

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

21 בפברואר 2017

**מרצה: פרופסור אליעזר רואן
סמסטר א' - 2017 תשע"ז**

ערך: איתי רוזנבאום

תורת גלואה – הרצאה ראשונה

מוסכמה בקורס F תמיד יסמל שדה

הגדרה 0.1 משוואה ממעלה n היא בצורה $\sum_{i=0}^n \alpha_i x^i = 0$ כאשר $\alpha_i \in F$ ו- $\alpha_n \neq 0$. משוואה מדרגה 1 תקרא **משוואה ליניארית**, משוואת ממעלה שנייה תקרא **משוואה ריבועית**.

מספרים בעלי בנייה

מתחילים עם הנקודות 0,1. מותר לנו ליצור מעגל שמרכזו בנקודת בנייה. מותר גם לחבר שתי נקודות בנויות לקו. כך, ניתן לבנות נקודה חדשה ע"י חיתוך של:

1. שני קווים שבנינו

2. קו ומעגל

3. שני מעגלים

כך, את המספר 2 נבנה ע"י מעגל ברדיוס 1 שמרכזו ב1, וחיתוך שלו עם הציר הממשי. כך נוכל לבנות גם את 3, 4 ואת כל שאר הטבעיים. את המספר 1.5 נבנה ע"י בניית מעגל שמרכזו ב1 ומעגל שמרכזו ב2 (בעלי רדיוס 1 כתמיד) והעברת ישר בין נקודות החיתוך שלהם. חיתוך ישר זה עם הציר הממשי יסמל את המספר 1.5. כך נבנה את המספרים הרציונלים.

שתי בניית נוספות וחשובות:

1. אנך מנקודה לציר הממשי שלנו.

2. אנך מנקודה על הקו.

כעת כבר מותר לנו לבנות ריבוע. ע"י בניית ריבוע באורך צלע 1 כאשר הבסיס מונח על הקטע $[0, 1]$, אורך האלכסון הוא $\sqrt{2}$

הוכחה אוריגמית (מה?) ש- $\sqrt{2}$ לא רציונלי

נניח $\sqrt{2} = \frac{p}{q}$ עבור $p, q \in \mathbb{N}$. מכאן נעשה כל מיני בניית עם משולשים ונקבל שזה לא שבר מצומצם ופוצץ.

פתרון משוואות

בהנתן $\sum_{i=0}^n \alpha_i x^i = 0$ ניתן להציב $y = x + \frac{\alpha_{n-1}}{n}$ ונקבל שהמקדם $\alpha_{n-1} = 0$, ולכן תמיד אפשר להניח שמקדם זה הוא 0. כמו כן, ניתן להניח שכל פולינום מתוקן. לכן, פתרון המשוואה $x^3 + b^2x = 2b^2c$ יאפשר פתרון של כל הפולינומים ממעלה שלישית. פתרון זה ניתן ע"י חיתוך הישר $x^2 = by$ עם הפרבולה $(x - c)^2 + y^2 = c^2$

תורת גלואה – הרצאה שנייה

המשפטים העיקריים בהם נתעסק בקורס

1. מיון מספרים בעלי בנייה.
2. לפתור את הבעיות העתיקות של היוונים.
3. המשפט היסודי של האלגברה.
4. המבנה של שדות סופיים.
5. התאמת גלואה בין הרחבות של שדות וחבורות סופיות.
6. משפט גלואה: מתי אפשר לפתור משוואה.

הרחבת שדות

נניח $F \subset K$ נאמר ש K/F הרחבה של שדות.¹

הערה 0.1 K/F מרחב וקטורי, לכן קיים מימד (אולי אינסופי).

