

$f \in F[x]$ - פולינום בתוך שדה. מחפשים שורש a של f .
 אם $\deg f = 1$ אז אפשר למצוא פתרון בתוך השדה (למשל $F = \mathbb{Q}$), אבל אם $\deg f > 1$ אז יכול להיות שצריך לעבור לשדה יותר גדול (למשל $F = \mathbb{R}$ או $F = \mathbb{C}$). אבל לאיזה שדה?
 אם $\deg f = 2$ ו $\frac{1}{2} \in F$ אז $a \in F(\sqrt{b})$ עבור איזהו $b \in F$.
 באופן כללי, מחפשים שדה $K \supset F$ (כותבים K/F - נקרא הרכבת שדות) כאשר K מכיל שורש a של f .
 בגישה אחת אנחנו רוצים לעבוד בתוך שדה גדול וטוב מאוד L - למשל סגור אלגברית, כמו \mathbb{C} - כדי שיהיו לנו שורשים לכל הפולינומים, ואז השיטה היא לקחת $a \in L$ שורש של f , ולעבוד עם השדה $F[a] \subset L$. אם g הפולינום המינימלי של a אז יודעים ש $g \mid f$ או פריק. $[F[a] : F] = \deg g$.
 גישה אחרת אומרת שנבנה את השדה הדרוש לפי הבעיה - כלומר אם נתון השדה F והפולינום f נרצה לבנות K/F כאשר K מכיל שורש a של f . כאן השיטה היא לקחת $g \in F[\lambda]$ פולינום אי פריק שמחלק את f , ואז $F[\lambda]/F[\lambda]g$ שדה. $\bar{\lambda} = \lambda + F[\lambda]g$ שורש של g בתוך השדה K . $K \cong F[a]$, $\bar{\lambda} \leftrightarrow a$.
 מתברר ש g שמקבלים בשיטה הראשונה וה g שמקבלים בשיטה השנייה הוא אותו g .

דוגמה

a הוא שורש 3-פרימיטיבי של 1

- הגדרה:**
- ρ הוא שורש n - של 1 אם $\rho^n = 1$
 - ρ הוא שורש n -פרימיטיבי של 1 אם $\rho^m \neq 1$ לכל $m < n$ הוא שורש- n של 1.

אם נסתכל על מעגל היחידה ב \mathbb{C} , נראה ש

$$\{n\text{-roots of } 1\} = \left\{ e^{2\pi k i/n} \mid k \in \mathbb{Z} \right\} = \left\{ e^{2\pi k i/n} \mid 0 < k \leq n \right\}$$

$$\{n\text{-primitive roots of } 1\} = \left\{ e^{2\pi k i/n} \mid \begin{array}{l} (k, n) = 1 \\ 0 \leq k < n \end{array} \right\}$$

אם יש לנו שורש n -פרימיטיבי אפשר להשתמש בו בשביל למצוא את כל שורשי- n ולבנות מצולע משוכלל¹

עבור $n = 3$, הפולינום המינימלי הוא $\lambda^2 + \lambda + 1 = 0$, והשורשים הם $\rho, \rho^2 = \bar{\rho}$.
 (עבור n כללי, $\rho^{-1} = \bar{\rho} = \rho^{n-1}$).

הערה: כאשר מדברים על שורש פרימיטיבי, תמיד מדברים על שדה אם מאפיין 0. למשל ב \mathbb{Z}_2 אין שורש 2-פרימיטיבי ל1.

כאשר $\mathbb{Q}[\rho] \cong \mathbb{Q}[\lambda]/\mathbb{Q}[\lambda]g$ כאשר $g = \lambda^2 + \lambda + 1$ הפולינום המינימלי של ρ מעל \mathbb{Q} . אבל הוא גם הפולינום המינימלי של ρ^2 מעל \mathbb{Q} (כי $\rho^2 = \bar{\rho}$), ולכן

$$\mathbb{Q}[\rho] \cong \mathbb{Q}[\lambda]/\mathbb{Q}[\lambda]g \cong \mathbb{Q}[\lambda]/\mathbb{Q}[\lambda]g$$

¹אם יש שורש- n לא פרימיטיבי, אז אי אפשר למצוא את כל השורשים באמצעים גיאומטריים.

