Estensioni ciclotomiche

Vogliamo studiare il campo di spezzamento del polinomio $f(x) = X^n - 1$ su $\mathbb{Q}$ $(n \geq 1)$

Abbiamo visto che è $\mathbb{Q}(\xi)$, ξ radice primitiva n-esima di 1 ($\xi = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, o più in gen. $e^{\frac{2\pi i k}{n}}$ con $(k,n)=1$).

Vogliamo determinare il polinomio minimo di ξ su $\mathbb{Q}$.

Per ogni $d \mid n$ sia $I_d = \{$radici primitive d-esime dell'unità$\}$ e $\Phi_d(x) = \prod_{\alpha \in I} (x - \alpha)$ d-esimo polinomio ciclotomico

Si ha

$$X^n - 1 = \prod_{d \mid n} \Phi_d(x)$$ perché ogni radice n-esima di 1 è radice primitiva d-esima per qc. $d \mid n$.

In particolare $\Phi_n(x) = \prod_{(k,n)=1} (x - \xi^k)$

$\deg \Phi_n(x) = \varphi(n)$ funzione di Eulero.

Prop.

1) $\Phi_n(x)$ è un polinomio monico a coeff in $\mathbb{Z}$

2) $\Phi_n(x)$ è irriducibile in $\mathbb{Q}[x]$ e quindi è il polinomio minimo di ξ

Dim.

1) Induzione su n. Per $n=1$ $\Phi_1(x) = x - 1$ ok.

Per $n > 1$ $$X^n - 1 = \Phi_n(x) \underbrace{\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x)}_{\text{monico a coeff in } \mathbb{Z} \text{ e divide } X^n - 1}$$

$\Rightarrow \Phi_n(x)$ è monico a coeff. in $\mathbb{Z}$. (lemma di Gauss)

2) Sia $f(x)$ il polinomio minimo di ξ su $\mathbb{Q}$.

Quindi $\Phi_n(x) = f(x)\, g(x)$, $f(x)$ possono essere scelti monici a coeff. interi per il lemma di Gauss

Per mostrare che Φ_n irid. basta mostrare che ogni radice primitiva n-esima annulla $f(x)$ cioè che $\forall k$ t.c. $(k,n)=1$ $f(\xi^k)=0$.

Per induzione basta mostrare che

$\forall p$ primo $p \nmid n \Rightarrow f(\xi^p)=0$

Altrimenti si avrebbe $g(\xi^p)=0$, quindi ξ sarebbe radice di $g(x^p) \Rightarrow f(x) \mid g(x^p)$

$\Rightarrow g(x^p) = f(x)\, h(x)$ tutti monici a coeff in $\mathbb{Z}$

$\Rightarrow \overline{g(x)}^p = \overline{f(x)}\,\overline{h(x)}$ in $\mathbb{F}_p[x]$

$\Rightarrow$ ogni fattore irid. di $\overline{f(x)}$ divide $\overline{g(x)}$

Sia $u(x) \in \mathbb{F}_p[x]$ un fattore irid di $\overline{f(x)}$

$u(x)^2 \mid \overline{x^n - 1} \Rightarrow \overline{x^n-1}$ ha radici multiple in $\overline{\mathbb{F}_p}$.

Ma una tale radice deve annullare $x^n - \bar{1}$ e la sua derivata nx^{n-1}, assurdo perché $p \nmid n$. $\boxtimes$

Quindi $\Phi_n(x)$ è il polinomio minimo su $\mathbb{Q}$ di ogni radice primitiva n-esima di 1, e $[\mathbb{Q}(\xi):\mathbb{Q}] = \varphi(n)$.

