

תזכורת

מגדל שורשים: נתון ספרבילי K/F . קיים $F = F_0 \subset F_1 \subset \dots \subset F_t = E \supset K$ כך ש $F_{i+1} = F_i[a_i]$, $a_i \in F_i$, גובה m אם כל $m_i \leq m$.

משפט

קיים מגדל שורשים עבור K/F $\iff K$ מוכל מהרחבה Galois E מעל F כאשר $\text{Gal}(E/F)$ פתירה (המנות מסדר $m \geq 2$).

מסקנה

(אחרי הוספת שורשי יחידה m פרימיטיביים ל F) אפשר לקחת $E = \text{סגור הנורמלי של } K$.

הוכחה לפי תמונה: \bar{E} הסגור הנורמלי של K .

$$\begin{array}{c} \bar{E} \\ | \\ F \end{array}$$

$$\text{Gal}(\bar{E}/F) = \text{Gal}(E/F)/\text{Gal}(E/\bar{E})$$

הכיוון השני נובע מהמשפט המרכזי + שימוש ב-Lagrange Resolvment.

הגדרה

אם $f \in F[\lambda]$, $\text{Gal}_f = \text{Gal}(E/F)$ כאשר $E = \text{שדה הפיצול של } f \text{ מעל } F$.

תרגום: f פתיר לפי רדיקלים (יש מגדל שורשים) $\iff \text{Gal}_f$ חבורה פתירה.

שימוש I - מספר בעל בניה.

כאן $m = 2$. כלומר a בעל בניה $\iff \text{Gal}_{f_a}$ הפולינום המינימלי של a הוא חבורה פתירה מסדר חזקת 2.

כל חבורה מסדר חזקת 2 היא פתירה (אפילו נילפוטנטית), לכן a בעל בניה $\iff [E:F] = |\text{Gal}_{f_a}|$ חזקת ש.2.

זהירות! אם $\deg a = 4$ $\neq |\text{Gal}_{f_a}|$ חזקת 2.

אבל ברור שאם $\deg a$ אינו חזקת 2 אז a אינו בעל בניה. למשל:

I. $\sqrt[3]{2}$ אינו בעל בניה (מעל \mathbb{Q})

II. $\cos 20^\circ$ אינו בעל בניה (מעל \mathbb{Q}) (גם מדרגה 3)

III. π אינו בעל בניה (משפט Weierstrass Lindenmann 1888(?))

IV. שורש e - n -פרימיטיבי של 1 \iff Kulen (n) חבורה(פתירה) מסדר חזקה 2 \iff $\varphi(n)$ חזקת 2. לכתוב

$$n = 2^{t_1} p_2^{t_2} \cdots p_k^{t_k}$$

p_i ראשוניים אי זוגיים

$$\varphi(n) = \varphi(2^{t_1}) \varphi(p_2^{t_2}) \cdots \varphi(p_k^{t_k})$$

$$\varphi(2^{t_1}) = 2^{t_1-1}$$

$$\varphi(p^t) = p^{t-1}(p-1)$$

חזקת 2 \iff $t=1$ $p-1$ חזקת 2.

$$n = 2^t p_1 \cdots p_k$$

כאשר p_i ראשוניים(שונים) ו $p_i - 1$ חזקת 2 נקרא ראשוני Fermat.

מתי p ראשוני Fermat? לכתוב $u = 2^v w$, $p - 1 = 2^u$ כאשר w אי זוגי

$$v = 2^{2^v w} + 1 = (2^{2^v})^w + 1 = (2^{2^v} + 1) (2^{2^v(w-1)} - 2^{2^v(w-2)} + \cdots + 1)$$

סתירה אלא אם $w \in 1$.

שימוש II - פתרון של פולינום f לפי רדיקלים: = בניית מגדל שורשים

תרגום: מתי Gal_f חבורה פתירה?

יש לנו שיכון טבעי $\text{Gal}_f \hookrightarrow S_n$ כאשר $n = \deg f$ לפי תמורה של השורשים של f (תוך שדה פיצול).

עבור $n = 3, 4$, S_n חבורה פתירה ולכן Gal_f חבורה פתירה.

