Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 22-05-2020

Gruppi di Galois di polinomi su campi finiti

p primo, $n > 0$, $q := p^n$, $0 \neq f \in \mathbb{F}_q[X]$, $G := \mathrm{G}_{\mathbb{F}_q}(f)$.

- f irriducibile, $d := \deg(f) \implies \mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ campo di spezzamento di f ($\implies G \cong C_d$): α radice di f (in $\overline{\mathbb{F}}_p$) $\implies [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d \implies \mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$.
- in generale $f = \prod_{i=1}^{k} f_i$ con f_i irriducibile, $d_i := \deg(f_i)$ $\forall\, i = 1, \ldots, k \implies d := \mathrm{mcm}(d_1, \ldots, d_k)$ tale che $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ campo di spezzamento di f ($\implies G \cong C_d$): per il punto precedente $\mathbb{F}_{q^{d_i}}$ è campo di spezzamento di f_i su $\mathbb{F}_q$, quindi f si spezza su $\mathbb{F}_{q^m} \iff \mathbb{F}_{q^{d_i}} \subseteq \mathbb{F}_{q^m}$ $\forall\, i = 1, \ldots, k \iff d_i \mid m$ $\forall\, i = 1, \ldots, k \iff d \mid m$.

Osservazione

$d > 0 \implies \exists\, f \in \mathbb{F}_q[X]$ irriducibile di grado d: per esempio $f = \mathrm{m}_{\alpha, \mathbb{F}_q}$ con $\alpha \in \mathbb{F}_{q^d}$ tale che $\langle \alpha \rangle = \mathbb{F}_{q^d}^*$.

Il gruppo di Galois di $X^n - 1$

$n > 0$, $\mathrm{char}(K) \nmid n$, $K \subseteq L$ campo di spezzamento di $X^n - 1$.

- $(X^n - 1)' = nX^{n-1} \neq 0$ ha solo la radice 0 (che non è radice di $X^n - 1$) $\implies$ $X^n - 1$ non ha radici multiple in L $\implies$ $R := \{\alpha \in L : \alpha^n = 1\}$ tale che $\#R = n$.
- $R < L^*$ $\implies$ R ciclico $\implies$ $\exists \omega \in R$ tale che $R = \langle \omega \rangle$ (quindi $\mathrm{ord}(\omega) = n$ in L^*, e si dice che ω è una radice n-esima primitiva dell'unità; per esempio $\omega = e^{(2\pi i)/n}$ se $K \subseteq \mathbb{C}$).
- $L = K(R) = K(\omega)$ $\implies$ $\#\mathrm{G}_K(L) = \#R'$ con $R' := \{\alpha \in L : \mathrm{m}_{\omega,K}(\alpha) = 0\} \subseteq R$ (perché $\mathrm{m}_{\omega,K} \mid (X^n - 1)$).
- $\mathrm{m}_{\omega,K}$ si spezza su L e non ha radici multiple $\implies$ $\#\mathrm{G}_K(L) = \deg(\mathrm{m}_{\omega,K}) = [L : K]$ $\implies$ $K \subseteq L$ di Galois.
- La funzione $\mathrm{G}_K(L) \to \mathrm{Aut}(R) < S(R)$, $\sigma \mapsto \sigma|_R$ è ben definita e è un omomorfismo iniettivo di gruppi.
- $\mathrm{G}_K(X^n - 1) = \mathrm{G}_K(L) \cong G < \mathbb{Z}/n\mathbb{Z}^* \cong \mathrm{Aut}(R)$ $\implies$ G abeliano e $\#G \mid \varphi(n)$.

Polinomi ciclotomici

$\alpha \in R' \implies \exists \sigma \in \mathrm{G}_K(L)$ tale che $\alpha = \sigma(\omega) \implies$
$\mathrm{ord}(\alpha) = \mathrm{ord}(\omega) = n \implies \exists \bar{j} \in \mathbb{Z}/n\mathbb{Z}^*$ tale che $\alpha = \omega^j \implies$

$$\mathrm{m}_{\omega,K} = \prod_{\alpha \in R'} (X - \alpha) \mid \Phi_n := \prod_{\bar{j} \in \mathbb{Z}/n\mathbb{Z}^*} (X - \omega^j) \in L[X],$$

dove Φ_n è detto n-esimo polinomio ciclotomico.

