

**חוברת תרגולים בקורס "תורת גלואה"
88-311**

21 בפברואר 2017

**מתרגלת: שירה גילת
סמסטר א' - 2017 תשע"ז**

ערך: איתי רוזנבאום

תורת גלואה – תרגול ראשון

חזרה מחוגים

F שדה

$F[\lambda]$ חוג הפולינומים עם מקדמים ב- F .

זהו חוג אוקלידי, כלומר לכל פולינומים f, g יש פולינומים q, r כך ש

$$f = qg + r \quad \text{או } \deg r < \deg g \text{ או } r = 0$$

דוגמא

$$\gcd(x^3 - 2x^2 + 1, x^2 - x - 3) = 1 \quad \mathbb{Q}[X]$$

מסקנה 0.1 חוג הפולינומים הוא ראשי, כלומר כל אידיאל נוצר ע"י איבר אחד.

$$I = \langle f(x) \rangle = F[x] \cdot f(x)$$

עוד תכונה טובה

אם f אי פריק, אזי המנה $F[x]/\langle f(x) \rangle$ למעשה כל הרחבת שדות של F הוא שרשרת של כאלה..

פריקות של פולינומים

האם הפולינום f הוא פריק מעל $F[x]$?

1. כל פולינום מדרגה 1 הוא אי פריק

2. $a \in F$ שורש של $f \Leftrightarrow (x - a) | f(x)$ ב- $F[x]$. בפרט, אם לפולינום מדרגה גדולה מאחת יש שורש אז הוא פריק. ההפך לא נכון.

3. אם הפולינום מדרגה 2 או 3 אז הוא פריק אמ"מ יש לו שורש. למשל $x^3 - x + 1$ אי פריק מעל \mathbb{Z}_3 כי נוכל לעבור על כל האיברים בשדה ולבדוק שאין שורש.

4. אם יש לו שורש $\frac{r}{q}$ רציונלי (מצומצם) אזי $a_n | a_0, q | a_n$. למשל $x^3 - x - 6$ מעל \mathbb{Q} , מצאו פירוק לגורמים אי פריקים. לפי הנל אם יש שורש $\frac{r}{q}$ אז $q | 1$ ו- $r | 6$ ולכן האופציות הן $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ וע"י מעבר על כולם נמצא ש-2 הוא שורש. $x^3 - x - 6 = (x - 2)(x^2 + 2x + 3)$

5. קריטריון אייזנשטיין $a_n x^n + \dots + a_0$ אם יש p ראשוני כך ש $p \nmid a_n, p \mid a_{n-1}, \dots, a_0$ ו $p^2 \nmid a_0$ אז f אי פריק. למעשה $x^n - 4x + 2$ אי פריק לפי אייזנשטיין עם $p = 2$

6. $f(x)$ אי פריק $\Leftrightarrow f(x+c)$ אי פריק. למעשה $f(x) = x^4 + 4x^3 + 6x^2 - 1$ אי פריק מעל \mathbb{Q} כי $f(x-1) = x^4 - 4x + 2$ שאי פריק לפי 5.

7. רדוקציה $f(x) \in \mathbb{Z}[x]$ ו p ראשוני. נסמן $\overline{f(x)} \in \mathbb{Z}_p[x]$ ("להפעיל על המקדמים מודולו p "), אם $\deg \overline{f} = \deg f$ אזי אם \overline{f} אי פריק $\Leftarrow f$ אי פריק. לדוגמא, עבור $8x^3 - 6x - 1$ ניקח $p = 3$ ונקבל $2x^3 - 1$ שפריק ולכן לא עוזר לנו. $p = 5$ נקבל $3x^3 - x - 1$ וזה אינו פריק ולכן גם הפולינום המקורי שלנו לא פריק ב $\mathbb{Z}[x]$

מציאת שורשים לפולינום

עבור פולינום מדרגה 2 $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$, נשלים לריבוע $(x + \frac{b}{2a})^2 + \frac{c}{a} - \frac{b^2}{4a^2} = 0$ ואז נקבל את נוסחת השורשים. נשם לב שנוסחה זו עובדת לכל שדה שהמאפיין בו הוא 2.

מאפיין של שדה המספר הטבעי הקטן ביותר כך ש $1 + 1 + \dots + 1 = 0$. אם אין כזה, המאפיין הוא 0.

תורת גלואה – תרגול שני

בנייה בסרגל ומחוגה

חושבים על המישור \mathbb{R}^2 .

כללי המשחק

נתון לנו ציר ה- x והנק 0 ו- $(0, 0)$ ו- $(1, 0)$.
מותר לנו:

1. להעביר ישר בין שתי נקודות
 2. להעביר מעגל בעזרת שתי נקודות
 3. כל נקודת חיתוך היא נקודה חדשה שלנו.
- כל הנקודות שניתן להגיע אליהן ככה נראות ברות בנייה.
מספר a ברי בנייה אם $(a, 0)$ היא נקודה בת בנייה.

טענה 0.1 אם יש נקודה מרחק a מ- 0 (אם ניתן לבנות קטע באורך a) אז המספר a ברי בנייה.

ראינו בהרצאה

אם a, b ברי בנייה אז גם $a + b, a - b, ab, \frac{a}{b}$ ברי בנייה.

מסקנה 0.2 אוסף המספרים ברי הבנייה זה שדה!

טענה 0.3 אם a ברי בנייה אז \sqrt{a} ברי בנייה.

הוכחה: a ברי בנייה, לכן $\frac{1+a}{2}, \frac{1-a}{2}$ ברי בנייה (לפי טענה קודמת). נעביר מעגל שמרכזו ב- 0 ורדיוסו $\frac{1+a}{2}$ ולכן זהו גם החיתוך עם ציר ה- y . נעביר ישר מהחיתוך על ציר ה- y לנקודה $1 - \frac{1+a}{2}$. הגענו למשולש ישר זווית, ולפי פתגורס אורך היתר שלו \sqrt{a} ■

שורשי יחידה

הגדרה 0.4 יהי F שדה, איבר $p \in F$ נקרא שורש יחידה n פרימיטיבי אם $p^n = 1$ וגם $p^i \neq 1$ לכל $1 \leq i < n$.

הערות

1. ב \mathbb{C} לכל n יש שורש יחידה n -פרימיטיבי לדוגמא $p_n = e^{\frac{2\pi i}{n}}$

2. אם p שורש יחידה n -פרימיטיבי אזי p^k שורש יחידה פרימיטיבי $\Leftrightarrow (k, n) = 1$

תרגיל

יהי p שורש יחידה n פרימיטיבי

א. הוכיחו כי $1, p, \dots, p^{n-1}$ הם כולם שונים זה מזה

ב. הוכיחו כי $x^n - 1 = \prod_{i=1}^n (x - p^i)$ הוכחה: א. נניח בשלילה $p^i = p^j$ כאשר $i \leq j$. זה אומר ש $p^{j-i} = 1$ אבל $1 \leq j - i < n$ וזה סתירה לכך ש p פרימיטיבי.

ב. נשם לב שכל p^i הוא שורש של $x^n - 1$ ומכיוון שהם שונים, אלו הם כל n השורשים של הפולינום ולכן $x^{n-1} = (x - 1) \cdot \dots \cdot (x - p^{n-1})$ ■

הרחבת שדות

אם $F \subseteq K$ שדות מסמנים K/F ואומרים ש K היא הרחבה של F . בפרט, K הוא מרחב וקטורי מעל F . את המימד שלו מסמנים ב $[K : F]$. זו נקראת **דרגת ההרחבה**. למשל $[C : R] = 2$ (בסיס $\{1, i\}$) ו $[C : Q] = \infty$

בנייה 1 (חיצונית)

נתון F שדה, לוקחים פולינום $f(x) \in F[x]$ אי פריק ואז $\langle f(x) \rangle$ היא שדה. יש שיכון $F \hookrightarrow F[x] / \langle f \rangle$ ע"י $a \mapsto \bar{a} = a + \langle f \rangle$ ולכן זו הרחבת שדות. נשם לב שבהרחבה $\bar{x} + \langle f \rangle = x + \langle f \rangle$ הוא שורש של הפולינום של f . לדוגמא $\langle x^2 + 1 \rangle$ נקבל ש $\bar{x}^2 + 1 = \overline{x^2 + 1} = \bar{0}$ ולכן \bar{x} שורש.

בנייה 2 (פנימית)

נתון שדה F והרחבה K/F ואיבר $a \in K$. אזי מגדירים $F(a)$ להיות השדה הקטן ביותר שמוכל ב K ומכיל את F ואת a . לכן $F(a)$ הוא חיתוך כל תתי השדות של K שמכילים את F ואת a .

¹לשם לב ש \ מסמל לפעמים חוג מנה ולפעמים הרחבה, נבין מההקשר

דוגמא

$$1. (\sqrt{2})^{-1} = \frac{1}{2}\sqrt{2}, (\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$$

$$2. \mathbb{Q}(\rho_n) = \{a_0 + \dots + a_{n-1}\rho_n^{n-1} | a_i \in \mathbb{Q}\} \text{ כאשר } \rho_n \text{ שורש יחידה } n\text{-פרימטיבי.}$$

$$3. \mathbb{Q}(\pi) = \dots \text{ מסובך.}$$

אפשר גם לספח יותר איברים (אבל לא את שטחי C).