Oss.: se $n = p^k$ è potenza di un primo, $\Phi_{p^k}(x)$ ha una scrittura esplicita:

$$\Phi_{p^k}(x) = \frac{x^{p^k}-1}{x^{p^{k-1}}-1} = x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \dots + x^{p^{k-1}} + 1$$

Ricordiamo che

$$\varphi(n) = |\mathbb{Z}_n^\times| = |\{k \in \mathbb{Z}_n \mid (k,n) = 1\}|$$

e che se $n = \prod_{i=1}^{s} p_i^{e_i}$ si ha

$$\varphi(n) = \prod_{i=1}^{s} p_i^{e_i-1}(p_i-1).$$

Teorema

$$\mathrm{Gal}\left(\mathbb{Q}(\xi)/\mathbb{Q}\right) \simeq \mathbb{Z}_n^\times.$$

Dim.

Sia $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(\xi)/\mathbb{Q}\right)$; σ permuta le radici di $\Phi_n(x)$ quindi $\sigma(\xi) = \xi^k$ per qualche k t.c. $(k,n)=1$.

k è ben definito modulo n, in quanto $\xi^n = 1$.

Definiamo

$$\begin{aligned} \theta : \mathrm{Gal}\left(\mathbb{Q}(\xi)/\mathbb{Q}\right) &\longrightarrow \mathbb{Z}_n^* \\ \sigma &\longmapsto k. \end{aligned}$$

θ omom. di gruppi: se $\sigma(\xi) = \xi^k$ e $\tau(\xi) = \xi^h$ si ha

$\sigma\tau(\xi) = \sigma(\xi^h) = \sigma(\xi)^h = \xi^{kh}$ ma $\theta(\sigma\tau) = kh = \theta(\sigma)\theta(\tau)$.

θ iniettivo: se $\sigma(\xi) = \xi$ allora $\sigma = id$ su $\mathbb{Q}(\xi)$.

Inoltre $\left|Gal\left(\mathbb{Q}(\xi)/\mathbb{Q}\right)\right| = [\mathbb{Q}(\xi):\mathbb{Q}] = \varphi(m) = |\mathbb{Z}_m^*| \Rightarrow \theta$ suriettiva. $\boxtimes$

In particolare

$$Gal\left(\mathbb{Q}(\xi)/\mathbb{Q}\right) \text{ è abeliano}$$

(si dice che l'estensione $\mathbb{Q}(\xi)/\mathbb{Q}$ è un' estensione abeliana)

Teorema di Kronecker-Weber: ogni estensione abeliana di $\mathbb{Q}$ è contenuta in un'estensione ciclotomica.

Esempio

Dimostrare che $\forall p,\ ^n$ esistono estensioni abeliane di $\mathbb{Q}$ di grado p^n e determinare un' estensione abeliana di grado 3.

Sol.

Per il teorema di classificazione dei gruppi abeliani finiti basta trovare un'estensione abeliana di $\mathbb{Q}$ di grado multiplo di p^n. (Se $|G|$ è abeliano e $n|m$ allora G ha un sottogruppo di ordine $\frac{m}{n}$ quindi un quoziente di ordine n)

Per esempio $\mathbb{Q}(\xi)$ con ξ radice prim. p^{n+1}-esima di 1.

Per $n=1$, $p=3$ $\quad \varphi(9) = 2\cdot 3 = 6 \quad Gal\left(\mathbb{Q}(\xi)/\mathbb{Q}\right) \simeq \mathbb{Z}_9^* \simeq \mathbb{Z}_2\times\mathbb{Z}_3$

$\mathbb{Z}_9^* = \langle \bar{2} \rangle$ e ha un sottogruppo di ordine 2, generato da $\langle \bar{8} \rangle = \langle -\bar{1} \rangle$

L'elemento di $Gal\left(\mathbb{Q}(\xi)/\mathbb{Q}\right)$ corrispondente a -1 è $\xi \longrightarrow \xi^{-1} = \bar{\xi}$ è il coniugio complesso.

Quindi un'estensione di grado 3 in $\mathbb{Q}(\xi)$ (di fatto l'unica) è $\mathbb{Q}(\zeta)^{\text{coniugio complesso}} = \mathbb{Q}(\zeta) \cap \mathbb{R}$.

Troviamo generatori.