כל זאת עבור $n = 3$ - מה עם n יתר גבוהים?
 ניקח $n = 4$. השורשים ה-4 פרימיטיביים הם $\pm i$ והפולינום המינימלי הוא $g = \lambda^2 + 1$
 ניקח $n = 5$. הפולינום המינימלי הוא $g = \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1$.
 באופן כללי - עבור n ראשוני הפולינום המינימלי של ρ הוא $\sum_{i=0}^{n-1} \lambda^i$.
 עבור n לא ראשוני זה יותר מסובך. ראינו את זה בדוגמה על 4, ועבור $n = 6$ הפולינום המינימלי הוא $\lambda^2 - \lambda + 1$.

דוגמה

$\sqrt[3]{2} \in \mathbb{Q}[\sqrt[3]{2}]$ (מספר ממשי). הפולינום המינימלי הוא $\lambda^3 - 2$. כל השורשים הם $\{\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}\}$. יש הבדל אנליטי בין השורשים השונים, אבל אין הבדל אלגברי ביניהם. אם מדברים רק על פעולות של $+$ ו- $*$, אז אין הבדל בין השורשים - אם רוצים להבדיל ביניהם צריך לדבר על מושגים לא-אלגבריים כמו סדר או טופולוגיה.
 למשל, $\sqrt{2}$ ו- $-\sqrt{2}$ הם שונים - כי אחד חיובי ואחד שלילי - אבל אי אפשר להבדיל ביניהם עם פעולות אלגבריות. כלומר $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[-\sqrt{2}]$.

טענה

אם a, b שורשים של אותו פולינום אי-פריק מעל F , אז קיים איזומורפיזם $F[a] \rightarrow F[b]$ לפי $a \mapsto b$.

הוכחה

$$F[a] \xrightarrow{a \mapsto \bar{\lambda}} F[\lambda]/\langle g \rangle^2 \xrightarrow{\bar{\lambda} \mapsto b} F[b]$$

הגדרה

אוטומורפיזם (automorphism) של K מעל F הוא איזומורפיזם $\sigma : K \rightarrow K$ שקובע את $(\forall \alpha \in F \sigma(\alpha) = \alpha)F$.
 כותבים $\sigma \in \text{Gal}(K/F)$. נקרא חבורת הגלואה של K/F .

מצד שני

אם $\sigma \in \text{Gal}(K/F)$ ו- a שורש של $f \in F[\lambda]$ אז $\sigma(a)$ גם שורש של f .

יותר כללי: משפט

נניח $\varphi : F_1 \rightarrow F_2$ הומומורפיזמים של שדות. ניקח $\sum_{i=0}^t \alpha_i \lambda^i = f \in F_1[\lambda]$ נגדיר:
 $\sigma : K_1 \rightarrow K_2$ נניח $K_1 = F_1(a_1)$ ו $\sigma : K_1 \rightarrow K_2$ הוא הומומורפיזם כך ש $a/F_2 = \varphi$.
אם a_1 שורש של f , אז $\sigma(a_1)$ שורש של f_φ .

הוכחה

$$f_\varphi(\sigma(a_1)) = \sum \varphi(\alpha_i) \sigma(a_1)^i = \sum \sigma(\alpha_i) \sigma(a_1)^i = \sigma\left(\sum \alpha_i a_1^i\right) = \sigma(f(a_1)) = \sigma(0) = 0$$

מסקנה

האוטומורפיזמים בעצם מסדרים מחדש את השורשים - כלומר $\text{Gal}(K/F) \leq S_n$ כאשר $n = \deg a$.

הערה

הסקנו ש $\text{Gal}(K/F)$ היא תת חבורה של S_n - אבל השאלה איזו תת חבורה של S_n היא שאלה פתוחה עד היום.