תרגיל $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ הוכחה: ימין מוכל בשמאל כי ברור ש $\sqrt{2} + \sqrt{3}$ נשם לב ש $(\sqrt{2} + \sqrt{3})^2 = 5 + \sqrt{6}$ ולכן $\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ אזי $\sqrt{6}(\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ ולכן $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. $2\sqrt{3} + 3\sqrt{2} - 2(\sqrt{2} + \sqrt{3}) = \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. לכן $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ ולכן ממינימליות סיימנו ■

תורת גלואה – תרגול 3

תזכורת

יהי ראשוני p אלגברי מעל F . אזי $\alpha \in E/f$ אלגברי מעל F . אזי $F[x]/\langle f(x) \rangle \cong F[\alpha] = F(\alpha)$ כאשר $f(x)$ הפולינום המינימלי של α .

דוגמא

p ראשוני, ρ_p שורש יחידה p -פרימיטיבי, אז הפולינום המינימלי $\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \dots + 1$ ולכן $[\mathbb{Q}[\rho_p] : \mathbb{Q}] = p - 1$

תרגיל

הפולינום המינימלי של α מעל F הוא $p(x) = x^3 - 6x^2 + 9x + 11$ מהו הפולינום המינימלי של $\frac{1}{\alpha}$?

פתרון

לפי הנתון $\alpha^3 - 6\alpha^2 + 9\alpha + 11 = 0$
נחלק ב α^3
 $1 - 6\frac{1}{\alpha} + 9(\frac{1}{\alpha})^2 + 11(\frac{1}{\alpha})^3 = 0$
ולכן $\frac{1}{\alpha}$ מאפס את הפולינום $1 - 6x + 9x^2 + 11x^3$
זהו פולינום אי פריק כי אין לו שורשים ומדרגה 3 (כי אם β היה שורש, $\frac{1}{\beta}$ היה גם שורש של $p(x)$) ולכן זהו הפולינום המינימלי של $\frac{1}{\alpha}$.

סיפור

יהי α אלגברי מעל F עם פולינום מינימלי $f(x)$ $F[\alpha] \cong F[x]/\langle f(x) \rangle$
אם β שורש אחר של $f(x)$ אז $f(x)$ פולינום מינימלי של β ואז $F[\alpha] \cong F[\beta]$
גם הכיוון ההפוך נכון:

טענה 0.1 אם K/F כך ש $F[\alpha] \cong K$ אז $K = F[\beta]$ לאיזהו $b \in K$ שהוא שורש של הפולינום המינימלי של α . זה כמובן לא אומר ש $\beta \in F[\alpha]$.

למשל

הפולינום המינימלי של $\sqrt[3]{2}$ מעל \mathbb{Q} : $x^3 - 2$ ולכן
 $\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[\sqrt[3]{2}\rho_3] \cong \mathbb{Q}[\sqrt[3]{2}\rho_3^2]$
 אבל אין שוויון כי שני שורשים מרוכבים ו $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$

תרגיל

כמה תתי שדות שונים יש ל \mathbb{C} שאיזומורפים ל $\mathbb{Q}[\sqrt{2 + \sqrt{5}}]$

פתרון

נמצא פולינום מינימלי של $x = \sqrt{2 + \sqrt{5}}$

$$x^2 = 2 + \sqrt{5}$$

$$x^2 - 2 = \sqrt{5}$$

$$x^4 - 4x^2 + 4 = 5$$

$$x^4 - 4x^2 + 1 = 0$$

השורשים $\pm\sqrt{2 \pm \sqrt{5}}$

$$\mathbb{Q}[-\sqrt{2 + \sqrt{5}}] = \mathbb{Q}[\sqrt{2 + \sqrt{5}}] \cong \mathbb{Q}[\sqrt{2 - \sqrt{5}}] = \mathbb{Q}[-\sqrt{2 - \sqrt{5}}]$$

אי השוויון נובע מכך שאחד מרוכב והשני ממשי.
 לכן יש לנו סה"כ 2 תתי שדות

שדה פיצול

הגדרה 0.2 יהי $f \in F[x]$, שדה E/F מפצל את $f(x)$ אם בפירוק מעל E מתפרק לגורמים ליניארים. כלומר, ב E יש את כל השורשים של $f(x)$.

למשל

1. \mathbb{C} שדה מפצל של כל פולינום מעל \mathbb{Q}

2. $\mathbb{Q}[\sqrt{2}]$ מפצל את $x^2 - 2$

3. $\mathbb{Q}[\sqrt{\Delta}]$ מפצל את $ax^2 + bx^2 + c$ (Δ היא הדיסקרימיננטה).

הגדרה 0.3 שדה הפיצול של פולינום $f(x) \in F[x]$ הוא הרחבה E/F מינימלית המפצל את $f(x)$.

איך בונים אותו? $F[\alpha_1, \dots, \alpha_n]$ כאשר α_i הם השורשים של $f(x)$.

טענה 0.4 שדה הפיצול יחיד עד כדי איזומורפיזם.

דוגמא

נמצא את שדה הפיצול של $f(x) = x^4 - 12$ מעל \mathbb{Q} .
 $f(x) = (x^2 - \sqrt{12})(x^2 + \sqrt{12}) = (x - \sqrt[4]{12})(x + \sqrt[4]{12})(x + \sqrt[4]{12}i)(x - \sqrt[4]{12}i)$
נסמן את שדה הפיצול ב E .
 $E = \mathbb{Q}[\sqrt[4]{12}, -\sqrt[4]{12}, \sqrt[4]{12}i, -\sqrt[4]{12}i] = \mathbb{Q}[\sqrt[4]{12}, \sqrt[4]{12}i] = \mathbb{Q}[\sqrt[4]{12}, i]$

תרגיל

מצא את שדה הפיצול $x^5 - 2$ מעל \mathbb{Q} , מה המימד שלו?

פתרון

השורשים $\sqrt[5]{2}, \sqrt[5]{2}\rho_5, \sqrt[5]{2}\rho_5^2, \dots, \sqrt[5]{2}\rho_5^4$
ולכן שדה הפיצול $E = \mathbb{Q}[\sqrt[5]{2}, \rho_5]$
 $[\mathbb{Q}[\sqrt[5]{2}] : \mathbb{Q}] = 5$
 $[\mathbb{Q}[\sqrt[5]{2}, \rho_5] : \mathbb{Q}[\sqrt[5]{2}]] = 4$
המימדים זרים, לכן לפי תרגיל משיעורי בית 3,
 $[E : \mathbb{Q}] = 5 \cdot 4$

טענה 0.5 יהי $f \in F[x]$ מדרגה n , ויהי E שדה הפיצול של $f(x)$ אזי $[E : F] \leq n!$. לא בהכרח יש שוויון, לדוגמא התרגיל הקודם או אם יש ריבוי אלגברי.

תרגיל

יהי F שדה ממאפיין p . נסתכל על $f(x) = x^p - x - a$ ויהי α שורש של $f(x)$. מצאו את שדה הפיצול ע"י α .

פתרון

נשם לב:

$$f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - a = \alpha^p + 1^p - \alpha - 1 - a = 0$$

באותו אופן:

$$f(\alpha + 2) = (\alpha + 2)^p - (\alpha + 2) - a = (\alpha^p - \alpha - a) + (2^p - 2) = 0$$

אזי $\alpha, \alpha + 1, \dots, \alpha + p - 1$ אלו כל השורשים של $f(x)$ ולכן שדה הפיצול

$$E = F[\alpha]$$

תורת גלואה – תרגול 5

הומומורפיזם של שדות

יש לנו הומו, $\varphi : F \rightarrow L$, ויש הרחבה E/F , אז רוצים להרחיב את φ ל $\psi : E \rightarrow L$

הבחנה 1

אם יש הומו' $\varphi : F \rightarrow L$ אז יש הומו' ברור
 $\hat{\varphi} : F[x] \rightarrow L[x]$ ע"י $x \mapsto x$.
 נסמן $\hat{\varphi}(f(x)) = \hat{f}(x)$

הבחנה 2

אם $\psi : E/F \rightarrow L$ שמרחיבה את φ .
 אם $a \in E$ שורש של פולינום $f(x) \in F[x]$,
 $0 = \psi(f(a)) = \psi(f)(\psi(a)) = \hat{f}(\psi(a))$
 אזי $\psi(a)$ הוא שורש של \hat{f} .
 \Leftarrow שורש של f הולך לשורש של \hat{f} .

הבחנה 3

אם $f(x)$ הוא פריק a שורש של גורם $(g|f)$ $g(x)$ אזי גם a הולך לשורש של \hat{g} .
ולכן איבר a עם פולינום מינימלי f_a אז a הולך לשורש של \hat{f}_a .
 מסתבר שזה מספיק בשביל להגדיר הרחבה:

למה 0.1 יהי $a \in E$ עם פולינום מינימלי $f(x)$ מעל F , אם $b \in L$ שורש של $\hat{f}(x)$ אזי יש הרחבה: $\psi : F[a] \rightarrow L$ כך ש $a \mapsto b$.