ζ soddisfa, su $\mathbb{R}$ il polinomio quadratico

$$X^2 - (\underbrace{\zeta + \bar{\zeta}}_{\in\, \mathbb{Q}(\zeta) \cap \mathbb{R}})X + 1$$

$$\begin{array}{c} \mathbb{Q}(\zeta) \\ |\,2 \\ \mathbb{Q}(\zeta)' \\ |\,3 \\ \mathbb{Q} \end{array}$$

Quindi

$$[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \bar{\zeta})] = 2$$

$$\Rightarrow \mathbb{Q}(\zeta + \bar{\zeta}) = \mathbb{Q}(\zeta \cap \mathbb{R})$$

$$\mathbb{Q}(\zeta+\bar{\zeta}) = \mathbb{Q}\left(\cos \frac{2\pi}{9}\right)$$

Composto di campi

Problemi:

1) Dato $f(x) \in K[x]$ e L/K est. finita, che relazione c'è tra il gruppo di Galois di $f(x)$ su K e quello su L?
2) Dati $f(x), g(x) \in K[x]$, che relazione c'è tra il gruppo di Galois di $f(x)g(x)$ e quelli di $f(x), g(x)$ su K?

<u>Def.</u>

Siano H, K due sottocampi di $\overline{\mathbb{Q}}$. Il loro composto è

$= H \cdot K$ è il più piccolo sottocampo di $\overline{\mathbb{Q}}$ contenente H, K

$= H(K) = K(H)$

<u>Prop.</u> Se uno tra H/E, K/E è finito.

$$H \cdot K = \underbrace{\left\{ \sum_{i=1}^{m} h_i k_i \,/\, h_i \in H, k_i \in K \right\}}_{A}$$

<u>Dim.</u>

Ovviamente A è un sottoanello di $\overline{\mathbb{Q}}$, contenente H e K, e ogni campo contenente H, K deve contenere A. Basta verificare che A è un campo.

Supponiamo che H/E sia finita. Allora A è un K-spazio vettoriale di dim. finita (è generato da una base di H su E)

Per ogni $\alpha \in A$, $\alpha \neq 0$ la moltiplicazione

$$A \longrightarrow A \qquad \beta \longmapsto \alpha\beta$$

è K-lineare e iniettivo $\Rightarrow$ suriettivo (perché $\dim_K(A) < \infty$)

$\Rightarrow \exists \beta$ t.c. $\alpha\beta = 1 \rightarrow A$ campo.

<u>Prop.</u>: se H/E, K/E sono finite allora HK/E finito e $[HK:E] \leq [H:E][K:E]$

<u>Dim.</u>

Si ha $[HK:E] = [HK:K][K:E]$

e abbiamo visto sopra che una base di H su E genera HK come K-sp. vett. $\Rightarrow [HK:K] \leq [H:E]$. $\blacksquare$

La costruzione si può generalizzare a più campi: se $H_1, \dots, H_s$ sono estensioni di E, si può considerare il loro <u>composto</u>: $H_1 \cdot H_2 \cdot \dots \cdot H_s$. Se H_i/E sono tutte finite allora

$$H_1 \cdot H_2 \cdot \dots \cdot H_s = \{ \sum_i a_{i_1} \cdots a_{i_s} \mid a_{i_j} \in H_j \}$$

e $[H_1 \dots H_s : E] \leq \prod_{i=1}^{s} [H_i : E]$.

<u>Teorema</u>

Sia E/K un'estensione finita di grado n e sia $\mathcal{J}(E/K) = \{\sigma_1, \dots, \sigma_n\}$. Allora

1) $E' = \sigma_1(E)\sigma_2(E) \dots \sigma_n(E)/K$ è di Galois

2) Ogni estensione F/E di Galois su K contiene E'.

3) $Gal\left(E'/K\right)$ è (canonicamente) isomorfo a un sottogruppo transitivo di S_n

(Un sottogruppo H di S_n è transitivo se l'azione di H su $\{1,\dots,n\}$ è transitiva, cioé $\forall i,j \; \exists \sigma \in H$ t.c. $\sigma(i)=j$)

L'estensione E'/K si dice chiusura di Galois di E/K : è la più piccola estensione di Galois di K contenente E.