Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 20-05-2020

Il teorema fondamentale

Ricordiamo che, fissato un campo L,

$$\{K \,:\, K \subseteq L \text{ di Galois}\} \to \{G \,:\, G < \mathrm{G}(L) \text{ finito}\} \quad K \mapsto \mathrm{G}_K(L)$$

$$\{G \,:\, G < \mathrm{G}(L) \text{ finito}\} \to \{K \,:\, K \subseteq L \text{ di Galois}\} \quad G \mapsto L^G$$

sono funzioni biunivoche una l'inversa dell'altra e che invertono le inclusioni. Inoltre $K \subseteq L$ di Galois $\implies \#\mathrm{G}_K(L) = [L : K]$.

Teorema fondamentale della teoria di Galois

$K \subseteq L$ estensione di Galois, $G := \mathrm{G}_K(L)$. Allora

$$\{F \,:\, K \subseteq F \subseteq L \text{ sottocampo}\} \to \{H \,:\, H < G\} \quad F \mapsto \mathrm{G}_F(L)$$

$$\{H \,:\, H < G\} \to \{F \,:\, K \subseteq F \subseteq L \text{ sottocampo}\} \quad H \mapsto L^H$$

sono funzioni biunivoche una l'inversa dell'altra e che invertono le inclusioni. Inoltre, se $K \subseteq F \subseteq L$ è un sottocampo, allora

1. $F \subseteq L$ di Galois e $\#\mathrm{G}_F(L) = [L : F]$;
2. $K \subseteq F$ normale $\iff H := \mathrm{G}_F(L) \triangleleft G \implies \mathrm{G}_K(F) \cong G/H$.

Dimostrazione

- La prima parte e il punto 1 seguono da quanto già visto, tenendo conto che $K \subseteq F \subseteq L$ sottocampo $\implies F \subseteq L$ di Galois (perché $K \subseteq L$ di Galois).
- Per dimostrare il punto 2, ricordiamo che $K \subseteq F$ è normale (e quindi di Galois) $\iff F$ è G-stabile.
- $K \subseteq F$ normale $\implies f\colon G \to \mathrm{G}_K(F)$, $\sigma \mapsto \sigma|_F$ ben definita. Chiaramente f omomorfismo e $\ker(f) = H$, per cui $H \lhd G$ e $G/H \cong \mathrm{im}(f)$ per il primo teorema di isomorfismo. Inoltre

$$\#\,\mathrm{im}(f) = \#(G/H) = \frac{\#G}{\#H} = \frac{\#[L:K]}{\#[L:F]} = [F:K] = \#\mathrm{G}_K(F),$$

$\implies f$ suriettiva e $\mathrm{G}_K(F) \cong G/H$.
- $H \lhd G \implies \sigma(\alpha) \in F\ \forall\, \sigma \in G$ e $\forall\, \alpha \in F$ (quindi $K \subseteq F$ normale): $\sigma(\alpha) \in F = L^H \iff \tau(\sigma(\alpha)) = \sigma(\alpha)\ \forall\, \tau \in H$ $\iff (\sigma^{-1}\tau\sigma)(\alpha) = \alpha\ \forall\, \tau \in H$, vero perché $\sigma^{-1}\tau\sigma \in H$ e $\alpha \in F = L^H$.

Esempio

$K := \mathbb{Q}$ e $L := \mathbb{Q}(\sqrt[3]{2}, \omega)$ con $1 \neq \omega \in \mathbb{C}$ tale che $\omega^3 = 1$.