הוכחה: נתבונן ב $L \xrightarrow{x \mapsto b} F[a]$

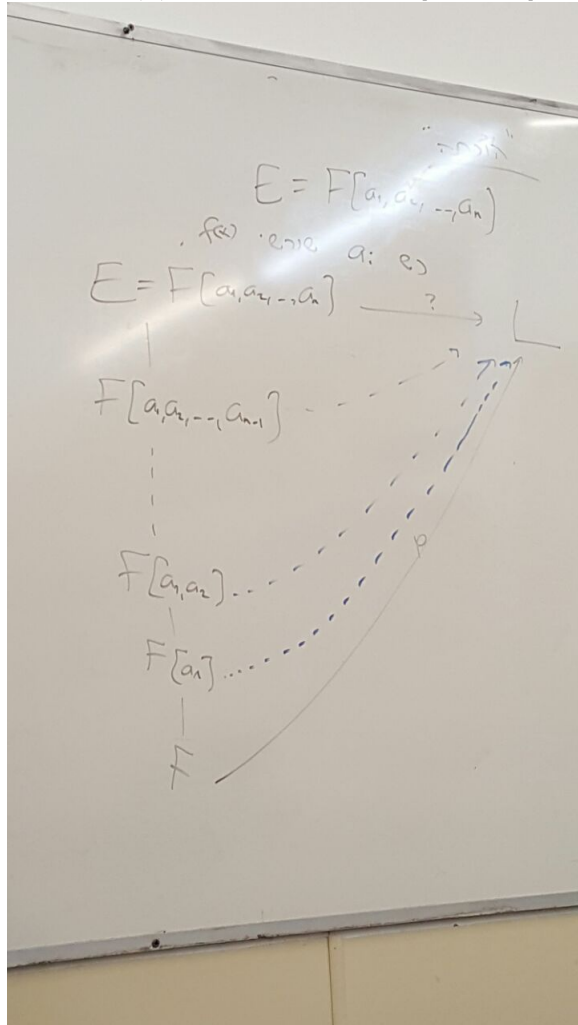
הגרעין הוא $\langle f(x) \rangle$ ולכן לפי משפט האיזומורפיזם הראשון,

$$F[a] \cong F[x]/\langle f(x) \rangle \hookrightarrow L$$

כמה הומומורפיזמים יש מ $F[a] \rightarrow L$?

לפי מספר השורשים השונים של $\hat{f}(x)$ ב L . לכל היותר $[F[a] : F]$ $\deg f =$

משפט 0.2 נתון $\varphi : F \rightarrow L$ ו $f(x) \in F[x]$ כך ש $\hat{f}(x)$ מתפצל מעל L . (בל יש את כל השורשים של \hat{f}), ויהי E שדה פיצול של $f(x)$ מעל F , אזי יש הרחבה $\psi : E \rightarrow L$ הוכחה: $E = F[a_1, \dots, a_n]$ כש a_i שורשי $f(x)$,



שלב 1

נקח את a_1 ואת הפולינום המינימלי של $f_{a_1} | f$ ובחרים שורש $b_1 \in L$ של \hat{f}_{a_1} ואז יש לנו הומומורפיזם (לפי הלמה): $\varphi_1 : F[a_1] \rightarrow L$.

שלב 2

נקח את a_2 , נסתכל בפולינום המינימלי שלו מעל $F[a_1]$: $f_{a_2}(x) \in F[a_1][x]$

ניקח שורש של $b_2 \in L$ של \hat{f}_{a_2} (הכובע מוגדר בעזרת φ_1).
 ונגדיר הומומורפיזם $\varphi_2 : F[a_1][a_2] \rightarrow L$ (לפי הלמה)
 $(a_1 \mapsto b_1, a_2 \mapsto b_2)$

כמה הומומורפיזמים שונים יש?

בשלב הראשון קיבלנו שיש לכל היותר $\deg f_a = [F[a] : F]$, בשלב השני לכל היותר
 $\deg f_{a_2} = [F[a_1, a_2] : F[a_1]]$

לכן סך הכל יש לכל היותר

$$[E : F] = [F[a_1] : F] \cdot [F[a_1, a_2] : F[a_1]] \dots$$

דוגמא

של $E \rightarrow \mathbb{C}$ כש E שדה הפיצול של f .
 $f(x) = (x^2 - 2)(x^2 - 3)$ מעל \mathbb{Q} ונשתמש בהכלה $\mathbb{Q} \hookrightarrow \mathbb{C}$. תרחיבו להומומורפיזם

פתרון

שדה הפיצול הוא $E = \mathbb{Q}[\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}]$

שלב 1 לוקחים את $\sqrt{2}$, הפולינום המינימלי מעל \mathbb{Q} הוא $x^2 - 2$.

$$\hat{\varphi}(x^2 - 2) = x^2 - 2 \text{ ולכן } \sqrt{2} \text{ ללכת ל} \pm\sqrt{2}$$

נבחר $\sqrt{2} \mapsto -\sqrt{2}$

זה מגדיר $\varphi_1 : \mathbb{Q}[\sqrt{2}] \mapsto \mathbb{C}$ ע"י $\sqrt{2} \mapsto -\sqrt{2}$.

שלב 2 השורש $-\sqrt{2}$. הפ"מ של $-\sqrt{2}$ מעל $\mathbb{Q}[\sqrt{2}]$ הוא $x + \sqrt{2}$.

$$\hat{\varphi}_1(x + \sqrt{2}) = x - \sqrt{2}$$

ולכן $-\sqrt{2}$ חייב ללכת ל $\sqrt{2}$ וכך הגדרנו

$$\varphi_2 : \mathbb{Q}[\pm\sqrt{2}] \rightarrow \mathbb{C}$$

שלב 3 השורש $\sqrt{3}$. הפ"מ של $\sqrt{3}$ מעל $\mathbb{Q}[\sqrt{2}, -\sqrt{2}]$ הוא $x^2 - 3$.

$$\hat{\varphi}_2(x^2 - 3) = x^2 - 3 \text{ ולכן } \sqrt{3} \text{ חייב ללכת ל} \pm\sqrt{3}$$

נבחר $\sqrt{3} \mapsto -\sqrt{3}$ וכך נגדיר:

$$\varphi_3 : \mathbb{Q}[\pm\sqrt{2}, \sqrt{3}] \rightarrow \mathbb{C}$$

תורת גלואה – תרגול 6

תזכורת

אם יש $\varphi : F \rightarrow L$ ו E/F שדה פיצול של פולינום $f(x)$ ו f מתפצל מעל L אזי אפשר להרים את φ ל L $\psi : E \rightarrow L$.
אנחנו מתעניינים בהרמות של F -הומומורפיזם

הגדרה 0.1 $\varphi : E \rightarrow E$ היא F -הומומורפיזם אם לכל $a \in F$ $\varphi(a) = a$. F -הומומורפיזם היא גם העתקה ליניארית. זה גם נותן שאם E/F סופית אז F -הומומורפיזם היא אוטומורפיזם.

הגדרה 0.2 תהי E/F (בד"כ סופי) חבורת גלואה של ההרחבה היא:
$$\text{Gal}(E/F) = \{\varphi : E \rightarrow E, F\text{-homo}\} \leq \text{Aut}(G)$$

הגדרה 0.3 פולינום אי פריק נקרא ספרבילי אם אין לו שורשים כפולים (בסגור האלגברי).

דוגמא לפולינום לא ספרבילי

$\text{char} F = p > 0$ ו $a \in F$ שאין לו שורש p , אזי $f(x) = x^p - a$ הוא אי פריק. אבל אם בשדה פיצול $\alpha \in E$ הוא שורש אזי ב E ,
$$x^p - a = x^p - \alpha^p = (x - \alpha)^p$$

כלומר כל השורשים הם α לא ספרבילי.

קריטריון

פולינום $f(x)$ ספרבילי אם ורק אם $\gcd(f, f') = 1$
למשל $f(x) = x^4 - 8x^2 + 16$ מעל \mathbb{Q}
 $f'(x) = 4x^3 - 16x = 4x(x^2 - 4)$, $x^2 - 4$ גורם משותף ל $f(x), f'(x)$ ולכן $f(x)$ לא ספרבילי.

ניסוח אחר

אם f א"פ אז הוא ספרבילי אם ורק אם $f' \neq 0$.

• במאפיין 0 כל הפולינומים האי פריקים ספרבילים.

• כל אי פריק הוא ספרבילי רק אם $\text{char} F = p$ ובכל החזקות יש גורם p .

הגדרה 0.4 הרחבה E/F מקראת ספרבילית אם לכל $\alpha \in E$ הפולינום המינימלי של α מעל F הוא ספרבילי.

דוגמא להרחבה לא ספרבילית

$\text{char} F = p$, למשל $F(y)/F$ כי שם $x^p - y$ לא ספרבילי.

טענה 0.5 $E/K/F$, אם E/F ספרבילי אז $E/K, K/F$ ספרבילי.

הוכחה: K/F ספרבילי מיידית. ניקח $a \in E$ אזי $f_{a,F}$ (פ"מ מעל F) ספרבילי, אזי $f_{a,K} | f_{a,F}$ \Leftrightarrow ל $f_{a,K}$ אין שורשים כפולים. ■

טענה 0.6 אם E/F שדה פיצול של פולינום ספרבילי אז $[E : F] = |Gal(E/F)|$.