Teorema

1. $\Phi_n \in K[X]$.
2. $K = \mathbb{Q} \implies \Phi_n$ *irriducibile* ($\implies \mathrm{G}_{\mathbb{Q}}(X^n - 1) \cong \mathbb{Z}/n\mathbb{Z}^*$).

Dimostrazione nel caso $n = p$ primo.

1. $\Phi_p = \left(\prod_{\bar{j} \in \mathbb{Z}/p\mathbb{Z}} (X - \omega^j)\right)/(X - 1) = (X^p - 1)/(X - 1) = X^{p-1} + \cdots + 1$.
2. Con la sostituzione $X = Y + 1$ si ottiene $\Phi_p(X) = \Phi_p(Y + 1) = \left((Y + 1)^p - 1\right)/Y = \sum_{j=1}^{p} \binom{p}{j} Y^{j-1}$, che è irriducibile in $\mathbb{Q}[Y]$ per Eisenstein.

Discriminante di un polinomio

- K campo, $0 \neq f \in K[X]$, $K \subseteq L$ campo di spezzamento di f.
- $n := \deg(f)$, $\alpha_1, \ldots, \alpha_n \in L$ radici di $f \implies$

$$\delta := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \in L$$

è ben definito a meno del segno (dipende dall'ordine delle radici), e chiaramente $\delta \neq 0 \iff f$ non ha radici multiple.

- Il discriminante di f è $\Delta = \Delta(f) := \delta^2 \in L$ (ben definito e tale che $\Delta \neq 0 \iff f$ non ha radici multiple).

Lemma

$\sigma(\delta) = \varepsilon(\sigma|_R)\delta$ *(con* $R := \{\alpha_1, \ldots, \alpha_n\}$*)* $\forall\, \sigma \in \mathrm{G}_K(f) = \mathrm{G}_K(L)$.

Dimostrazione.

Per definizione di segno di una permutazione

$$\sigma(\delta) = \prod_{1 \leq i < j \leq n} (\sigma(\alpha_i) - \sigma(\alpha_j)) = \prod_{1 \leq i < j \leq n} (\sigma|_R(\alpha_i) - \sigma|_R(\alpha_j)) = \varepsilon(\sigma|_R)\delta.$$

Proprietà del discriminante

Assumiamo che K sia perfetto.

Corollario

$\Delta \in K$. Se inoltre $\mathrm{char}(K) \neq 2$, f non ha radici multiple e identifico $\mathrm{G}_K(f)$ a un sottogruppo di $S_n \cong S(R)$, allora $\mathrm{G}_K(f) \subseteq A_n \iff \delta \in K \iff \Delta$ è un quadrato in K.

Dimostrazione.

- $K \subseteq L$ di Galois $\implies K = L^{\mathrm{G}_K(L)}$. Dunque, dato $\beta \in L$, $\beta \in K \iff \sigma(\beta) = \beta \ \forall \sigma \in \mathrm{G}_K(L) = \mathrm{G}_K(f)$.
- $\sigma(\Delta) = \sigma(\delta^2) = \sigma(\delta)^2 = (\varepsilon(\sigma|_R)\delta)^2 = \varepsilon(\sigma|_R)^2\delta^2 = \delta^2 = \Delta$ $\forall \sigma \in \mathrm{G}_K(f) \implies \Delta \in K$.
- $\mathrm{G}_K(f) \subseteq A_n \implies \sigma(\delta) = \delta \ \forall \sigma \in \mathrm{G}_K(f) \implies \delta \in K$.
- $\delta \in K$, f senza radici multiple $\implies \delta \in K^*$ e $\forall \sigma \in \mathrm{G}_K(f)$ $\delta = \sigma(\delta) = \varepsilon(\sigma|_R)\delta \implies \varepsilon(\sigma|_R)_K = 1_K \implies \varepsilon(\sigma|_R) = 1$ (cioè $\mathrm{G}_K(f) \subseteq A_n$) se $\mathrm{char}(K) \neq 2$.
- Chiaramente $\delta \in K \iff \Delta = \delta^2$ è un quadrato in K.

