1}^{r} f_i$ con $f_1, \ldots, f_r$ irriducibili.

$q = 2$ f non ha radici (perché $f(\bar{0}) = f(\bar{1}) = \bar{1}$), ma è divisibile per $X^2 + X + 1$ (l'unico irriducibile di grado 2 in $\mathbb{F}_2[X]$) e risulta $f = (X^2 + X + 1)(X^3 + X^2 + 1) \implies d = \mathrm{mcm}(2, 3) = 6$.

$q = 3$ $f = X^5 - X = X(X - 1)(X + 1)(X^2 + 1) \implies d = 2$.

$q = 4$ $\mathbb{F}_{2^6 = 4^3}$ campo di spezzamento di f su $\mathbb{F}_2 \implies$ anche su $\mathbb{F}_4$ $\implies d = 3$.

$q = 5$ $\alpha \in \mathbb{F}_{5^d} \implies f(\alpha) = \mathcal{F}(\alpha) - \alpha + \bar{3} \implies f(a) = \bar{3} \neq \bar{0}$ se $a \in \mathbb{F}_5$ e $f(\alpha + a) = f(\alpha)\ \forall\, \alpha \in \mathbb{F}_{5^d}$ e $\forall\, a \in \mathbb{F}_5 \implies$ $\mathbb{F}_{5^d} = \mathbb{F}_5(\alpha)$ se α radice di $f \implies d = \deg(\mathrm{m}_{\alpha, \mathbb{F}_5})$ non dipende dalla radice α di $f \implies f$ irriducibile in $\mathbb{F}_5[X]$ (non ha radici in $\mathbb{F}_5$ e non può essere $f = gh$ in $\mathbb{F}_5[X]$ con $\deg(g) = 2$ e $\deg(h) = 3$) $\implies d = 5$.

Esercizio su $\overline{\mathbb{Q}}$

$f \in \mathbb{C}[X]$ monico $\implies$ sono equivalenti:

1. $f \in \overline{\mathbb{Q}}[X]$;
2. f si spezza su $\overline{\mathbb{Q}}$;
3. $\exists\, g \in \mathbb{Q}[X] \setminus \{0\}$ tale che $f \mid g$.

Esercizio su $\overline{\mathbb{Q}}$

$f \in \mathbb{C}[X]$ monico $\implies$ sono equivalenti:

1. $f \in \overline{\mathbb{Q}}[X]$;
2. f si spezza su $\overline{\mathbb{Q}}$;
3. $\exists\, g \in \mathbb{Q}[X] \setminus \{0\}$ tale che $f \mid g$.

$1 \implies 2$ Perché $\overline{\mathbb{Q}}$ algebricamente chiuso.

$2 \implies 1$ $f = \prod_{j=1}^{n}(X - \alpha_j)$ con $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ (perché f monico) $\implies$ $f \in \overline{\mathbb{Q}}$.

$2 \implies 3$ $f = \prod_{j=1}^{n}(X - \alpha_j)$ con $\alpha_j \in \overline{\mathbb{Q}}\ \forall\, j = 1, \ldots, n \implies \alpha_j$ algebrico su $\mathbb{Q} \implies \exists\, g_j \in \mathbb{Q}[X] \setminus \{0\}$ tale che $g_j(\alpha_j) = 0$ $\implies (X - \alpha_j) \mid g_j \implies f \mid g := \prod_{j=1}^{n} g_j \in \mathbb{Q}[X] \setminus \{0\}$.

$3 \implies 2$ $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ radici di $f \implies \alpha_j$ radice di $g\ \forall\, j = 1, \ldots, n$ $\implies \alpha_j$ algebrico su $\mathbb{Q} \implies \alpha_j \in \overline{\mathbb{Q}} \implies f = \prod_{j=1}^{n}(X - \alpha_j)$ si spezza su $\overline{\mathbb{Q}}$.