תרגיל: חשבו את $Gal(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$

פתרון

$E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ זה שדה פיצול $f(x) = (x^2 - 2)(x^2 - 3)$, אין לו שורשים כפולים ולכן $|Gal(E/F)| = [E : F] = 4$

$\sqrt{2}$ חייב ללכת לשורשים של הפולינום המינימלי $x^2 - 2$ ולכן ל $\pm\sqrt{2}$.
לאן אפשר לשלוח את $\sqrt{3}$?

מסתבר שזה לא תלוי בלאן נשלח את $\sqrt{2}$. למה?

• הפ"מ של $\sqrt{3}$ מעל $\mathbb{Q}[\sqrt{2}]$ הוא עדיין $x^2 - 3$

• $|Gal| = 4$ ולכן חייב להיות של $\sqrt{3}$ יש 2 פתרונות

ולכן $\sqrt{3}$ הולך ל $\pm\sqrt{3}$ בלי תלות ב $\sqrt{2}$.

נמספר את השורשים: $1 = \sqrt{2}, 2 = -\sqrt{2}, 3 = \sqrt{3}, 4 = -\sqrt{3}$

אוטומורפיזם.	יוצרים	תמורה על השורשים.
Id	$\sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$	Id
σ_1	$\sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$	(12)
σ_2	$\sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$	(3,4)
$\sigma_1\sigma_2 = \sigma_2\sigma_1$	$\sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$	(12)(34)

אז $Gal(E/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \langle (12), (34) \rangle \leq S_4$

תרגיל

חשבו את $Gal(E/F)$ כש E שדה פיצול של הפולינום $f(x) = x^4 - 2$

פתרון

השורשים של f הם $1 := \alpha = \sqrt[4]{2}, 2 := -\alpha, 3 := \alpha i, 4 := -\alpha i$.
 $E = \mathbb{Q}[\alpha, i]$ (דורש בדיקה). α חייב ללכת לאחד מהשורשים, i חייב ללכת ל $\pm i$ (שורשים של $x^2 + 1$) (גם פה α ו i הם לא תלויים זה בזה, למשל פולינום מינימלי של i מעל $\mathbb{Q}[\alpha]$ הוא עדיין $x^2 + 1$)

אוטומורפיזם.	יוצרים	תמורה על השורשים.
Id	$\alpha \mapsto \alpha, i \mapsto i$	Id
τ	$\alpha \mapsto -\alpha, i \mapsto -i$	(34)
σ	$i \mapsto i, \alpha \mapsto \alpha i$	(1234)
σ^2		(12)(34)
σ^3		(1432)
$\tau\sigma$		(14)(23)
$\sigma\tau$		

סך הכל:

$Gal(E/\mathbb{Q}) \cong D_4 \cong \langle (34), (1234) \rangle \leq S_4$

תורת גלואה – תרגול 7

0.1 הגדרה E/F הרחבה נורמלית אם לכל $a \in E$ הפ"מ של a מעל F מתפצל ממעל E .

אם E/F הרחבה סופית אז אפשר לבנות $E'/E/F$ נורמלית:

$$E = F[\alpha_1, \dots, \alpha_n]$$

$$F[x] \ni f_i \alpha_i$$

ונקח את E' להיות שדה פיצול של $\prod f_i(x)$

דוגמא להרחבה לא נורמלית וספרבילית

$$\mathbb{Q}[\sqrt[3]{2}] \text{ כי אין את כל השורשים של } x^3 - 2$$

דוגמא להרחבה נורמלית ולא ספרבילית

0.2 טענה $F_p(y)/F_p(y^p)$ הוא השורש (היחיד) של $x^p - y^p$ ובמודולו p שווה ל $(x - y)^p$ התנאים הבאים שקולים עבור הרחבה E/F :

1. E/F ספרבילית ונורמלית

2. E/F שדה פיצול של פולינום ספרבילי

3. $E^{\text{Gal}(E/F)} = F$

4. $E^K = F$ לאיזושהי ת"ח סופית $K \leq \text{Aut}(E)$

5. $|\text{Gal}(E/F)| = [E : F]$

הרחבה כזו נקראת **הרחבת גלואה**.

יותר מזה

עבור $a \in E$ הפ"מ של a הוא

$$f(x) = \prod_{\{\sigma(a), \forall \sigma \in \text{Gal}(E/F)\}} (x - \sigma(a))$$

תרגיל

מצאו את הפ"מ של $\alpha = \sqrt{2} - 3\sqrt{3} + 2\sqrt{6}$ מעל \mathbb{Q}

פתרון

נשם לב ש $\alpha \in \mathbb{Q}[\sqrt{2}, \sqrt{3}] = E$
ראינו פעם שעברה ש $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
נחשב:

$$\text{Id}(\alpha) = \alpha$$

$$\sigma_1(\alpha) = -\sqrt{2} - 3\sqrt{3} - 2\sqrt{6}$$

$$\sigma_2(\alpha) = \sqrt{2} + 3\sqrt{3} - 2\sqrt{6}$$

$$\sigma_1\sigma_2(\alpha) = -\sqrt{2} + 3\sqrt{3} + 2\sqrt{6}$$

(אלו איברים שונים כי $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ הוא בסיס של E/\mathbb{Q} ולכן:

$$f_\alpha(x) = (x - \alpha)(x - \sigma_1(\alpha))(x - \sigma_2(\alpha))(x - \sigma_1\sigma_2(\alpha))$$

$$[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$$

תרגיל ממבחן

נניח $E = \mathbb{Q}[\alpha]/\mathbb{Q}$ הרחבת גלואה ונניח $\sigma(\alpha) = \alpha^2$ לאיזהו $\sigma \in \text{Gal}(E/\mathbb{Q})$.

1. האם ייתכן ש $[E : \mathbb{Q}] = 2$?

2. האם ייתכן ש $[E : \mathbb{Q}] = 3$?

פתרון

1. נניח שכן, אז $|G| = 2$ ו- σ מסדר 2.

$$\alpha = \sigma^2(\alpha) = \sigma(\alpha^2) = \alpha^4$$

$$\alpha = \alpha^4 \Rightarrow \alpha^3 = 1 \Rightarrow \alpha = \rho_3$$

$$[\mathbb{Q}[\rho_3] : \mathbb{Q}] = 2 \text{ ואכן}$$

2. נניח שכן $|G| = 3$ אז הסדר של σ הוא 3.

$$\alpha = \sigma^3(\alpha) = \alpha^8 \Rightarrow \alpha^7 = 1 \Rightarrow \alpha = \rho_7$$

אבל אז $[\mathbb{Q}[\rho_7] : \mathbb{Q}] = 6$ בסתירה לכך שהגודל הוא 3

התאמת גלואה

E/F גלואה, $G = \text{Gal}(E/F)$ אז יש התאמה חח"ע בין קבוצת שדות הביניים של E/F לת"ח של G ע"י $H \mapsto E^H$ ו- $L \mapsto \text{Gal}(E/F)$

עם תכונות

$$1. E^{H_1} = E^{H_2} \Leftrightarrow H_1 = H_2 \text{ (חח"ע)}$$

$$2. |H| = [E : E^H]$$

$$3. L^{H_2} \subseteq L^{H_1} \Leftrightarrow H_1 \subseteq H_2$$

$$4. \text{Gal}(E^H/F) \cong G/H \text{ ואז } E^H/F \Leftrightarrow H \triangleleft G$$

תרגיל ממבחן

- מצא את חבורת גלואה של שדה פיצול של $x^3 - 7$ מעל \mathbb{Q}
- מצא את כל שדות הביניים.

פתרון

השורשים $\sqrt[3]{7}, \sqrt[3]{7}\rho_3, \sqrt[3]{7}\rho_3^2$ ושדה הפיצול הוא $E = \mathbb{Q}[\sqrt[3]{7}, \rho_3]$
 הגודל של חבורת גלואה $[E : \mathbb{Q}] = 6$

נזהה:

$$(123) \sigma(\sqrt[3]{7}) = \sqrt[3]{7}\rho_3$$

$$(23) \tau(\rho_3) = \rho_3^2 = \bar{\rho}_3$$

$$\tau\sigma\tau = \sigma^{-1} \text{ ואפשר לראות}$$

ולכן $G \cong D_3$

ת"ח	שדות ביניים
$\langle \sigma \rangle$	$E^{\langle \sigma \rangle} = \mathbb{Q}[\rho_3]$
$\langle \tau \rangle$	$E^{\langle \tau \rangle} = \mathbb{Q}[\sqrt[3]{7}]$
$\langle \tau\sigma \rangle$	$\mathbb{Q}[\sqrt[3]{7}\rho_3]$
$\langle \tau\sigma^2 \rangle$	$\mathbb{Q}[\sqrt[3]{7}\rho_3^2]$
$\{Id\}$	$E^{\{id\}} = E$
D_3	$E^{D_3} = \mathbb{Q}$