Discriminante dei polinomi di grado 2 e 3

- Si può dimostrare che $\Delta(f)$ è esprimibile come polinomio valutato nei coefficienti di f.
- $\Delta(X^2 + aX + b) = a^2 - 4b$:

  $X^2 + aX + b = (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta \implies$
  $a = -\alpha - \beta,\ b = \alpha\beta;$
  $\delta = \alpha - \beta \implies \Delta = (\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = a^2 - 4b.$
- $\Delta(X^3 + aX + b) = -4a^3 - 27b^2$:

  $X^3 + aX + b = (X - \alpha)(X - \beta)(X - \gamma) =$
  $X^3 - (\alpha + \beta + \gamma)X^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)X - \alpha\beta\gamma \implies$
  $\alpha + \beta + \gamma = 0,\ a = \alpha\beta + \alpha\gamma + \beta\gamma,\ b = -\alpha\beta\gamma \implies$
  $a = -(\alpha^2 + \alpha\beta + \beta^2),\ b = \alpha\beta(\alpha + \beta);$
  $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) = (\alpha - \beta)(2\alpha + \beta)(\alpha + 2\beta) =$
  $2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3 \implies$
  $\Delta = (2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3)^2 = 4\alpha^6 + 12\alpha^5\beta - 3\alpha^4\beta^2 -$
  $26\alpha^3\beta^3 - 3\alpha^2\beta^4 + 12\alpha\beta^5 + 4\beta^6 = -4a^3 - 27b^2.$

Gruppo di Galois di un polinomio di grado 3

$\mathrm{char}(K) \neq 2$, $\deg(f) = 3$, f irriducibile in $K[X] \implies$

$$\mathrm{G}_K(f) \cong \begin{cases} C_3 & \text{se } \Delta(f) \text{ è un quadrato in } K \\ S_3 & \text{altrimenti.} \end{cases}$$

Esempio

- $f = X^3 - 3X + 1$ irriducibile in $\mathbb{Q}[X]$ (non ha radici in $\mathbb{Q}$) $\implies \Delta = -4(-3)^3 - 27 \cdot 1^2 = 81 = 9^2 \implies \mathrm{G}_{\mathbb{Q}}(f) \cong C_3$.
- $f = X^3 + 3X + 1$ irriducibile in $\mathbb{Q}[X]$ (non ha radici in $\mathbb{Q}$) $\implies \Delta = -4 \cdot 3^3 - 27 \cdot 1^2 = -135 < 0 \implies \mathrm{G}_{\mathbb{Q}}(f) \cong S_3$.

Osservazione

$\mathrm{char}(K) \neq 3$, $f(X) = X^3 + aX^2 + bX + c \in K[X] \implies$ con la sostituzione $X = Y - a/3$ si ottiene $f(X) = f(Y - a/3) =: g(Y)$ con $g(Y) = Y^3 + a'Y + b' \in K[Y]$. Chiaramente $\alpha \in L$ (campo di spezzamento di f su K) è radice di $g \iff \alpha - a/3$ è radice di f $\implies L$ è campo di spezzamento di g su $K \implies \mathrm{G}_K(f) \cong \mathrm{G}_K(g)$.

Soluzioni di equazioni di grado 2 e 3

- $\mathrm{char}(K) \neq 2$, $f(X) = X^2 + aX + b \in K[X] \implies$ con la sostituzione $X = Y - a/2$ si ottiene

$$f(X) = f(Y - a/2) = Y^2 - a^2/4 + b =: g(Y).$$

$\alpha^2 = a^2/4 - b = \Delta(f)/4 \iff \alpha$ radice di $g \iff \alpha - a/2$ radice di f.

