

שדות סופיים

נניח ש E שדה סופי.

1. הוכחנו ש $|E| = p^t$ עבור p ראשוני, $(E : \mathbb{F}_p) = t$ ו $\mathbb{F}_p \subseteq E$.
2. [משפט משנה שעברה: $E \setminus \{0\}$ חבורה ציקלית. נובע מהמשפט היסודי של חבורות אבליות סופיות]
3. יש הומומורפיזם "Frobenius" $\varphi_p : E \rightarrow E$ לפי $a \mapsto a^p$

הוכחה: $(a+b)^p = a^p + b^p$, $(ab)^p = a^p b^p$, $1^p = 1$. φ_p חח"ע ולכן על כי $\varphi_p \in \text{Gal}(E/\mathbb{F}_p)$. $|E| < \infty$. $\varphi_p|_{\mathbb{F}_p} = 1_{\mathbb{F}_p}$ לפי מש' הקטן של פרמה.

למה: $o(\varphi_p) = t$

הוכחה: $(E \setminus \{0\}, \cdot)$ חבורה מסדר $n-1$ $\iff \forall a \in E \setminus \{0\} a^{n-1} = 1$
 $\iff \forall a \in E \varphi_p^t(a) = a^n = a \iff o(\varphi) \mid t$

נניח $o(\varphi_p) = j \iff \forall a \in E a^{p^j} = a \iff$ כל איבר של E שורש של $\lambda - \lambda^{p^j}$. לכן, לפי החלק הקל של המש' היסודי של האלגברה $\iff |E| \leq p^j \iff p^t = |E| \leq p^j \iff t \leq j$ לכן $o(\varphi_p) = t$.

מסקנה

E שדה פיצול של $\lambda^n - \lambda$ מעל \mathbb{F}_p ולכן הרחבת גלואה (נבדוק בהמשך)
 $\text{Gal}(E/\mathbb{F}_p) = \langle \sigma_p \rangle$

הוכחה

$|\langle \sigma_p \rangle| = t = |\text{Gal}(E/\mathbb{F}_p)| = [E : \mathbb{F}_p] = t \iff \langle \sigma_p \rangle \subseteq \text{Gal}(E/\mathbb{F}_p)$
 $\langle \sigma_p \rangle = \text{Gal}(E/\mathbb{F}_p) \iff |\text{Gal}(E/\mathbb{F}_p)| = t$

למה

$\lambda^n - \lambda$ פולינום ספרבילי מעל \mathbb{F}_p .

הוכחה

$$(\lambda^n - \lambda)' = \underbrace{n\lambda^{n-1}}_{=0 \iff n=p^t} - 1 = -1$$

לכן $\lambda^n - \lambda$ ספרבילי.

φ_p הסדר של $o(\varphi_p) = t$

סיכום

$$\lambda^n - \lambda = \prod_{a \in E} (\lambda - a)$$

מסקנה

אם $|E_1| = |E_2| = n$ אז $E_1 \cong E_2$.

הוכחה

שניהם שדה פיצול של $\lambda^n - \lambda$ מעל \mathbb{F}_p .

אינטואיציה

הדרך לבנות שדה מסדר $n = p^t$:
ניקח פולינום אי פריק f מדרגה t מעל \mathbb{F}_p ונגדיר $E = \mathbb{F}_p[\lambda]/\mathbb{F}_p[\lambda]f$.

דוגמה

שדה $\mathbb{F}_4 \cong \mathbb{F}_2[\lambda]/\mathbb{F}_2[\lambda](\lambda^2 + \lambda + 1)$.

הערה: היינו חייבים לקחת את הפולינום $\lambda^2 + \lambda + 1$, כי הוא היחיד שאי פריק.

שדה אחר: $\mathbb{F}_8 \cong \mathbb{F}_2[\lambda]/\mathbb{F}_2[\lambda](\lambda^3 + \lambda + 1) \cong \mathbb{F}_2[\lambda]/\mathbb{F}_2[\lambda](\lambda^3 + \lambda^2 + 1)$.

דרך אחרת לבנות שדה מסדר $n = p^t$

ניקח \tilde{E} = שדה הפיצול של $\lambda^n - \lambda$ מעל \mathbb{F}_p . ניקח $E = \tilde{E}^G$ כאשר $G = \langle \sigma_p^t \rangle$. לפי הגדרה

$$E \text{ הוא שדה } \lambda^n - \lambda \text{ שדה } \left\{ a \in \tilde{E} \mid \underbrace{\sigma_p^t(a)}_{=a^n} = a \right\} = \{\text{roots of } \lambda^n - \lambda\}.$$

בסופו של דבר $\tilde{E} = E$.