נתון $a \in K$ נגדיר:

$$F[a] = \left\{ \sum_{i=0}^n \alpha_i a^i : n \in \mathbb{N}, \alpha_i \in F \right\}$$
$$\sum_{i=0}^n \alpha_i a^i + \sum_{i=0}^n \alpha'_i a^i = \sum_{i=0}^n (\alpha_i + \alpha'_i) a^i :$$
$$\left(\sum_{i=0}^n \alpha_i a^i \right) \cdot \left(\sum_{j=0}^n \alpha_j a^j \right) = \sum_u \left(\sum_{i=0}^u \alpha_i \beta_{u-i} \right) a^u$$

למה 0.2 יש הומומורפיזם (הומומורפיזם ההצבה) $\varphi : F[x] \rightarrow K$ ע"י

$$\sum_{i=0}^n \alpha_i x^i \mapsto \sum_{i=0}^n \alpha_i a^i$$
$$\varphi_a(F[x]) = F[a]$$

"המילה היפה ביותר באלגברה היא הומומורפיזם" פרופסור רואן.

¹נשתמש מעתה בסימון K/F להרחבת שדות ואילו K/F לחוג מנה. ייתכן שאתבלבל לפעמים ביניהם.

הוכחה: נכתוב $g = \sum \beta_j x^j, f = \sum \alpha_i x^i$

$$\varphi_a(fg) = \varphi_a\left(\sum_{i=0}^u \left(\sum_{i=0}^u \alpha_i \beta_{u-i}\right) x^u\right) = \sum_u \left(\sum_{i=0}^u \alpha_i \beta_{u-i}\right) a^u = \sum \alpha_i a^i \cdot \sum \beta_j a^j =$$

$$f(a)g(a) = \varphi_a(f)\varphi_a(g)$$

■ $\varphi_a(f+g) = \varphi_a(f) + \varphi_a(g)$ (תבדקו).

איברים אלגבריים וטרנסנדנטים

$F[a] = K \Leftrightarrow \varphi_a$ על
 $\{a \text{ כל פולינום שמאפס את } a\} = \ker \varphi_a = F[\lambda]f_a$
 עבור איזשהו פולינום f_a .
 f_a נקרא הפולינום המינימלי של a (אם $f_a \neq 0$)
 איבר a נקרא **טרנסנדנטי** מעל F אם $f_a = 0$
 (ואז $\varphi_a : F[x] \rightarrow F[a]$ הוא איזומורפיזם)
 איבר a נקרא **אלגברי** (מדרגה n) מעל F אם $\deg f = n$ ו- $f_a \neq 0$
 $F[a] \subset K$ תת מרחב (וקטורי) של K מעל F ותחום שלמות
 $F[a] \cong F[\lambda]/F[\lambda]f_a = \ker \varphi_a$
 לכן $F[\lambda]f_a$ אידיאל ראשוני (שמניחים ששונה מ-0)
 אבל כל אידיאל ראשונה שונה מאפס בתחום ראשי הוא מקסימלי, לכן $F[a]$ הוא שדה.

מהו המימד של $F[a]$ מעל F ?

נגדיר $\dim_F F[a] = [F[a] : F]$

הגדרה 0.3 $\deg a = \deg f_a$

טענה 0.4 $[F[a] : F] = \deg f_a$ עם בסיס $1, a, a^2, \dots, a^{n-1}$ כאשר $n = \deg f_a$

הוכחה: בת"ל: נניח $\sum_{i=0}^{n-1} \beta_i a^i = 0$ לכן a שורש של $\sum_{i=0}^{n-1} \beta_i \lambda^i$ מדרגה קטנה מ- n

פורש: נגדיר $V = \sum_{i=0}^{n-1} Fa^i$. צ"ל: $a^m \in V$ לכל m . (כי $F[a]$ נפרש ע"י a^i $i \in \mathbb{N}$).

נכתוב $f_a = \sum_{i=0}^n \alpha_i \lambda^i$ לכן $f_a(a) = \sum_{i=0}^n \alpha_i a^i = 0$

$$a^n = -\frac{1}{\alpha_n} \sum_{i=0}^{n-1} \alpha_i a^i \in V$$

$$a^{n+1} = aa^n \in aV = a \sum_{i=0}^{n-1} Fa^i = \sum Fa^{i+1} = Fa^n + \sum_{j=1}^{n-1} Fa^j \subseteq V + V = V$$

אפשר לסיים לפי אינדוקציה (תרגיל). ניתן גם לפי נימוק מהיר לפי אלגוריתם.