הסברים

קל לראות ש:

$$E^{\langle \tau \rangle} = \mathbb{Q}[\sqrt[3]{7}] \text{ כי } \sqrt[3]{7} \in E^{\langle \tau \rangle} \text{ והמימד הוא } 3.$$

$$E^{\langle \sigma \rangle} = \mathbb{Q}[\rho_3] \text{ כי } \sigma(\rho_3) = \rho_3 \text{ והמימד הוא } 2.$$

$$\tau\sigma = (23)(123) = (13) \text{ ורואים ששומר על השורש השני, כלומר } \sqrt[3]{7}\rho_3 \text{ ולכן}$$

$$E^{\langle \tau\sigma \rangle} \subseteq \mathbb{Q}[\sqrt[3]{7}\rho_3] \text{ והמימדים שווים ולכן שווים.}$$

$$\tau\sigma^2 = (12) \text{ שומר על } \sqrt[3]{7}\rho_3^2$$

תורת גלואה - תרגול 8

תרגיל

מצא את חבורת גלואה ואת שדות הביניים של ההרחבה $E = \mathbb{Q}[\sqrt[4]{2}, i]/\mathbb{Q}$

פתרון

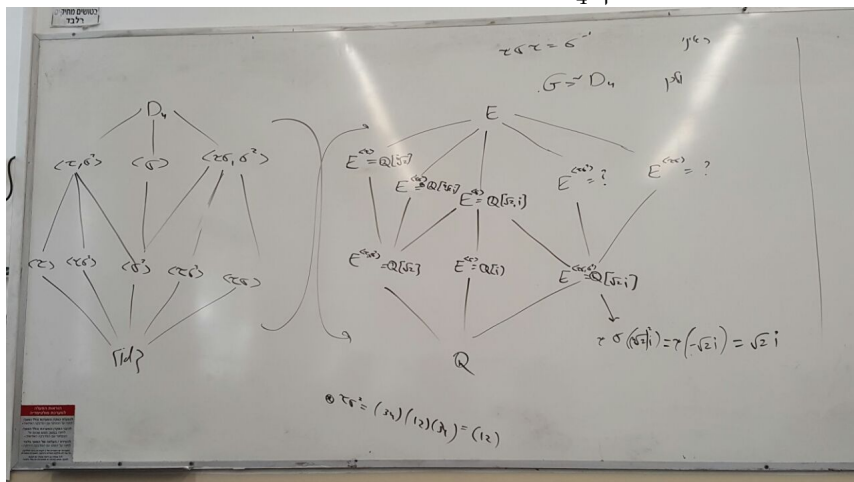
E זה שדה פיצול של $x^4 - 2$, שהוא ספרבילי ולכן E/\mathbb{Q} גלואה.

$[E : \mathbb{Q}] = 8$ ולכן $G = \text{Gal}(E/\mathbb{Q})$ מגודל 8.

השורשים של f הם $1 := \alpha, 2 := -\alpha, 3 := \alpha i, 4 := -\alpha i$.
 $E = \mathbb{Q}[\alpha, i]$ (דורש בדיקה). α חייב ללכת לאחד מהשורשים, i חייב ללכת ל $\pm i$ (שורשים של $x^2 + 1$) גם פה α ו i הם לא תלויים זה בזה, למשל פולינום מינימלי של i מעל $\mathbb{Q}[\alpha]$ הוא עדיין $x^2 + 1$

אוטומורפיזם.	יוצרים	תמורה על השורשים.
Id	$\alpha \mapsto \alpha, i \mapsto i$	Id
(34)	$\alpha \mapsto \alpha, i \mapsto -i$	τ
(1234)	$i \mapsto i, \alpha \mapsto \alpha i$	σ

ראינו $G \cong D_4$ ולכן $\tau\sigma\tau = \sigma^{-1}$



חישוב של $E^{\langle \tau \sigma^3 \rangle}$

נחשב תמונה של איבר כללי ב E .

$$\tau \sigma^3 (a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{2}^3 + ei + f\sqrt[4]{2}i + g\sqrt{2}i + h\sqrt[4]{2}^3 i) =$$

$$= a + b\sqrt[4]{2}i - c\sqrt{2} - d\sqrt[4]{2}^3 i - ei + f\sqrt[4]{2} + g\sqrt{2}i - h\sqrt[4]{2}^3$$

ע"י השוואת מקדמים:

$$c = e = 0, b = f, d = -h$$

למשל ניקח $b = 1$ ו $d = 0$ כלומר

$$\sqrt[4]{2} + i\sqrt[4]{2} = (1 + i)\sqrt[4]{2}$$

אזי

$$\mathbb{Q}[(1 + i)\sqrt[4]{2}] \subseteq E^{\langle \tau \sigma^3 \rangle}$$

והמימד שווה ולכן יש שוויון.

חישוב של $E^{\langle \tau \sigma \rangle}$

נחשב מסלול של $\tau \sigma$

$$\sqrt[4]{2} \xrightarrow{\tau \sigma} -\sqrt[4]{2}i \xrightarrow{\tau \sigma} \sqrt[4]{2}$$

$$\sqrt[4]{2} - \sqrt[4]{2}i = (1 - i)\sqrt[4]{2}$$

$$\mathbb{Q}[(1 - i)\sqrt[4]{2}] = E^{\langle \tau \sigma \rangle}$$

בזכות המימד/כי צמוד לקודם/כי זה לא אף שדה אחר.

תרגיל (ממבחן)

מצאו הרחבה של \mathbb{Q} עם חבורת גלואה איזו ל $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

פתרון

ניקח $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ הרחבת גלואה כי זה שדה פיצול של $(x^2 - 2)(x^2 - 3)(x^2 - 5)$ שספרבילי. $|\text{Gal}(E/\mathbb{Q})| = 8$ ולכן $8[E : \mathbb{Q}] =$ נראה שכל האיברים הם מסדר 2. יהי $\sigma \in \text{Gal}(E/\mathbb{Q})$.
 $\sigma(\sqrt{2}) = \pm\sqrt{2}$
 $\sigma(\sqrt{3}) = \pm\sqrt{3}$
 $\sigma(\sqrt{5}) = \pm\sqrt{5}$
מכיוון שאלו יוצרים בסיס של E , σ מסדר לכל היותר 2.

טענה 0.1 תהי E/F הרחבת גלואה, שדה פיצול של פולינום ספרבילי מדרגה n . אזי, יש שיכון טבעי (של חבורות)

$$\text{Gal}(E/F) \hookrightarrow S_n$$

ע"י הפעולה על השורשים של f

תרגיל

יהי p מספר ראשוני ויהי $f(x) \in \mathbb{Q}[x]$ פולינום אי פריק מדרגה p . נניח של f יש $p - 2$ שורשים ממשיים 21 מרוכבים, ויהי E שדה פיצול של $f(x)$ מעל \mathbb{Q} . הוכיחו כי $\text{Gal}(E/\mathbb{Q}) \cong S_p$

פתרון

יש שורשים מרוכבים ולכן אוטו' ההצמדה (של המרוכבים) הוא איבר ב G . הוא פועל על השורשים בתור חילוף כי יש בדיוק 2 שורשים מרוכבים (ובהכרח צמודים). מצד שני, $p = \deg f \mid |G| = [E : \mathbb{Q}]$. לפי קושי יש ב G איבר מסדר p ולכן יש מחזור מאורך p ב G . לכן, לפי תורת החבורות, החילוף והמחזור יוצרים את S_p ואז $G \cong S_p$

תורת גלואה – תרגול 9

שדות סופיים

תזכורות

1. יהי F שדה סופי ממאפיין p , יש שיכון של $F \hookrightarrow \mathbb{Z}_p$.
2. F מ"ו מעל \mathbb{Z}_p ולכן מגודל p^n .
3. ב F^* לגרנז' $x^{p^n} = x$, $x^{p^n} - x = 0$, ולכן F שדה פיצול של $x^{p^n} - x$.

תוצאות

- קיום של שדות מכל גודל p^n .
- יחידות: קיים שדה יחיד כזה ונסמנו \mathbb{F}_n .
- $\mathbb{F}_{p^n}/\mathbb{F}_p$ היא גלואה, $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma \rangle \cong \mathbb{Z}_n$ כאשר $\sigma(x) = x^p$ אוטו' פרוביניוס.

תרגיל

חשבו את היוצר של חבורות גלואה של שדה פיצול של $x^3 - 2$ מעל:

1. \mathbb{F}_3

2. \mathbb{F}_5

3. \mathbb{F}_7

פתרון

1. מעל \mathbb{F}_3 , $x^3 - 2 = (x - 2)^3$, ולכן שדה פיצול הוא \mathbb{F}_3 ולכן חבורת גלואה טריוויאלית.