שימוש

איך מוצאים פולינומים f אי פריקים מדרגה t מעל \mathbb{F}_p ?

תשובה

$$f \mid \lambda^n - \lambda$$

דוגמה

מעל $\mathbb{F}_2 (+1 = -1)$
 $\lambda^8 - \lambda = \lambda(\lambda - 1)(\lambda^2 + \lambda + 1)$ - לא נכון! הוא מדרגה 2, אבל
 $\lambda^8 - \lambda$ הוא ממימד 3, ו-2 נתקן:

$$\lambda^8 - \lambda = \lambda(\lambda - 1)(\lambda^3 + \lambda + 1)(\lambda^3 + \lambda^2 + 1)$$

נמשיך:

$$\lambda^{16} - \lambda = \underbrace{\lambda(\lambda - 1)(\lambda^2 + \lambda + 1)}_{\lambda^4 - \lambda} (\lambda^4 + \lambda^3 + 1)(\lambda^4 + \lambda^2 + 1)(\lambda^4 + \lambda + 1)(\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1)$$

אבל כאן אנו מקבלים דרגה גבוהה מדי! $1 + 1 + 2 + 4 + 4 + 4 + 4 = 20$. הסיבה לכך היא שאחד מהם פריק: $(\lambda^4 + \lambda^2 + 1) = (\lambda^2 + \lambda + 1)^2$. לכן

$$\lambda^{16} - \lambda = \lambda(\lambda - 1)(\lambda^2 + \lambda + 1)(\lambda^4 + \lambda^3 + 1) \cancel{(\lambda^4 + \lambda^2 + 1)} (\lambda^4 + \lambda + 1)(\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1)$$

$$\lambda^{16} - \lambda = \lambda(\lambda - 1)(\lambda^2 + \lambda + 1)(\lambda^4 + \lambda^3 + 1)(\lambda^4 + \lambda + 1)(\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1)$$

נשים לב ש $\mathbb{F}_4 \subseteq \mathbb{F}_{16}$, כי $\lambda^4 - \lambda \mid \lambda^{16} - \lambda$.

דוגמה

מה המבנה של $\mathbb{Q}[\rho]$ עבור ρ שורש n -פרימיטיבי של 1?

נשים \heartsuit : $\mathbb{Q}[\rho]$ שדה פיצול של $\lambda^n - 1$ מעל \mathbb{Q} , לכן הרחבת Galue.

מה $[\mathbb{Q}[\rho] : \mathbb{Q}]$? יותר כללי:מה $[\text{Gal}(\mathbb{Q}[\rho] / \mathbb{Q})]$?
 עבור n ראשוני התשובה היא $n - 1$ כי $\lambda^{n-1} + \dots + \lambda + 1$ פולינום אי פריק.

למה כללית

נניח E שדה ו- G חבורת אוטומורפיזמים של E ו- $a_1, \dots, a_m \in E$ שונים כאשר עבור כל $\sigma \in G$, $\{\sigma(a_1), \dots, \sigma(a_n)\} = \{a_1, \dots, a_n\}$.
 במילים אחרות, כל $\sigma \in G$ פועל כתמורה על ה- a_i .
 נגדיר

$$f = \prod_{i=1}^m (\lambda - a_i) \in E[\lambda]$$

אי

$$f \in E^G[\lambda]$$

הוכחה

$$f = \sum_{i=0}^m \alpha_i \lambda^i \text{ לכתוב}$$

$$\forall \sigma \in G \sum_{i=0}^m \sigma(\alpha_i) \lambda^i = \sigma(f) = \sigma\left(\prod_{i=0}^m (\lambda - a_i)\right) = \prod_{i=0}^m (\sigma(\lambda) - \sigma(a_i)) =$$

$$= \prod_{i=0}^m (\lambda - \sigma(a_i)) = \prod_{i=0}^m (\lambda - a_i) = f = \sum_{i=0}^m \alpha_i \lambda^i$$

$$\therefore \forall \sigma \in G \forall_i \sigma(\alpha_i) = \alpha_i$$

$$\therefore \forall_i \alpha_i \in E^G$$

$$f_n = \prod_{(j,n)=1} (\lambda - \rho^j) \text{ נגדיר}$$

$E = \mathbb{Q}[\rho]$ נשים \heartsuit ש $\text{Gal}(E/\mathbb{Q})$ פועל כתמורות על השורשים הפרימיטיביים של 1.
 $f \in E^{\text{Gal}(E/\mathbb{Q})}[\lambda]$ לכן הלמה אומרת ש

למה

$$\lambda^n - 1 = \prod_{d|n} f_d$$

הוכחה

$$\lambda^n - 1 = \prod_{1 \leq j \leq n} (\lambda - \rho^j) = \prod_{d|n} \prod_{(j,n/d)=1} (\lambda - (\rho^d)^j) = \prod_{d|n} f_{n/d} = \prod_{d|n} f_d$$

טענה

$$\forall_n f_n \in \mathbb{Z}[\lambda]$$

הוכחה

לפי אינדוקציה על n .