הגדרה 0.5 $a, b \in K$ כאשר $F[a, b] = (F[a])[b] = \sum_{\text{final}} \alpha_{ij} a^i b^j = \sum_j \left(\sum_i \alpha_{ij} a^i \right) b^j$ לכן גם $F[a, b] = F[b][a]$ כי הכל מתחלף.

טענה 0.6 אם a, b אלגברים מעל F אז $F[a, b]$ שדה ו $[F[a, b] : F] \leq [F[a] : F] [F[b] : F]$

הוכחה: $[F[a, b] : F] = [F[a, b] : F[a]] \cdot [F[a] : F] \neq \deg f_b \cdot \deg g_a$
 תשימו לב כי $f_b \in F[\lambda]$ קל וחומר $f_b \in (F[a])[\lambda]$

1. $\deg a = 1 \Leftrightarrow F[a] = F \Leftrightarrow a \in F$

2. אם $a = b \notin F$ (מקרה חריג) אז $F[a, b] = F[a]$ ולכן $[F[a, b] : F] = \deg a < (\deg a)^2 = \deg a \deg b$

3. $F = \mathbb{Q}$ $a = \sqrt{2}$ $b = \sqrt{3}$ $f_a = \lambda^2 - 2$ $f_b = \lambda^2 - 3$ f_b עדיין הפולינום המינימלי של $\sqrt{3}$ שעל $\mathbb{Q}[\sqrt{2}]$

מסקנה 0.7 אם a, b אלגברים מעל F אז $a + b, ab, a^{-1}$ גם אלגברים מעל F .

הוכחה: כולם נמצאים בתוך השדה $F[a, b]$

משפט 0.8 נניח $F \subset K \subset L$ שדות אז $[L : K][K : F] = [L : F]$

הוכחה: ניקח בסיס a_1, \dots, a_m של K מעל F .

ניקח בסיס b_1, \dots, b_n של L מכל K .

צ"ל: $\{a_i b_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ בסיס של L מעל F .

פורש: כל איבר ב L הוא בצורה $\sum_{j=1}^n \beta_j b_j$ כאשר $\beta_j \in K$ כי זה

בסיס מעל F .

$$\sum \beta_j b_j = \sum_{j=1}^n \sum_{i=1}^m \alpha_{ij} a_i b_j = \sum_{i=1}^m \sum_{j=1}^n \alpha_{ij} a_i b_j$$

ב"ת: נניח $0 = \sum_{i=1}^m \sum_{j=1}^n \alpha_{ij} a_i b_j = \sum_{i=1}^m \left(\sum_{j=1}^n \alpha_{ij} a_i b_j \right)$

$\forall i, \forall j \alpha_{ij} = 0$ לכן $\sum_{i=1}^m \alpha_{ij} a_i \leftarrow$ בסיס b_1, \dots, b_n

תורת גלואה – הרצאה 3

משפט 0.1 הוכחנו שאם $F \subset K \subset L$ שדות, אזי $[L : K][K : F] = [L : F]$

מסקנה 0.2 $[K : F][L : F]$

מסקנה 0.3 אם $[L : F]$ ראשוני ו $K \neq F$ אז $K = L$

הוכחה: $[K : F] \neq 1$ לכן $[K : F] = [L : F]$ ומליניאריות 1 אנו יודעים שנת מרחב מהמימד של המרחב הגדול – שווה למרחב הגדול!

■

דוגמא

אם $F \subset K_1, K_2 \subseteq L$ חוגים, שדה, נגדיר $a_i \in K_1, b_i \in K_2$, $t \in \mathbb{N}$, $K_1 K_2 = \left\{ \sum_{i=1}^t a_i b_i \right\}$.

צריך לבדוק שזה סגור ביחס לסכום (טריוויאלי) ומכפלה (קללל), לכן $K_1 K_2$ תת חוג של L .

למה 0.4 אם L שדה ו $[L : F] < \infty$ אז $K_1 K_2$ שדה.