2. יש שורש 3 ולכן אפשר לפרק:

$$x^3 - 2 = (x - 3)(x^2 + 3x + 1)$$

ו $x^2 + 3x + 1$ אי פריק כי אין שורשים ולכן שדה פיצול הוא הרחבה ממימד 2,

$$\mathbb{F}_5(\alpha) \cong \mathbb{F}_{25}$$

כאשר α שורש של $x^2 + 3x + 1$ ואז

$$\text{Gal}(\mathbb{F}_{25}/\mathbb{F}_5) \cong \mathbb{Z}_2$$

איברים בשדה פיצול נראים מהצורה $a + b\alpha$

$$\sigma(a + b\alpha) = a + b\alpha^5 = a + b\alpha(-3\alpha - 1)(-3\alpha - 1) = a + b\alpha(4\alpha^2 + \alpha + 1) = \dots = a - 2 + 3b\alpha$$

3. אין לפולינום שורש ב \mathbb{F}_7 ולכן הוא אי פריק, ולכן שדה פיצול הוא הרחבה ממימד

$$3, \mathbb{F}_7(\alpha) = \mathbb{F}_{7^3} \text{ כאשר } \alpha \text{ שורש של } x^3 - 2.$$

$$\text{Gal}(\mathbb{F}_{7^3}/\mathbb{F}_7) = \langle \sigma \rangle \cong \mathbb{Z}_3$$

איבר כללי הרחבה $a + b\alpha + c\alpha^2$,

$$\sigma(a + b\alpha + c\alpha^2) = a + b\alpha^7 + c\alpha^{14} = \dots = 1 + 4b\alpha + 2c\alpha^2$$

הגדרה 0.1 יהיו $F \subseteq K, L \subseteq E$ **הקומפוזיטום** KL הוא השדה המינימלי שמכיל את

$$K, L \text{ אם } L = F[\alpha_1, \dots, \alpha_n] \text{ אזי } KL = K[\alpha_1, \dots, \alpha_n]$$

טענה 0.2 אם L/F שדה פיצול של פולינום $f(x)$ אזי LK/K ש"פ של אותו פולינום.

תרגיל

יהיו $L, K \subseteq F$ הרחבות סופיות ונתון ש K/F הוא גלואה. הוכיחו כי:

1. $K/L \cap K$ גלואה

2. LK/L גלואה

3. $\text{Gal}(LK/L) \cong \text{Gal}(K/L \cap K)$

הוכחה

1. K/F גלואה $\Leftarrow K/L \cap K$ גלואה (מיידית).

2. LK/L גלואה מהטענה הקודמת (בחילוף תפקידים).

3. נבנה

$$\varphi : \text{Gal}(LK/K) \rightarrow \text{Gal}(L/L \cap K)$$

ע"י

$$\sigma \mapsto \sigma|_K$$

נוכיח שזו איזומורפיזם

מוגדר היטב: $\sigma(K) = K$ כי K/F גלואה ולכן הוא שדה פיצול של פולינום, $K = F[\alpha_1, \dots, \alpha_n]$ כאשר α_i שורשים של פולינום ספרבילי. σ שומר על F ועושה פרמוטציה על השורשים של פולינום מעל F :

$$\sigma(\{\alpha_1, \dots, \alpha_n\}) = \{\alpha_1, \dots, \alpha_n\}$$

אזי $\sigma(K) = K$

בנוסף, σ שומר על L ולכן $\sigma|_K$ שומר על $L \cap K$ וסך הכל $\sigma_k \in \text{Gal}(K/L \cap K)$

הומומורפיזם: צמצום ולכן טריוויאלי

חח"ע: נניח $\sigma|_K = \text{Id}_K$ ($\sigma = \text{Id}_{KL}$ צ"ל)

σ שומרת על K (כי $\sigma|_K$ זה הזהות)

σ שומרת על L (כי איבר מגלואה)

ולכן בהכרח שומר על $KL \Leftarrow \sigma = \text{Id}_{LK}$

על: צ"ל: $\text{Im} \varphi = \text{Gal}(K/L \cap K)$. נראה $K^{\text{Im} \varphi} = L \cap K = L^{\text{Gal}(K/L \cap K)}$

(\supseteq) ברור

(\subseteq) כלומר $a \in K$ ו $a \in K^{\text{Im} \varphi}$ לכל $\sigma|_K \in \text{Im} \varphi$ לכל $\sigma|_K(a) = a$

זה אומר ש $\sigma(a) = a$ לכל $\sigma \in \text{Gal}(LK/L)$ ולכן $a \in L$ ולכן $a \in L \cap K$ ולכן

סיימנו לפי התאמת גלואה.

$$[KL : F] = \frac{[K:F][L:F]}{[K \cap L:F]} \quad \mathbf{0.3 \text{ מסקנה}}$$

תורת גלואה – תרגול 10

שדות סופיים – המשך

חזרה

F שדה מגודל p^n . שדה פיצול של $x^{p^n} - x$ ב F_p^n/F_p , $[F_p^n : F_p] = n$.

$$\text{Gal}(F_p^n/F_p) = \langle \sigma \rangle \cong \mathbb{Z}_n$$

E/F הרחבה סופית של שדות סופיים (במאפיין p). היא גם גלואה והחבורה נוצרת ע"י חזקה של פרוביניוס.

0.1 מסקנה אם $f(x) \in F_p[x]$ א"פ מדרגה n ו α שורש שלו באיזושהי הרחבה אזי כל השורשים של $f(x)$ הם $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{n-1}}$ ני השורשים של פולינום מינימלי של α הם המסלול של α תחת חבורת גלואה $\{\sigma(\alpha) | \sigma \in \text{Gal}\}$. אזי $F_p[\alpha]/F_p$ היא נורמלית.

תרגיל (ממבחן)

יהי F שדה מגודל 5^3 ויהי $\alpha \in F$ כך ש $F = F_5[\alpha]$. רשום את כל שאר השורשים של הפ"מ של α מעל F_5 .

פתרון

$\alpha, \alpha^5, \alpha^{5^2}$ (המסלול של α תחת פרוביניוס).

דוגמא

שדה מגודל 2^3 $F = \mathbb{Z}_2[y]/\langle y^3 + y^2 + 1 \rangle$

$$\bar{y} = y + \langle y^3 + y^2 + 1 \rangle$$

הוא שורש של $x^3 + x^2 + 1$. שאר השורשים הם:

$$\bar{y}, \bar{y}^2, \bar{y}^{2^2} = \dots = \bar{y}^2 + \bar{y} + 1$$

פולינומים אי פריקים מעל שדה סופי F_p

משפט 0.2 כל $f(x) \in F_p[x]$ פולינום אי פריק מדרגה n מחלק את $x^{p^n} - x$.

מסקנה 0.3 $x^{p^n} - x$ מתפרק לכל הפולינומים האי פריקים מעל F_p מדרגה המחלקת את n .

הוכחת המשפט

הי $f(x)$ פולינום כזה. נתבונן בשדה $F = F_p[x]/\langle f(x) \rangle$ שדה מגודל p^n . כל האיברים בשדה זה מקיימים $t^{p^n} - t = 0$. זה אומר

$$t^{p^n} - t \equiv 0 \pmod{\langle f(x) \rangle}$$

$$t^{p^n} - t \in \langle f(x) \rangle$$

$$f(x) \mid t^{p^n} - t$$

מסקנה 0.4 מעל F_p , כל פולינום אי פריק הוא ספרבילי.

הערה 0.5 הטענה עוזרת למצוא את כל הפולינום האי פריקים בצורה רקורסיבית.

תרגיל (נפוץ במבחנים!)

כמה פולינומים אי פריקים מדרגה 4 יש מעל F_2 ?

פתרון

הפולינומים הא"פ מדרגה מחלקים את

$$x^{2^4} - x = x^{16} - x$$

וזוהי מכפלת הפולינומים האי פריקים מדרגה 1 כפול מכפלת הפולינומים האי פריקים מדרגה 2 כפול מכפלת הפולינומים האי פריקים מדרגה 4. פולינומים אי פריקים מדרגה 1: מחלקים את $x^2 - x = x(x - 1)$. לכן, יש שני פולינומים אי פריקים מדרגה 1. פולינומים אי פריקים מדרגה 2: מחלקים את $x^2 - x = x^4 - x = x(x - 1)(x^2 + x + 1)$ ולכן $x^2 + x + 1$ הוא הפולינום האי פריק היחיד מדרגה 2. פולינומים אי פריקים מדרגה 4: כמו מקודם, מחלקים את $x^{16} - x = x(x - 1)(x^2 + x + 1)g$ כאשר g מכפלת הפולינומים האי פריקים מדרגה 4. בהכרח מדרגה 12, ולכן יש 3 פולינומים מדרגה 4. לכן סך הכל יש שלושה פולינומים אי פריקים מדרגה 4.

הבחנה

יהי F_{p^n} שדה סופי, $\text{Gal}(F_{p^n}/F_p) = \langle \sigma \rangle \cong \mathbb{Z}_n$. איך נראים תתי שדות של F_{p^n} ? לפי התאמת גלואה כל תת שדה מתאים לת"ח. תתי החבורות האמיתיות של \mathbb{Z}_n הם $m\mathbb{Z}_n$ כאשר $m|n$. בהתאם לאיזומורפיזם, הת"ח של $\langle \sigma \rangle$ הם $\langle \sigma^m \rangle$ לכל $m|n$. תת השדה המתאים:

$$[F_{p^n}^{\langle \sigma^m \rangle} : F_p] = [\langle \sigma \rangle : \langle \sigma^m \rangle] = m$$

$$F_{p^n}^{\langle \sigma^m \rangle} = F_{p^m} \text{ ולכן}$$

0.6 מסקנה תתי השדות של F_{p^n} הם כולם מהצורה F_{p^m} עבור $m|n$.

עד כאן לשדות סופיים

משפט האיבר הפרימיטיבי

אם E/F סופית (ממימד סופית) ספרבילית אזי יש $\alpha \in E$ כך ש $E = F[\alpha]$ הוכחה: (בערך)

עבור שדות סופיים, E^x היא צקלית ונוצרת ע"י איזשהו α ואז ברור ש $E = F[\alpha]$ ■
עבור שדות אינסופיים, נבין ע"י הדוגמא הבאה:

דוגמא

מצא איבר פרימיטיבי ל $\mathbb{Q}[\sqrt{3}, \sqrt{5}]$.

