W13D2 04/06/2012 הרצאה

יהי F שדה ו- n מספר טבעי. נניח ש- F מכיל את כל שורשי היחידה מסדר n, כלומר $x^n - 1$ מתפרק לגורמים לינאריים ב- F. (נזכיר כי $\mathrm{char}(F) = 0$ או $\mathrm{char}(F)$ לא מחלק את n.)

משפט: יהי K/F הרחבת גלois כך ש- $G_{K/F} \cong (\mathbb{Z}/n\mathbb{Z})^*$.

הוכחה: לכל $\sigma \in G_{K/F}$, מכיוון ש- $\mu_n(K)$ הוא חבורה ציקלית מסדר n, נובע כי $\sigma(\mu_n(K)) = \mu_n(K)$.

כי לכל $\alpha \in K$, $\alpha^n = 1 \iff \sigma(\alpha)^n = 1$

$\alpha \in \mu_n(K) \iff \sigma(\alpha) \in \mu_n(K)$

ולכן $\mu_n(K) \cong \mu_n(K)/\sigma$ איזומורפיזם של חבורות.

לכן $\sigma(\zeta)$ הוא יוצר של אותה חבורה.

מסדר n של 1.

לכן, יש איזה l (מהצורה n), כלשהו σ,

כך ש: $\sigma(\zeta) = \zeta^l$

- נגדיר: $t : G_{K/F} \to (\mathbb{Z}/n\mathbb{Z})^*$

$$t(\sigma) = l + n\mathbb{Z}$$

- t האיזומורפיזם:

$t(\sigma_1\sigma_2) = ?$

$\sigma_1(\sigma_2(\zeta)) = \sigma_1(\zeta^{l_2}) = \sigma(\zeta)^{l_2} = \zeta^{l_1 l_2}$

$t(\sigma_1\sigma_2) = l_1 l_2 + n\mathbb{Z} = t(\sigma_1)\, t(\sigma_2)$

- t חח"ע:

אזי $t(\sigma) = 1 + n\mathbb{Z}$

אז $\sigma(\zeta) = \zeta$

לכן σ הוא האיבר ב- $K = F[\zeta]$,

כלומר $\sigma = id$.

מסקנה: $\varphi(n) \mid [K:F]$

כי: $[K:F] = |G_{K/F}|$, $G_{K/F}$ איזו חבורה יש כזו $H < (\mathbb{Z}/n\mathbb{Z})^\times$

ולכן

$$[K:F] = |H| \mid |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$$

משפט

יהי $f(x)$ הפולינום הא-פרידי מעל F ויהי K שדה הפיצול שלו מעל F.

$$f(x) = \prod_{\sigma \in G_{K/F}} (x - \sigma(\beta))$$

כך שורש $\sigma(\beta)$ הוא שורש של f לכל $\sigma \in G_{K/F}$ ומספר n של f

שונים: $\{$מספר n של 1 $\}$ = C_n

נגדיר: $\Phi_n(x) = \prod_{\eta \in C_n} (x - \eta) \in K[x]$

משפט: $\Phi_n(x) \in F[x]$

הוכחה: יהי $\sigma \in G_{K/F}$, $\sigma(C_n) = C_n$

כי יהי $\mu_n(K)$ שם n = מספר $\sigma(\eta)$

כי $\mu_n(K)/\sigma$ הוא אוטומורפיזם על $\mu_n(K)$ שמקיים

$$[\sigma\Phi_n](x) = \prod_{\eta \in C_n} (x - \sigma(\eta)) = \prod_{\sigma\eta \in C_n} (x - \eta) = \Phi_n(x)$$

לכן, מקדמי Φ_n שייכים ל- $F = K^{G_{K/F}}$

ו- Φ_n מקיים הפירוק הקנוני מעל F

שאלה: $f(x) \mid \Phi_n(x)$, $\deg \Phi_n(x) = |C_n| = \phi(n)$

הוכחה

$$x^{n-1} = \prod_{\mu \in \mu_n(K)} (x-\mu)$$ לכן

$$\Phi_n(x) \mid x^n - 1$$

מסקנה:

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

נוסחת:

$$x^n - 1 = \prod_{\mu \in \mu_n(K)} (x-\mu)$$

סכל $\mu \in \mu_n(K)$ יסודר d מתקיים $d \mid n$.