הוכחה: ניקח $\sum_{i=1}^b a_i b_i \in K_1 K_2$ אז

$\sum a_i b_i \in F[a_1, \dots, a_t, b_1, \dots, b_t] = (((F[a_1])[a_2]) \dots [a_t])[b_1] \dots [b_t]$ שדה לפי אינדוקציה, לכן $\sum a_i b_i$ הפיך ב $F[a_1, \dots, a_t, b_1, \dots, b_t]$ וקל וחומר הפיך ב $K_1 K_2$

■

מסקנה 0.5 אם $[K_1 : F], [K_2 : F]$ זרים אז $[K_1 K_2 : F] = [K_1 : F][K_2 : F]$

הוכחה: $[K_1 : F], [K_2 : F]$ מחלקים את $[K_1 K_2 : F]$ לכן גם המכפלה מחלקת.

■

דוגמא

$$\mathbb{Q}[\sqrt{2}, \sqrt[3]{5} : \mathbb{Q}] = 6$$

דוגמא

$$[\mathbb{Q}[\sqrt{2}, \sqrt{5}] : \mathbb{Q}] = ?$$

נשים לב:

$$[\mathbb{Q}[\sqrt{2}, \sqrt{5}] : \mathbb{Q}] = 2 \text{ אם}$$

$$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[\sqrt{2}, \sqrt{5}] \text{ אז}$$

$$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 \text{ כי}$$

$$\sqrt{5} = \mathbb{Q}[\sqrt{2}] \text{ ואז נקבל ש}$$

$$\sqrt{5} = \alpha + \beta\sqrt{2}, \alpha, \beta \in F \text{ ואז}$$

$$5 = (\alpha + \beta\sqrt{2})^2 = \alpha^2 + 2\beta^2 + \alpha\beta\sqrt{2} \text{ לכן}$$

$$\alpha\beta = 0 \text{ לכן בהכרח}$$

$$\alpha = 0 \text{ גורר } 5 = 2\beta^2 \text{ בסתירה}$$

$$\beta = 0 \text{ גורר } 5 = \alpha^2$$

$$\sqrt{5} \notin \mathbb{Q}[\sqrt{2}] \text{ לכן}$$

ולכן המימד חייב להיות 4.

"אם שואלים אתכם ברחוב על פולינום אם הוא פריק ואין לכם זמן לחשב, תגידו אייזנשטיין" פרופסור רואן.

שאלה

נניח a, b אלגבריים מעל F עם פולינום מינימליים f_a, f_b האם f_b נשאר הפולינום המינימלי של b מעל $F[a]$?

טענה 0.6 נניח $f(a) = 0$ אז $f = f_a$ או $f \Leftrightarrow f = f_a$ פולינום אי פריק.

הוכחה: \Leftarrow נוכיח כי f_a אי פריק. נניח $f_a = gh$, $0 = f_a(a) = g(a)h(a)$, לכן $g(a) = 0$ או $h(a) = 0$, לכן $\deg g = \deg f_a$ או $\deg h = \deg f_a$ לכן h (או g) קבוע ולכן נמצא ב- F והפיך. \Rightarrow אם f אינו הפולינום המינימלי, אז $\deg f_a < \deg g$ לכן f פריק. ($f = gf_n$)
כאשר $\deg g > 0$ ■

מסקנה 0.7 אם $\deg g \leq 3$ ואין ל- f שורש בתוך F אז f אי פריק ולכן $f = f_a$. ההפך לא נכון, לדוגמא $(\lambda^2 - 2)^2$ פריק אבל ללא שורש.

מסקנה 0.8 כל שימוש של אייזנשטיין, למשל $\lambda^n - p$ אי פריק מעל \mathbb{Q} עבור p ראשוני. למעשה מספיק לדרוש ש- p חופשי מריבועים (כלומר, מכפלה של מספרים ראשוניים ללא חזקות).

דוגמא

של 1 אז $f_\omega = f$ עבור $f = \lambda^{p-1} + \lambda^{p-2} + \dots + 1$ ראשוני מעל \mathbb{Q} . לכן, אם ω שורש $-p$ פרימיטיבי

דוגמא

הם f_a שורשים אחרים של $f_a = \lambda^5 - 2$, $a = \sqrt[5]{2}$ (אם $b^5 = 2$ אז $(\frac{b}{a})^5 = 1$, שורש 5 של 1, $0 \leq l \leq 4$, $\frac{b}{a} = \omega_5^l$, $b = \omega_5^l a$ עבור $0 \leq l \leq 4$).