- $\mathbb{Q} \subset L$ di Galois (è campo di spezzamento di $X^3 - 2$) e $G := \mathrm{G}_{\mathbb{Q}}(L) = \mathrm{G}(L)$ tale che $\# G = [L : \mathbb{Q}] = 6$.
- $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ non normale $\implies \mathrm{G}_{\mathbb{Q}(\sqrt[3]{2})}(L) < G$ non normale $\implies G \cong S_3$.
- $\exists!\, H \lhd G$ non banale (di ordine 3) $\implies [L : L^H] = 3$, $\mathbb{Q} \subset L^H$ normale e $\mathrm{G}_{\mathbb{Q}}(L^H) \cong G/H \cong C_2 \implies L^H = \mathbb{Q}(\omega)$.
- G ha anche 3 sottogruppi non normali non banali (di ordine 2), che corrispondono a $\mathbb{Q}(\omega^i \sqrt[3]{2})$ per $i = 0, 1, 2$.

Osservazione

- $K \subseteq L$ di Galois $\implies \#\{F : K \subseteq F \subseteq L \text{ sottocampo}\} < \infty$ perché coincide con $\#\{H : H < \mathrm{G}_K(L)\}$.
- $K \subseteq L$ finita $\implies \#\mathrm{G}_K(L) \leq [L : K] < \infty \implies L^{\mathrm{G}_K(L)} \subseteq L$ di Galois e $\#\mathrm{G}_K(L) = [L : L^{\mathrm{G}_K(L)}] \mid [L : K]$ (perché $K \subseteq L^{\mathrm{G}_K(L)} \subseteq L$, quindi $[L : K] = [L : L^{\mathrm{G}_K(L)}][L^{\mathrm{G}_K(L)} : K]$).

p primo, $n > 0$.

- $\mathbb{F}_{p^n} \subseteq L$ estensione tale che $[L : \mathbb{F}_{p^n}] = d \implies L \cong \mathbb{F}_{p^n}^d$ come $\mathbb{F}_{p^n}$-spazio vettoriale $\implies \#L = (p^n)^d = p^{nd} \implies L \cong \mathbb{F}_{p^{nd}}$.
- $d > 0 \implies \mathbb{F}_p \subseteq \mathbb{F}_{p^{nd}}$ di Galois con $G := \mathrm{G}_{\mathbb{F}_p}(\mathbb{F}_{p^{nd}}) = \langle \mathcal{F} \rangle \cong C_{nd} \implies H := \langle \mathcal{F}^n \rangle \lhd G$ e $F := \mathbb{F}_{p^{nd}}^H \subseteq \mathbb{F}_{p^{nd}}$ di Galois con $\mathrm{G}_F(\mathbb{F}_{p^{nd}}) = H \cong C_d$, $\mathrm{G}_{\mathbb{F}_p}(F) \cong G/H \cong C_n \implies F \cong \mathbb{F}_{p^n}$.
- Dunque $\exists$ estensione $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^{n'}} \iff n \mid n'$, e in questo caso l'estensione è di Galois con gruppo di Galois $\langle \mathcal{F}^n \rangle \cong C_{n'/n}$.

Osservazione

Fissata una chiusura algebrica $\mathbb{F}_p \subseteq \overline{\mathbb{F}}_p$ di $\mathbb{F}_p$, l'unico campo di spezzamento di $X^{p^n} - X$ su $\mathbb{F}_p$ contenuto in $\overline{\mathbb{F}}_p$ è $\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}}_p \,:\, \alpha^{p^n} = \alpha\}$ (e in questo caso $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^{n'}}$ sottocampo se $n \mid n'$). Inoltre $\overline{\mathbb{F}}_p = \bigcup_{n>0} \mathbb{F}_{p^n}$: $\alpha \in \overline{\mathbb{F}}_p \implies n := [\mathbb{F}_p(\alpha) : \mathbb{F}_p] < \infty \implies \mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^n} \implies \alpha \in \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$.