פתרון

מנחשים $\alpha = \sqrt{3} + c\sqrt{5}$ כאשר $c \in \mathbb{Q}$.

(בהוכחת המשפט מראשים שזה יוצר כמעט לכל c , כלומר חוץ ממספר סופי).

ניקח $\alpha = \sqrt{3} + \sqrt{5}$. נסתכל בחזקות:

$$\alpha^0 = 1, \alpha = \sqrt{3} + \sqrt{5}, \alpha^2 = 8 + 2\sqrt{3}\sqrt{5}, \alpha^3 = (*) + (*)\sqrt{3} + (*)\sqrt{5} + (*)\sqrt{3}\sqrt{5}^1$$

¹איך בודקים? זורקים על סטודנט שנה א שיעשה את זה.

תורת גלואה – תרגול 11

הפולינום הציקלוטומי

הפולינום הציקלוטומי Φ_n הוא הפולינום המינימלי של ρ_n (שורש היחידה ה- n פרמיטיבי) מעל \mathbb{Q} .

(אם p ראשוני אז אנחנו כבר יודעים $\Phi_p = x^{p-1} + x^{p-2} + \dots + x + 1$)
 ρ_n הוא שורש של $x^n - 1$ ולכן $\Phi_n | x^n - 1$.
מצד שני, כל שורש של $x^n - 1$ הוא שורש יחידה ולכן $x^n - 1$ ולכן

טענה 0.1

$$x^n - 1 = \prod_{d|n} \Phi_d$$

ודרגתו

$$\deg \Phi_d = \varphi(d)$$

פונקצית אוילר. וכן,

$$\text{Gal}(\mathbb{Q}[\rho_n]/\mathbb{Q}) = \left\{ \rho_n \mapsto \rho_n^k \mid (k, n) = 1 \right\} \cong u_n$$

תזכורת

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right)$$

כאשר p_i הם הגורמים הראשונים השונים של n .

הערה 0.2 המרצה אוהב לתת שאלות בנושא בניות של שדות סופיים וחישוב פולינום ציקלוטומי.

תרגיל

חשבו את Φ_{15}

פתרון

Φ_{15} גורם של $x^{15} - 1$

$$x^{15} - 1 = \Phi_{15}\Phi_5\Phi_3\Phi_1$$

נמצא "באנדוקציה" (נשכח לרגע שאנחנו יוצאים כל אחד מהם כי 3 ו 5 ראשוניים, על מנת שנוכל לתת אלגוריתם כללי שנכון גם כשיש גורמים לא ראשוניים)

$$\Phi_1 = x - 1$$

כעת נמצא את Φ_3 .

$$x^3 - 1 = \Phi_1\Phi_3$$

לכן

$$\Phi_3 = \frac{x^3 - 1}{\Phi_1} = x^2 + x + 1$$

$$x^5 - 1 = \Phi_5\Phi_1$$

לכן =

$$\Phi_5 = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_{15} = \frac{x^{15} - 1}{\Phi_1\Phi_3\Phi_5} = \frac{x^{15} - 1}{(x^5 - 1)\Phi_3} = \frac{x^{10} + x^5 + 1}{\Phi_3} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

בדיקה:

$$\varphi(15) = 8$$

למה 0.3 $\sigma \in \text{Gal}(\mathbb{Q}[\rho_n]/\mathbb{Q})$ אזי יש מספר שלם k שזר ל n כך ש $\sigma(x) = x^k$ לכל x שהוא שורש יחידה.

הוכחה: נבחר שורש יחידה פרימיטיבי, אזי כל שורשי היחידה הם ρ_n^i כאשר $1 \leq i \leq n$. ρ_n פרימיטיבי, כלומר $\rho_n^n = 1$ ו $\rho_n^j \neq 1$ לכל $j < n$. ניקח $\sigma \in G$, נפעיל אותו ונקבל

$$\text{לכן } \sigma(\rho_n) \text{ היא גם שורש פרימיטיבי.} \quad \begin{cases} \sigma(\rho_n^n) = \sigma(\rho_n)^n = \sigma(1) = 1 \\ \sigma(\rho_n^j) = \sigma(\rho_n)^j = \sigma(1) = 1 \end{cases}$$

לפי טענה מחבורות,

$$\sigma(\rho_n) = \rho_n^k$$

$$(k, n) = 1$$

אזי אם x שורש יחידה $x = \rho_n^i$, $1 \leq i \leq n$

$$\sigma(x) = \sigma(\rho_n^i) = \sigma(\rho_n)^i = (\rho_n^k)^i = x^k$$

■

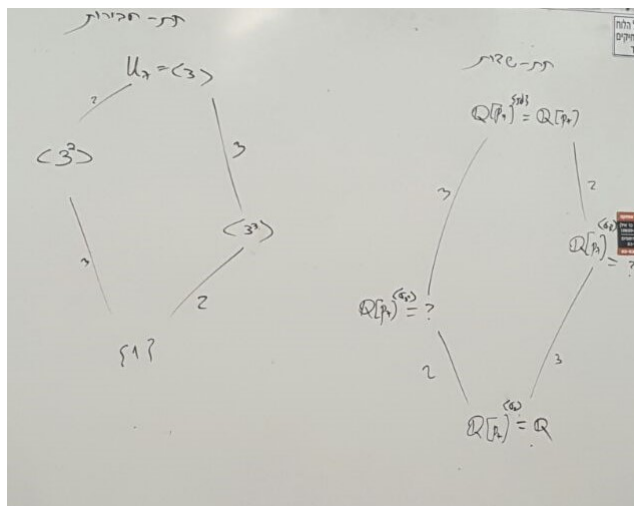
תרגיל (ממבחן)

חשבו את חבורת גלואה ואת שדות הביניים של $\mathbb{Q}[\rho_7]/\mathbb{Q}$.

פתרון

הפ"מ של ρ_7 הוא $x^6 + \dots + x + 1$, ולכן $G = \text{Gal}(\rho_7)$ היא מסדר 6. לפי התאוריה,

$$G = \{ \sigma_k : \rho_7 \mapsto \rho_7^k \mid (k, 7) = 1 \} = \langle \sigma_3 \rangle \cong u_3 = \langle 3 \rangle$$



כעת נותר לחשב:
 $\underline{\mathbb{Q}[\rho_7]^{<\sigma_{3^2}>}} = ?$

$$\rho_7 \xrightarrow[\sigma_{3^2}]{} \rho_7^2 \xrightarrow[\sigma_{3^2}]{} \rho_6^4 \xrightarrow[\sigma_{3^2}]{} \rho_7$$

ולכן

$$\mathbb{Q}[\rho_7 + \rho_7^2 + \rho_7^4] \subseteq \mathbb{Q}[\rho_6]^{<\sigma_{3^2}>}$$

ומטעמי מימד יש שוויון.

$\underline{\mathbb{Q}[\rho_7]^{<\sigma_{3^3}>}} = ?$

$$\rho_7 \xrightarrow[\sigma_{3^3}]{} \rho_7^6 \xrightarrow[\sigma_{3^3}]{} \rho_7$$

ולכן

$$\mathbb{Q}[\rho_7 + \rho_7^6] \subseteq \mathbb{Q}[\rho_7]^{<\sigma_{3^3}>}$$

ומשיקולי מימד יש שוויון.

טענה 0.4 אם E/\mathbb{Q} סופית, שלא מכילה שדות ביניים שהם הרחבות אבליות (כלומר, הרחבות שחבורת גלואה שלהם אבלית) אזי

$$\text{Gal}(E[\rho_n]/E) \cong u_n$$

לפי טענה מפעם,

$$\text{Gal}(E[\rho_n]/E) \cong \text{Gal}(\mathbb{Q}[\rho_n]/E \cap \mathbb{Q}[\rho_n])$$

נטען ש $E \cap \mathbb{Q}[\rho_n] = \mathbb{Q}$. אחרת, זהו תת שדה של E/\mathbb{Q} שהיא הרחבה **אבלית**, כי היא שדה ביניים של $\mathbb{Q}[\rho_n]/\mathbb{Q}$ שהיא אבלית (כי זה מתאים לת"ח של חבורה אבלית) וזו סתירה.