באופן יותר כללי, השורשים של $\lambda^n - m$ הם $\omega_n^k \sqrt[n]{m}$ עבור $0 \leq k \leq n-1$. ניתן לראות זאת ע"י חישוב ישיר של $(\omega_n^k \sqrt[n]{m})^n$.

הערה 0.9 כל שורש יחידה ω_n^k מקיים את הפולינום $\lambda^n - 1$. זהו אינו הפולינון המינימלי מכיוון שהוא פריק, $\lambda^n - 1 = (\lambda - 1)(\lambda^{n-1} + \dots + 1)$. כעת $\lambda^{n-1} + \dots + 1$ אמ"מ n פריק.

דוגמא

$\lambda^5 - 7$ הפולינום המינימלי של $\sqrt[5]{7}$ וגם של $\omega_5^k \sqrt[5]{7}$.

מסקנה 0.10 (תרגיל) הפולינום f_a הוא הפולינום המינימלי של כל שורש שלו.

הוכחה: הוא אי פריק.

נתון פולינום $f \in F[\lambda]$, נמצא שדה $K \supset F$ ואיבר $\bar{a} \in K$ כך ש $f(\bar{a}) = 0$. **נשים לב:** ניקח פולינום g אי פריק שמחלק את f . $F[\lambda]g$ אידיאל ראשוני ושונה

מ-0, ולכן מקסימלי בתוך $F[\lambda]$.

לכן, $K := F[\lambda]/F[\lambda]g$ הוא שדה.

$\alpha \mapsto \alpha \mapsto \alpha + F[\lambda]$ ע"י $\psi : F \hookrightarrow F[\lambda] \rightarrow K$

ψ שיכון.

נגדיר $\bar{a} = \lambda + F[\lambda]g$.

K בתוך $g(\bar{a}) = g(\lambda) + F[\lambda]g \in F[\lambda]g = 0$

כי אם $g(\lambda) = \sum \beta_i \lambda^i$

$g(\bar{a}) = \sum \beta_i \lambda^i + F[\lambda]g = 0$

הערה חשובה $K \simeq F[a]$ ע"י $a \mapsto \bar{a}$ (אי פריק)

0.11 מסקנה אם a_1, a_2 שורשים של אותו פולינום אי פריק, אז $F[a_1] \simeq K \simeq F[a_2]$ ע"י

$$a_1 \mapsto \underbrace{\bar{a}}_{\lambda + F[\lambda]f} \mapsto a_2$$

איך נקבל את כל השורשים כל פולינום $f \in F[\lambda]$?

0.12 הגדרה f (מתוקן) מתפצל בתוך שדה E אם $\deg f = h$ וקיימים a_1, \dots, a_n זרים כך ש

$$f = (\lambda - a_1) \cdot \dots \cdot (\lambda - a_n)$$

פירוק בתוך $E[\lambda]$.

0.13 הערה כל שורש a של f ב E הוא שייך ל $\{a_1, \dots, a_n\}$ כי $0 = f(a) = (a - a_1) \cdot \dots \cdot (a - a_n)$ ואז $a - a_i = 0$ לאיזשהו i .

0.14 למה קיים E/F כאשר f מתפצל בתוך E .

הוכחה: ניקח $K_1 \supset F$ שמכיל שורש $a_1 = \bar{a}$ של f בתוך K_1 . $[K_1 : F] = 1$.

$$\deg f_1 \leq n - 1, f = (\lambda - a_1)f_1$$

נמשיך, קיים שדה K_2 מעל K_1 עם שורש של f_1 , $[K_2 : K_1] \leq n - 1$.

⋮
⋮
⋮

בסוף $E = K_n$, $[E : F] \leq n \cdot (n - 1) \cdot \dots \cdot 1 = n!$.