נניח $f_d \in \mathbb{Z}[\lambda]$ עבור כל $d \mid n, d \neq n$.

$$\lambda^n - 1 = f_n \prod_{\substack{d \mid n \\ d < n}} f_d \in \mathbb{Z}[\lambda]$$

לפי אינדוקציה $f_n \in \mathbb{Z}[\lambda]$ לפי למת Galue.

משפט

f_n אי פריק ב $\mathbb{Z}[\lambda]$

הוכחה

לפי למת Galue, מספיק להוכיח f_n אי פריק ב $\mathbb{Z}[\lambda]$.
 בדרך השלילה נניח $f_n = gh, g, h \in \mathbb{Z}[\lambda]$, לא קבועים.
 נגדיר: $f_n = \prod_{(f,n)=1} (\lambda - \rho^j)$. נניח(בתוך E):

• ρ שורש של g

• ρ^j שורש של h

• $(j, n) = 1$

$j = p_1 p_2 \dots p_n$ עבור ראשוניים p_i , לאו דווקא שונים אבל זרים ל n .
 קיים מספר s כך ש $\rho^{p_1 \dots p_s}$ שורש של g ו $\rho^{p_1 \dots p_{s+1}}$ שורש של h . לפי שינוי שמות, אפשר
 להניח ρ שורש של g , ρ^p שורש של h , כאשר $p = pp_{s+1}$ (זר ל n) $\Leftarrow \rho$ שורש של $h(\lambda^p)$.
 כלומר: $h(\lambda^p) \mid g$ בעלי שורש משותף(כלומר ρ) $\Leftarrow g, h(\lambda^p)$ אינם זרים ב $\mathbb{Z}[\lambda]$.
 ניקח $q(\lambda) = \gcd(g, h(\lambda^p)) \in \mathbb{Z}[\lambda]$.
 עכשיו נעבור מודולים ל $(\mathbb{Z}/p\mathbb{Z})[\lambda]$, לכתוב

$$\bar{f} = f + p\mathbb{Z}[\lambda] \in (\mathbb{Z}/p\mathbb{Z})[\lambda]$$

$$\bar{f}_n = \bar{g}\bar{h}$$

$$\overline{h(\lambda^p)} = \overline{h(\lambda)^p} \text{ Fermat+Frobenious } \bar{q} \mid \bar{g} \text{ ו } \bar{q} \mid \overline{h(\lambda^p)}$$

$$\left(\sum [\alpha_i] \lambda^i \right)^p = \sum [\alpha_i]^p \lambda^{ip} = \sum [\alpha_i] (\lambda^p)^i = \overline{h(\lambda^p)}$$

לכן \bar{h}^p אינם זרים. לכן \bar{g}, \bar{h} אינם זרים. לכן $\bar{f} = \bar{g}\bar{h}$ אינו ספרבילי.

$$\bar{f}_n \mid \overline{\lambda^n - 1}$$

$$(\overline{\lambda^n - 1})' = (\overline{\lambda^n - 1})' = n\overline{\lambda^{n-1}}$$

\bar{f}_n ספרבילי $\Leftarrow \bar{f}_n \mid n\overline{\lambda^{n-1}}$ לכן $\bar{f}_n \mid \overline{\lambda^n - 1}$ לכן $\bar{f}_n \mid \overline{\lambda^n - 1}$ וזו סתירה.

המשפט היסודי של תורת Galois

התנאים הבאים שקולים עבור E/F סופי.

I. E/F Galois שדה פיצול של פולינום ספרבילי מעל F

II. $E^G = F$ עבור איזושהי חבורה $G = \text{Gal}(E/F)$

III. E הרחבה ספרבילית ונורמלית של F .

הוכחה

$I \iff II$ עשינו

$III \iff II$ לוקחים $a \in E$. G עושה תמורה של הורשים של הפולינום $f = \prod_{\sigma \in G} (\lambda - \sigma(a))$

לכן $f \in E^G[\lambda] = F[\lambda]$, $\sigma(a)$ שונים. f ספרבילי ומתפצל, לכן הפולינום המינימלי של a מחלק את $f \iff$ ספרבילי ומתפצל.

$I \iff III$ $E = F[a_1, \dots, a_t]$. ניקח f_i פולינום המינימלי של a_i , ואז $f_i =$
no
duplicates

$f \iff E$ שדה פיצול של f מעל F .