תורת גלואה – תרגול 12

תרגיל ממבחן

$$K = \mathbb{Q}(\rho_9)$$

1. חשבו את הדרגה K/\mathbb{Q} ואת $\text{Gal}(K/\mathbb{Q})$
2. חשבו את דרגת ההרחבה $K/\mathbb{Q}(\rho_9 + \rho_9^{-1})$
3. מצאו את הפולינום המינימלי של $\rho_9 + \rho_9^{-1}$

פתרון

1. צריך לחשב את הדרגה של ϕ_q (הפולינום הציקלוטומי). ידוע ש

$$x^9 - x = \phi_1 \phi_3 \phi_9$$

$$\phi_9 = \frac{x^9 - x}{\phi_1 \phi_3} = \frac{x^9 - x}{(x-1)(x^2 + x + 1)}$$

$$\deg \phi_9 = 6$$

חבורת גלואה ציקלוטומית

$$\text{Gal}(\mathbb{Q}[\rho_9]/\mathbb{Q}) \cong u_9 = \{1, 2, 4, 5, 7, 8\}$$

2. זהו שדה ביניים. נציג אותו:

$$\mathbb{Q}(\rho_9 + \rho_9^{-1}) = K^H$$

ואז לפי משפט גלואה

$$[K : \mathbb{Q}(\rho + \rho^{-1})] = |H|$$

נעבור על איברי חבורת הגלואה, $\{\sigma_k : \sigma_k(p) = p^k\}$ ונבדוק איזה מהם שומרים על H .

$$\sigma_1 = id \quad \checkmark$$

$$\sigma_2(\rho + \rho^{-1}) = \rho^2 + \rho^7 \quad X$$

$$\sigma_4(\rho + \rho^{-1}) = \rho^4 + \rho^5 \quad X$$

$$\sigma_5(\rho + \rho^{-1}) = \rho^5 + \rho^4 \quad X$$

$$\sigma_7(\rho + \rho^{-1}) = \rho^7 + \rho^2 \quad X$$

$$\sigma_8(\rho + \rho^{-1}) = \rho^8 + \rho = \rho^{-1} + \rho \quad \checkmark$$

ולכן $H = \langle \sigma_8 \rangle \cong \langle 8 \rangle$ ולכן הדרגה היא 2.

3. הדרגה של הפולינום המינימלי היא $[\mathbb{Q}(\rho + \rho^{-1}) : \mathbb{Q}]$ שזה לפי התאמת גלואה $[u_8 : \langle 8 \rangle] = 3$.

נמצא את שאר השורשים ע"י הפעלת חבורה גלואה ומציאת כל הצמודים של $\rho + \rho^{-1}$.
כבר חשבנו:

$$\rho + \rho^{-1}, \rho^2 + \rho^7, \rho^4 + \rho^5$$

ולכן הפ"מ הוא

$$(x - (\rho + \rho^{-1}))(x - (\rho^2 + \rho^7))(x - (\rho^4 + \rho^5))$$

מסקנה ממשפט גלואה

אם E/F הרחבת גלואה סופית, יש מספר סופי של שדות ביניים.

מסקנה 0.1 E/F סופית ספרבילית \Leftrightarrow יש מספר סופי של שדות ביניים. (ניתן להרחיב $K/E/F$ כך ש K/F גלואה סופית).

משפט שטייניץ

F שדה אינסופי K/F הרחבה סופית, אזי $K = F[a]$ אם ורק אם יש ל K/F מספר סופי של שדות ביניים.

דוגמא נגדית (לא ברור למה)

שדה K ממאפיין p $K = F(y^p)$. ההרחבה $K(y)/K(y^p) = F(y)/F$ היא לא ספרבילית אבל כן יש איבר פרמיטיבי. (היא לא ספרבילית כי פ"מ של y זה $x^p - y^p = (x - y)^p$ שלא ספרבילי.)

דוגמא

נראה שהיא לא ספרבילית ע"י כך שנצביע על אינסוף שדות ביניים. $F(x + \alpha y)$. $\mathbb{Z}_p(x, y)/\mathbb{Z}_p(x^p, y^p)$ הרחבה סופית. נראה שהיא לא ספרבילית ע"י כך שנצביע על אינסוף שדות ביניים. נראה שבאמת יש פה אינסוף:

$$F(x + \alpha y) = F(x + \beta y)$$

$$(\alpha - \beta)y = (x + \alpha y) - (x + \beta y) \in F(x + \alpha y)$$

אם $\alpha \neq \beta$ אז $x, y \in F(x + \alpha y)$ ואז $F(x + \alpha y) = F(x, y)$ וזו סתירה.

הגדרה 0.2 שדה F נקרא סגור אלגברית אם אין לו אף הרחבה אלגברית סופית \Leftrightarrow כל פולינום מעל F מתפצל לגורמים ליניאריים.

הוכחנו בהרצאה משפטים נפלאים:

1. \mathbb{C} סגור אלגברית

2. \mathbb{C}/\mathbb{R} היא הרחבה אלגברית יחידה של \mathbb{R} .

הגדרה 0.3 יהי F שדה. הסגור האלגברי של F הוא הרחבה E/F כך ש E סגור אלגברית.

תורת גלואה – תרגול 13

הגזרה 0.1 הרחבת שדות E/F מוגדרת ריבועית/2 – רדיקלית אם יש שדות ביניים

$$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = E$$

כך ש

$$[F_{i+1} : F_i] = 2$$

משפט 0.2 מספר a הוא בר בנייה אם הוא מוכל בהרחבה E/\mathbb{Q} כך ש E/\mathbb{Q} רדיקלית. **בפרט:** $[\mathbb{Q}[a] : \mathbb{Q}] = \deg f_a$ חזקת 2. כלומר, זהו תנאי הכרחי אך לא מספיק.

עבור הרחבת גלואה E/F

$$|\text{Gal}(E/F)| = 2^n \text{ אם ורק אם } E/F$$

תרגיל (נפוץ במבחנים!)

האם ρ_7 הוא בר בנייה?

פתרון

$$[\mathbb{Q}[\rho_7] : \mathbb{Q}] = 6 \text{ לא חזקת 2 ולכן לא בר בנייה.}$$

תרגיל

האם ניתן לחלק ע"י סרגל ומחוגה כל זווית לשבע?
שקול: האם ניתן לבנות מצולע משוכלל עם 7 צלעות?

פתרון

זווית בגודל π ברור שניתן לבנות. אם היה ניתן, היה אפשר לקבל גם את $\frac{\pi}{7}$. אז, ע"י חיתוך במעגל היחידה נקבל את ρ_7 , בסתירה לתרגיל הקודם.

תרגיל

אם p ראשוני מהצורה $2^x + 1$, אז ρ_p ולכן גם $\cos \frac{2\pi}{p}$ הוא בר בנייה.

פתרון

$\mathbb{Q}[\rho_p]/\mathbb{Q}$ היא הרחבת גלואה. כידוע,

$$\text{Gal}(\mathbb{Q}[\rho_p]/\mathbb{Q}) \cong u_p$$

$$|u_p| = p - 1 = 2^k$$

כלומר חבורה גלואה היא מסדר 2^k ולכן ρ_n בר בנייה.

$$\cos \frac{2\pi}{p} \in \mathbb{Q}[\rho_p]$$

ולכן $\cos \frac{2\pi}{p}$ שייך להרחבה 2 רדיקלית ולכן הוא בר בנייה.

דוגמא

ρ_3, ρ_5 ברי בנייה, לכן ניתן לבנות מצולע משוכלל עם $5 \setminus 3$ צלעות.

טענה שתהיה לנו בש"ב

אם

$$F \subseteq K, L \subseteq E$$

2-רדיקלים, הקומפוזיטום KL הוא גם 2-רדיקלי.

שאלה

אם K, L הם ממימד שהוא חזקת 2. האם גם KL היא ממימד חזקת 2?

תשובה

לא!

נניח E/F גלואה כך ש $\text{Gal}(E/F) \cong S_4$ וניח

$$K = E^{H_1}$$

$$K = E^{H_2}$$

כאשר H_1 היא ת"ח התמורות ששומרות על $S_3 \cong 1$
 H_2 היא ת"ח התמורות ששומרת על $S_3 \cong 2$
 כעת

$$[K : F] = [S_4 : H_1]$$

כעת,

$$[K : F] = [S_4 : H_1] = 4$$

$$[L : F] = [S_4 : H_2] = 4$$

אבל,

$$[KL : F] = [E^{H_1} E^{H_2} : F] = [E^{H_1 H_2} : F] = [S_4 : H_1 \cap H_2] = 12 \neq 2^n$$

משפט 0.3 $f(x) \in \mathbb{Q}[x]$ עם שדה פיצול E . את f ניתן לפתור ע"י רדיקלים אם ורק אם $\text{Gal}(E/\mathbb{Q})$ פתירה.

תרגיל

האם הפולינום $f(x) = 5x^5 - 100x + 10$ פתיר ע"י רדיקלים?

פתרון

f אי פריק לפי אייזנשטיין עם 2.

$$f' = 25x^4 - 100$$

זה מתאפס כאשר

$$x^4 = 4$$

$$x = \pm\sqrt{2}$$

נשים לב ש

$$f(\sqrt{2}) > 0 \quad f(\sqrt{2}) < 0$$

ולהסיק שיש 3 שורשים ממשיים ו-2 מרוכבים

הוכחנו פעם

אם p ראשוני ולפולינום אי פריק מדרגה p יש $p - 2$ שורשים ממשיים 21 מרוכבים, אז $\text{Gal}(E/\mathbb{Q}) \cong S_p$ כש E שדה הפיצול. ולכן, אצלנו

$$\text{Gal}(E/\mathbb{R}) \cong S_5$$

שהיא לא פתירה

תזכורת

S_n, A_n אינן פתירות עבור $n \geq 5$.

הבהרה מתרגול שעבר

אמרנו בתרגול ש $E = F[a] \Leftrightarrow$ יש מספר סופי של שדות ביניים. בהרצאה אמרנו E/K ספרבילית \Leftarrow מספר סופי של שדות ביניים. אם $[E : F]$ לא ראשוני, גם הכיוון השני נכון