■

תורת גלואה – הרצאה 4

תזכורת

0.1 הגדרה $F \subset E$ שדות, $f \in F[\lambda]$ מתוקן **מתפצל** ב- E אם אם $f = (\lambda - a_1) \cdot \dots \cdot (\lambda - a_n)$ עבור $a_i \in E$ ($n = \deg f$)

הוכחנו גם את המשפט (החשוב) הבא:

0.2 משפט אפשר לקחת $E = F[a_1, \dots, a_n]$ כאשר $[E : F] \leq n!$

דוגמא

$E = \mathbb{C} = \mathbb{R}[i], F = \mathbb{R}$
 $\lambda^2 + 1 = (\lambda + i)(\lambda - i)$ מתפצל ב- E .
 $[\mathbb{C} : \mathbb{R}] = 2!$

דוגמא

μ שורש- n של 1, שורש של $\lambda^n - 1$, $f = \lambda^n - 1$,
כל μ^R שורש של f (ושונים זה מזה!) כי
 $(\mu^R)^n - 1 = (\mu^n)^R - 1 = 1^R - 1 = 1 - 1 = 0$
לכן $f = \prod_{R=0}^{n-1} (\lambda - \mu^R)$.
שימו לב כי כל $\mu^R \in F[\mu]$.

דוגמא

הם: $a \in F, f = \lambda^n - a$, השורשים של f :
 $\sqrt[n]{a} \mu^R$ עבור $0 \leq R \leq n - 1$.

0.3 הגדרה E שדה **פיצול** של פולינום $f \in F[\lambda]$ (מעל F) אם:

1. f מתפצל בתוך E

2. מינימליות: אם $E' \subseteq E$ ו- f מתפצל ב- E' אז $E = E'$

אז כותבים $E = F[a_1, \dots, a_n]$ כאשר $f = (\lambda - a_1) \cdot \dots \cdot (\lambda - a_n)$

דוגמאות

1. שדה הפיצול של $\lambda^2 + 1$ מעל \mathbb{R} הוא \mathbb{C}
2. שדה הפיצול של $\lambda^n - 1$ מעל \mathbb{Q} (ולמעשה, מעל כל תת שדה F של \mathbb{C}) הוא $\mathbb{Q}[\mu]$
3. שדה הפיצול של $\lambda^n - a$ מעל \mathbb{Q} הוא $E = \mathbb{Q}[\sqrt[n]{a}, \mu]$

הוכחה ל-3

ברור ש $\mu^R \sqrt[n]{a} \in E$ אבל אם $\sqrt[n]{a} \in E'$ ו $\mu \sqrt[n]{a} \in E'$ אז $\mu = \frac{\mu \sqrt[n]{a}}{\sqrt[n]{a}} \in E'$

בניה מופשטת יותר:

נתון $f \in F[\lambda]$, ניקח g גורם אי פריק של f , $K_1 = F[\lambda]/F[\lambda]g$, יש לו שורש $a_1 = f(a_1) = 0$, $g(a_1) = 0$ בתוך K_1 לכן $(\lambda - a_1) | f$ בתוך $K_1[\lambda]$.
מכאן נובע ש $f = (\lambda - a_1)f_1$, $\deg f_1 = \deg f - 1$. ממשיכים לפי אינדוקציה
(ניקח g_2 גורם אי פריק של f_1 בתוך $K_1[\lambda]$, $K_2 = K_1[\lambda]/K_1[\lambda]g_2$,
 $g_2(a_2) = 0$, $a_2 = \lambda + K_1[\lambda]g_2$ לכן $(\lambda - a_2) | f_1$, $f = (\lambda - a_1)(\lambda - a_2)g_3$, וכך הלאה.)

דוגמא

$f = \lambda^3 - 2$ מעל \mathbb{Q} , שורש של f , אבל $\mathbb{Q}[\sqrt[3]{2}]$ אינו שדה פיצול של f כי $\sqrt[3]{2}\mu_3$ שורש של f ולא נמצא ב $\mathbb{Q}[\sqrt[3]{2}]$. שדה הפיצול, כפי שהראנו בדוגמא 3 קודם, הוא:
 $E = \mathbb{Q}[\mu_3, \sqrt[3]{2}]$ ו $[E : \mathbb{Q}] = 2 \cdot 3 = 6$. הפולינום המינימלי של μ_3 הוא $\lambda^2 + \lambda + 1$ (קל לראות שהוא אי פריק בכך שנמצא את השורשים).

