POLINOMI CICLOTOMICI

venerdì 26 novembre 2021 15:19

POLINOMI CICLOTOMICI

- Sia $f(x) = x^n - 1$ $(n \geq 1)$ il polinomio le cui radici in $\mathbb{C}$ sono tutte le radici n-esime dell'unità.
- Una radice w di $f(x) = x^n - 1$ si dice radice primitiva n-esima dell'unità se $w^k \neq 1$ per ogni $1 \leq k \leq n-1$.
- Le radici n-esime dell'unità sono i numeri complessi $e^{i\frac{2k\pi}{n}}$ per $k = 0, \dots, n-1$.
- la radice $e^{i\frac{2k\pi}{n}}$ è primitiva $\Leftrightarrow (k,n) = 1$
- Dunque le radici primitive n-esime dell'unità sono $\varphi(n)$
- e le radici primitive hanno ordine n
- Chiamo n-esimo pol. ciclotomico il polinomio $\phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \alpha_i)$ dove le α_i sono le radici primitive n-esime dell'unità.
- Per ogni intero positivo n pongo $\xi_n = e^{\frac{2\pi i}{n}}$
- $f(x) = \prod_{d \mid n} \phi_d(x) = x^n - 1$ è a priori una fatt. in $\mathbb{C}[x]$ in realtà è una fatt in $\mathbb{Z}[x]$.
- $\langle \xi_n \rangle \cong \mathbb{Z}_n$

LISTA DEI PRIMI POLINOMI CICLOTOMICI

$\phi_1 = x - 1$
$\phi_2 = x + 1$
$\phi_3 = x^2 + x + 1$
$\phi_4 = x^2 + 1$
$\phi_5 = x^4 + x^3 + x^2 + x + 1$
$\phi_6 = x^2 - x + 1$
$\phi_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\phi_8 = x^4 + 1$
$\phi_9 = x^6 + x^3 + 1$
$\phi(10) = x^4 - x^3 + x^2 - x + 1$

Se p è primo $\Rightarrow$ il p-esimo pol. ciclotomico è $\phi_p(x) = 1 + x + \dots + x^{p-1}$

Il primo pol. ciclotomico che ha coeff $\neq 0, 1, -1$ è ϕ_{105}

Teorema

- $\forall n \geq 1$ $\phi_n(x) \in \mathbb{Z}[x]$ ed è irrid in $\mathbb{Z}[x]$ e quindi in $\mathbb{Q}[x]$.
  Inoltre il c.d.s di $\phi_n(x)$ su $\mathbb{Q}$ è $\mathbb{Q}(\xi_n)$ e ha grado $\varphi(n)$

  cioè $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi_n$
  Inoltre $Aut(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong \mathbb{Z}_n^*$

- **Lemma (utile nella dim del teorema sopra)**
  Sia n intero positivo, sia w una radice n-esima primitiva di 1
  Sia $q(x) \in \mathbb{Z}[x]$ il suo pol. minimo primitivo
  Allora $\forall p$ primo t.c. $p \nmid n$ vale che w^p è radice di $q(x)$

Dal teo + lemma so che:
- w^p è radice del pol. min. di w. con w = n-esima radice di 1 e $(n,p)=1$
- $|Aut(\mathbb{Q}(\xi_n)/\mathbb{Q})| = [\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$
- c.d.s di $\phi_n(x)$ e $\mathbb{Q}(\xi_n)$
- $Gal(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong \mathbb{Z}_n^*$
- $q(x)$ = pol min di w è in realtà $\phi_n(x)$

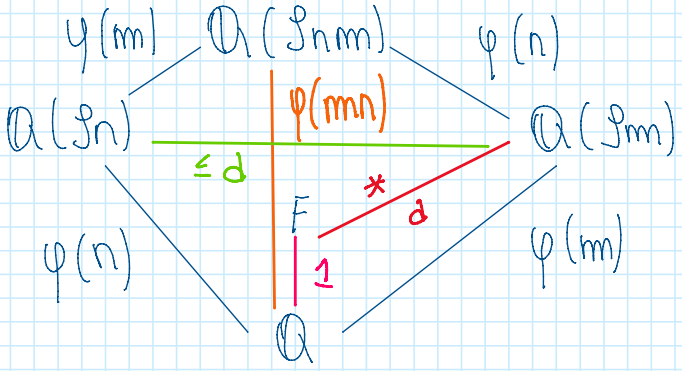
- Se n, m sono due interi positivi primi fra loro allora
  1) $\mathbb{Q}(\xi_n, \xi_m) = \mathbb{Q}(\xi_{n \cdot m})$
  2) $F = \mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m) = \mathbb{Q}$

dim

1) $\subseteq$ $\mathbb{Q}(\xi_{mn}) \subseteq \mathbb{Q}(\xi_n, \xi_m)$ poiché $\mathbb{Q}(\xi_n, \xi_m)$ contiene la radice primitiva mn-esima dell'unità $\xi_n \xi_m$
  infatti $\xi_n \cdot \xi_m = \xi_{m.c.m(ord(\xi_n), ord(\xi_m))} = \xi_{m.c.m(n,m)} = \xi_{n \cdot m}$

  $\supseteq$ $\xi_{mn}^m = \xi_n$ e $\xi_{mn}^n = \xi_m$ $\Rightarrow$ $\mathbb{Q}(\xi_{mn}) \supseteq \mathbb{Q}(\xi_n, \xi_m)$

2) Considero il seguente diamante



*= $d \leq \varphi(m)$

perché se fosse $[\mathbb{Q}(\zeta_m) : F] = d < \varphi(m)$ allora avrei che il pol. minimo $p(x)$ di ζ_m su $\mathbb{Q}(\zeta_n)$ dovrebbe avere grado minore o uguale a d. $\Rightarrow [\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}(\zeta_n)] \leq d$ ↯

Dunque $[\mathbb{Q}(\zeta_m) : F] = \varphi(m)$ e allora $[F : \mathbb{Q}] = 1$ cioè $F = \mathbb{Q}$

Se $(n, m) \neq 1 \Rightarrow \mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{m.c.m(n,m)})$

$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{m.c.d(n,m)})$

Esempio

$\mathbb{Q}(\zeta_4, \zeta_5) = \mathbb{Q}(\zeta_{20})$

$\subseteq \mathbb{Q}(\zeta_4, \zeta_5) = \mathbb{Q}(\zeta_{mcm(4,5)}) = \mathbb{Q}(\zeta_{20})$.

$\supseteq \zeta_{20}^4 = \zeta_5$ e $\zeta_{20}^5 = \zeta_4 \Rightarrow \zeta_{20} \in \mathbb{Q}(\zeta_4, \zeta_5)$

Esempio

$Gal(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \cong \mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$

Da finire !! manca (Giulio del corso pag da 7.42 7.7.