כיוון ש $\mu_n(K)$ חבורה ציקלית שסדרה n,

אזי לכל $d \mid n$ יש תת-חבורה (ציקלית)

יחידה מסדר d, אשר מסומנת כ- C_d,

ו- μ איבר ב $\mu_n(K)$ שאינו מסדר d.

נקבע את $\prod_{\mu \in \mu_n(K)} (x-\mu)$ לפי:

$$x^n - 1 = \prod_{d \mid n} \left(\prod_{\mu \text{ מסדר } d \text{ ב } \mu_n(K)} (x-\mu) \right) = \prod_{d \mid n} \Phi_d(x)$$

הגדרה:

$$\Phi_1(x) = x - 1$$

p - ראשוני כלשהו:

$$x^p - 1 = \prod_{d|p} \Phi_d(x) = \Phi_1(x)\,\Phi_p(x) = (x-1)\,\Phi_p(x)$$

$$\Rightarrow \Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

- $$x^{p^\mu} - 1 = \prod_{d|p^\mu} \Phi_d(x) = \prod_{j=0}^{\mu} \Phi_{p^j}(x) = \Phi_{p^\mu}(x) \cdot \prod_{j=0}^{\mu-1} \Phi_{p^j}(x)$$

$$= \Phi_{p^\mu}(x) \cdot \left(x^{p^{\mu-1}} - 1\right)$$

כלומר:

$$\Phi_{p^\mu}(x) = \frac{x^{p^\mu} - 1}{x^{p^{\mu-1}} - 1} = \Phi_p\left(x^{p^{\mu-1}}\right) =$$

$$= x^{p^{\mu-1}(p-1)} + x^{p^{\mu-1}(p-2)} + \ldots + x^{p^{\mu-1}} + 1$$

- דוגמה:

$$\Phi_2(x) = x + 1 \qquad \Phi_3(x) = x^2 + x + 1$$

$$\Phi_4(x) = \Phi_2(x^2) = x^2 + 1 \qquad \Phi_9(x) = \Phi_3(x^3) = x^6 + x^3 + 1$$

$$\Phi_8(x) = \Phi_2(x^4) = x^4 + 1 \qquad \Phi_{27}(x) = \Phi_3(x^9) = x^{18} + x^9 + 1$$

$$\Phi_6(x) = ?$$

$$x^6 - 1 = \Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_6(x)$$

לכן:

$$\Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = \frac{x^6 - 1}{(x+1)(x^3-1)} = \frac{x^3+1}{x+1} = x^2 - x + 1$$

משפט באוסו:

כאשר $F = \mathbb{Q}$

1. $\Phi_n(x)$ אי-פריק מעל $\mathbb{Q}$
2. $G \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^* \cong \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$

הוכחה:

(1), (2) שקולים.

אם $\Phi_n(x)$ אי-פריק, אז כמו הוכחנו הוא-פריק

על $\mathbb{Q}$ מעל $\mathbb{Q}$, לכן:

$$\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |G_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}|$$

ואת הכיוון 2 הוכחנו בקורס הקודם הוא

שהכבוד לפי על לכן אוטומורפיזם.

יתר הפולינום הוא-פריק של $\mathbb{Q}$ מעל $\mathbb{Q}$

הוא שמקיים $\varphi(n) = \Phi_n$ שורש.

לכן, $\Phi_n(x)$ הוא הפולינום הוא-פריק

על $\mathbb{Q}$. נפרט, $\Phi_n(x)$ אי-פריק.