עבור $n = 5$ אינה חבורה פתירה.

השאלה ההפוכה

בתורת Galois, נתונה חבורה G סופית(אולי יחד עם F). האם קיים $F[\lambda]$ כאשר $\text{Gal}_f = G$?

אם לא קובעים את F , ניקח $G \subset S_n$, $E =$ שדה שברים של $F_0[\lambda_1, \dots, \lambda_n]$ (נגיד $F_0 = \mathbb{Q}$). לכתוב

$$F(\lambda_1, \dots, \lambda_n)$$

נגדיר

$$\forall \pi \in S_n \sigma_\pi \left(\frac{f(\lambda_1, \dots, \lambda_n)}{g(\lambda_1, \dots, \lambda_n)} \right) = \frac{f(\lambda_{\pi 1}, \dots, \lambda_{\pi k})}{g(\lambda_1, \dots, \lambda_{\pi k})}$$

שורש של E לפי התיאוריה.

$$G = \text{Gal}(E/F) \text{ אז } F = E^G$$

מטרה

נבנה פולינום $f \in \mathbb{Q}[\lambda]$ אי פריק מדרגה 5 כאשר $\text{Gal}_f = S_5$ (לא פתירה)
נניח n ראשוני. אז $n \mid |G| \iff \sigma \in G$ מסדר f לפי משפט Cauchy $G \iff$
מכיל מחזור של S_n .

משפט

אם $G \subseteq S_n$ ו- G מכיל חילוף ומחזור מסדר n אז $G = S_n$.

לכך

מספיק למצוא איבר של Gal_f שחילוף ביחס לשיכון הטבעי $S_n \hookrightarrow \text{Gal}_f$. כלומר רוצים
אוטומורפיזם שמחליף 2 שורשים וקובע את האחרים.
אפשר לקחת σ עם f בעל בדיוק 2 שורשים לא ממשיים. כלומר הגרף של f צריך לעבור
את ציר ה- x בדיוק $n-2$ פעמים.

$$f = \lambda^5 - pq\lambda + p$$

p ראשוני, $q \in \mathbb{Z}$

$$f' = 5\lambda^4 - pq$$

$$f'(x) = 0 \implies x = \pm \sqrt[4]{\frac{pq}{4}}$$

עבור x הזה

$$f(x) = x(x^4 - pq) + p = x\left(\frac{pq}{5} - pq\right) + p =$$

$$= p\left(-\frac{4}{5}qx\right) + p = p\left(-\frac{4}{5}qx + 1\right)$$

$$x = -\sqrt[4]{\frac{pq}{5}}$$

ברור ש $f(x) > 0$ נשאר: האם $(x = \sqrt[4]{\frac{pq}{5}})$ הוא שלילי? ברור שכן
אם g גדול מספיק.

המשך הקורס

(1) איך לבנות מספר בעל בניה?

שיטה אלגברית: רוצים לבנות שדות בניס מהחבורות שלהם.

$$L = E^H \text{ - רוצה לבנות איברים של } L.$$

למשל אם $[E : \mathbb{Q}] = 4$ רוצים לבנות $a \in E$ מדרגה 2.

הגדרה

נתון $a \in E$ ו $L = E^H, H \subset G$ מגדירים (trace) tr ע"י

$$\text{tr}_{E/L}(a) = \sum_{\sigma \in H} \sigma(a)$$

$$N_{E/L}(a) = \prod_{\sigma \in H} \sigma(a)$$

לכל $\tau \in H$,

$$\tau(\text{tr}_{E/L}(a)) = \tau\left(\sum_{\sigma \in H} \sigma(a)\right) = \sum_{\sigma \in H} \tau\sigma(a) = \text{tr}(a) \implies \text{tr}(a) \in E^H$$

אותו סוג נימוק $\iff N(a) \in E^H$
מגדירים

$$\text{tr}_{E/L} : E \rightarrow L$$

$a \mapsto \text{tr}_{E/L}(a)$

$$N : E \rightarrow L$$

$a \mapsto N_{E/L}(a)$

בפעם הבאה נדבר על אלו, ואולי גם על הדיסקרימיננטות האחרות.