Gruppi finiti come gruppi di Galois

G gruppo finito $\implies \exists\, K \subseteq L$ di Galois tale che $\mathrm{G}_K(L) \cong G$:

- basta trovare L campo e $G' < \mathrm{G}(L)$ tale che $G' \cong G$ (perché poi $K := L^{G'} \subseteq L$ di Galois con $\mathrm{G}_K(L) = G' \cong G$);
- per il teorema di Cayley basta dimostrare che $\forall\, n > 0\ \exists\, L$ campo e $\exists\, G_n < \mathrm{G}(L)$ tale che $G_n \cong S_n$;
- F campo, $L := F(X_1, \dots, X_n)$ e $G_n := \{\tilde{\sigma} \in \mathrm{G}_F(L) : \sigma \in S_n\}$ con $\tilde{\sigma}$ tale che $\tilde{\sigma}(X_i) = X_{\sigma(i)}\ \forall\, i = 1, \dots, n$.

Il problema di Galois inverso chiede, fissato un campo K, per quali gruppi finiti G esiste $K \subseteq L$ di Galois tale che $\mathrm{G}_K(L) \cong G$.

- K algebricamente chiuso $\implies G \cong C_1$ (perché K non ha estensioni algebriche non banali).
- $K = \mathbb{R} \implies G \cong C_1$ o C_2 (perché $\mathbb{R} \subseteq K$ algebrica $\implies \exists$ $\mathbb{R}$-omomorfismo $K \to \mathbb{C}$, dato che $\mathbb{R} \subset \mathbb{C}$ è una chiusura algebrica di $\mathbb{R}$).
- K finito $\implies G \cong C_n$ con $n > 0$.
- Il problema è aperto per $K = \mathbb{Q}$.

Definizione

K campo, $0 \neq f \in K[X]$. Il gruppo di Galois di f su K (ben definito a meno di isomorfismo) è $\mathrm{G}_K(f) := \mathrm{G}_K(L)$ con $K \subseteq L$ campo di spezzamento di f.

Osservazione

$K \subseteq L$ campo di spezzamento di $f \in K[X] \setminus \{0\}$, $G := \mathrm{G}_K(f)$.

- K perfetto $\implies$ $K \subseteq L$ di Galois $\implies$ $\#G = [L : K]$.
- $K = L$ $\implies$ $G = \{1\}$; vale $\impliedby$ se K è perfetto.
- $R := \{\alpha \in L \,:\, f(\alpha) = 0\}$ $\implies$ $n := \#R \leq \deg(f)$. $\sigma \in G$, $\alpha \in R$ $\implies$ $\sigma(\alpha) \in R$, quindi si ottiene una funzione $G \to S(R) \cong S_n$, $\sigma \mapsto \sigma|_R$, che è un omomorfismo iniettivo (perché $L = K(R)$) $\implies$ $G \cong G' < S_n$ ($\implies$ $\#G \mid n!$, e dunque $[L : K] \mid n!$ se $K \subseteq L$ di Galois).
- K perfetto, f irriducibile $\implies$ $\deg(f) = n$ e $n \mid \#G \mid n!$.

Esempi

K perfetto, $f \in K[X]$ irriducibile, $n := \deg(f)$, $G := \mathrm{G}_K(f)$.

- $n = 2 \implies 2 \mid \#G \mid 2! \implies \#G = 2 \implies G \cong C_2$.
- $n = 3 \implies 3 \mid \#G \mid 3! \implies \#G = 3$ o $6 \implies G \cong C_3$ o S_3 (perché $G \cong G' < S_3$).

  $f = X^3 - 2 \implies G \cong S_3$ se $K = \mathbb{Q}$, $G \cong C_3$ se $K = \mathbb{Q}(\omega)$.
- $n = 4 \implies 4 \mid \#G \mid 4! \implies \#G = 4, 8, 12$ o $24 \implies$ $G \cong C_4, C_2^2, D_4, A_4$ o S_4 (perché $G \cong G' < S_4$).