- $\mathrm{char}(K) \neq 2, 3$, $f(X) = X^3 + aX + b \in K[X] \implies$ con la sostituzione $X = Y - a/(3Y)$ si ottiene

$$f(X) = f(Y - a/(3Y)) = Y^3 + b - a^3/(27Y^3) = Y^{-3}g(Y)$$

con $g(Y) := h(Y^3)$ e $h(Z) := Z^2 + bZ - a^3/27$.
α radice di $g \implies \alpha - a/(3\alpha)$ radice di f e α^3 radice di h.
Si noti che $\Delta(h) = b^2 + 4a^3/27 = -\Delta(f)/27$.

Osservazione

Analogamente si può trattare il caso $\deg(f) = 4$.

Risolubilità per radicali

Definizione

- $K \subseteq L$ estensione; $\alpha \in L$ è radicale su K se $\exists\, n > 0$ tale che $\alpha^n \in K$.
- $K \subseteq L$ è un'estensione per radicali se esistono estensioni $K = L_0 \subseteq \cdots \subseteq L_r = L$ e $\forall\, i = 1, \ldots, r\ \exists\, \alpha_i \in L_i$ radicale su L_{i-1} tale che $L_i = L_{i-1}(\alpha_i)$.
- $f \in K[X] \setminus \{0\}$ è risolubile (per radicali) se esiste un'estensione per radicali $K \subseteq L$ tale che f si spezza su L.

Teorema (Galois)

Se $\mathrm{char}(K) = 0$, *allora* $f \in K[X] \setminus \{0\}$ *è risolubile* $\iff$ $\mathrm{G}_K(f)$ *è un gruppo risolubile.*

Esempio

$f = X^5 - 4X + 2 \in \mathbb{Q}[X]$ non è risolubile perché $\mathrm{G}_{\mathbb{Q}}(f) \cong S_5$ non è risolubile.

Idea della dimostrazione di $\Longrightarrow$

- Si dimostra che $\exists\, K \subseteq L$ normale e per radicali tale che f si spezza su L. Inoltre si trova $K = L_0 \subseteq \cdots \subseteq L_r = L$, dove: $L_1 = L_0(\omega)$ con ω radice primitiva n-esima dell'unità; $i = 2, \ldots, r \implies L_i = L_{i-1}(\alpha_i)$ con $\alpha_i^{n_i} \in L_{i-1}$ e $n_i \mid n$.
- $i = 1, \ldots, r \implies L_{i-1} \subseteq L_i$ normale (quindi di Galois): già visto se $i = 1$, mentre se $i > 1$ L_i è campo di spezzamento di $X^{n_i} - \alpha_i^{n_i} = \prod_{j=1}^{n_i}(X - \alpha_i \omega^{jn/n_i})$ su L_{i-1}.
- $i = 1, \ldots, r \implies \mathrm{G}_{L_{i-1}}(L_i)$ abeliano: già visto se $i = 1$, mentre se $i > 1$ e $\sigma, \sigma' \in \mathrm{G}_{L_{i-1}}(L_i)$, $\sigma(\alpha_i) = \alpha_i \omega^{jn/n_i}$ e $\sigma'(\alpha_i) = \alpha_i \omega^{j'n/n_i} \implies (\sigma\sigma')(\alpha_i) = \alpha_i \omega^{(j+j')n/n_i} = (\sigma'\sigma)(\alpha_i)$ $\implies \sigma\sigma' = \sigma'\sigma$.
- $G := \mathrm{G}_K(L)$, $H_i := \mathrm{G}_{L_i}(L) < G\ \forall\, i = 0, \ldots, r$ tali che $\{1\} = H_r < \cdots < H_0 = G$. Inoltre $H_i \triangleleft H_{i-1}$ (perché $L_{i-i} \subseteq L_i$ normale) e $H_{i-1}/H_i \cong \mathrm{G}_{L_{i-1}}(L_i)$ abeliano $\forall\, i = 1, \ldots, r \implies G$ risolubile.
- $\mathrm{G}_K(f)$ risolubile perché isomorfo a un quoziente di G.