  $f = X^4 - 10X^2 + 1 = \mathrm{m}_{\alpha,\mathbb{Q}}$ con $\alpha = \sqrt{2} + \sqrt{3} \implies G \cong C_2^2$: $\mathbb{Q} \subset \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ normale (perché campo di spezzamento di $(X^2 - 2)(X^2 - 3)$) $\implies f$ si spezza su $\mathbb{Q}(\alpha)$ $\implies \mathbb{Q} \subset \mathbb{Q}(\alpha)$ campo di spezzamento di $f \implies$ $G = \mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) \implies \#G = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 4$ e $G \not\cong C_4$ perché $\sigma \in G = \mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \implies$ $\sigma(\sqrt{2}) = \pm\sqrt{2}$ e $\sigma(\sqrt{3}) = \pm\sqrt{3} \implies \sigma^2(\sqrt{2}) = \sqrt{2}$ e $\sigma^2(\sqrt{3}) = \sqrt{3} \implies \sigma^2 = \mathrm{id}_{\mathbb{Q}(\sqrt{2},\sqrt{3})}$.

Generatori di S_n

Lemma

$\sigma, \tau \in S_n$ con σ n-ciclo e τ trasposizione.

1. $\sigma = (1, 2, \dots, n)$, $\tau = (1, 2) \implies S_n = \langle \sigma, \tau \rangle$.
2. $n = p$ *primo* $\implies S_p = \langle \sigma, \tau \rangle$.

Dimostrazione.

1. $\sigma^k \tau \sigma^{-k} = (k+1, k+2) \in \langle \sigma, \tau \rangle$ per $k = 0, \dots, n-2 \implies \langle \sigma, \tau \rangle \supseteq H_n := \langle (1, 2), \dots, (n-1, n) \rangle$, e basta dimostrare che $H_n = S_n$ per induzione su $n \geq 2$. Vero per $n = 2$, e per $n > 2$ basta dimostrare che $1 \leq i < j \leq n \implies (i, j) \in H_n$: $j < n \implies (i, j) \in H_{n-1} \subset H_n$; $j = n \implies$ posso supporre $i < n-1 \implies (i, n) = (i, n-1)(n-1, n)(i, n-1) \in H_n$ perché $(i, n-1) \in H_{n-1} \subset H_n$ e $(n-1, n) \in H_n$.
2. Posso supporre $\tau = (1, 2)$. $\exists 1 \leq k < p$ tale che $\sigma^k(1) = 2$. $\mathrm{ord}(\sigma^k) = p \implies \sigma^k = (1, 2, \dots)$ p-ciclo e $\langle \sigma, \tau \rangle = \langle \sigma^k, \tau \rangle \implies$ posso supporre $\sigma = (1, 2, \dots, p)$ e applico il punto 1.

Polinomi con gruppo di Galois S_p

Corollario

$f \in \mathbb{Q}[X]$ irriducibile, $\deg(f) = p$ *primo, f con esattamente $p - 2$ radici reali (e 2 complesse coniugate non reali)* $\implies \mathrm{G}_{\mathbb{Q}}(f) \cong S_p$.

Dimostrazione.

$\mathrm{G}_{\mathbb{Q}}(f) \cong G < S_p$, $p \mid \#G \implies \exists\, \sigma \in G$ tale che $\operatorname{ord}(\sigma) = p \implies \sigma$ p-ciclo. Inoltre il coniugio $\mathbb{C} \to \mathbb{C}$, $a + bi \mapsto a - bi$ è un automorfismo che manda l'insieme R delle radici di f in R (perché $f \in \mathbb{R}[X]$), e dunque si restringe a un elemento di $\mathrm{G}_{\mathbb{Q}}(f)$. Indicando con $\tau \in G < S_p$ l'elemento corrispondente e identificando S_p con $S(R)$, chiaramente τ è la trasposizione che scambia le 2 radici non reali di f. Allora $G = S_p$ per il Lemma. $\square$

Esempio

$f := X^5 - 4X + 2$ irriducibile per Eisenstein, ha al massimo 3 radici reali perché $f' = 5X^4 - 4$ ha 2 radici reali e ne ha almeno 3 perché $f(-2) < 0$, $f(0) > 0$, $f(1) < 0$, $f(2) > 0 \implies \mathrm{G}_{\mathbb{Q}}(f) \cong S_5$.