משפט 0.4 נניח E, E' שדות פיצול של f מעל F אז $E \cong E'$.

הכנה להוכחה

משפט 0.5 נניח $\varphi : F_1 \rightarrow F_2$ הוא איזומורפיזם, נגדיר: $\tilde{\varphi} : F_1[\lambda] \rightarrow F_2[\lambda]$
 ע"י: $\tilde{\varphi}(\sum \alpha_i \lambda^i) = \sum \varphi(\alpha_i) \lambda^i$ כאשר $\alpha_i \in F_1$
 אז $\tilde{\varphi}$ היא איזומורפיזם

■ הוכחה: $\tilde{\varphi}^{-1}(\sum \beta_i \lambda^i) = \varphi^{-1}(\beta_i) \lambda^i$

משפט 0.6 נניח $\varphi : K \rightarrow L$ הוא הומומורפיזם של שדות אז $\ker \varphi = \leftarrow \ker f \triangleleft K$
¹⁰, כלומר φ הוא חח"ע. למשל, נניח $F \subseteq K, L$ ו $\varphi|_F = 1_F$ אם $[K : F] = [L : F]$
 אז φ איזומורפיזם.

■ הוכחה: $[L : F] = [K : F] = [\varphi(K) : F]$
 תת מרחב מאותו מימד, לכן $\varphi(K) = L$, לכן $\varphi(K)$ גם על.

משפט 0.7 נניח $a \in E$ שורש של $f, f = (\lambda - a)h$ עבור $h \in K[\lambda]$ כאשר $K = F[a]$
 לכן שדה הפיצול של f מעל F הוא גם שדה הפיצול של h מעל K .

משפט 0.8 אם $\varphi : F_1 \rightarrow L$ הומו' אז אפשר להגדיר הומו $\tilde{\varphi} : F_1[\lambda] \rightarrow L[\lambda]$ לפי
 $\tilde{\varphi}(\sum \alpha_i \lambda^i) = \sum \varphi(\alpha_i) \lambda^i$

משפט 0.9 בהמשך למשפט הקודם, נניח $f \in F_1[\lambda]$ נכתוב $f_\varphi = \tilde{\varphi}(f) \in L[\lambda]$, נניח
 $f(a_1) = 0$ ונניח φ ממשיך להומו' (φ_1) , כאשר על F ו φ_1 זהים),
 $f_\varphi = \sum \varphi(\alpha_i) \lambda^i, f = \sum \alpha_i \lambda^i$ כי לכתוב $f_\varphi(\varphi_1(a_1)) = 0$ אז $\varphi_1 : F_1[a_1] \rightarrow L$
 $f_\varphi(\varphi_1(a_1)) = \sum \varphi(\alpha_i) \varphi_1(a_1)^i = \varphi_1(f(a_1)) = \varphi(0) = 0$
 מצד שני, נניח שרוצים להמשיך את ההומו'
 $\varphi : F \rightarrow L$ הומו $\varphi : F[a_1] \rightarrow L$ אז $\varphi_1(a_1)$ מוכרח להיות שורש של f_φ .
 זה מוכיח שהאופציות להמשיך φ הומו $\varphi_1 : F_1[a_1] \rightarrow L$ הם בדיוק השורשים של f_φ

משפט 0.10 נניח $\varphi : F \rightarrow L$ הומו' של שדות אז אפשר להמשיך את φ להומו' $\varphi : E \rightarrow L$
 כאשר E שדה הפיצול של f

הוכחה: נכתוב $E = F[a_1, \dots, a_n]$ ת ניקח $K = F[a_1], k \cong F[\lambda]/F[\lambda]g$ כאשר g גורם
 אי פריק של f, a_1 שורש של $\tilde{\varphi} : F[\lambda] \rightarrow L, \varphi : F[\lambda] \rightarrow L$,
 בוחרים שורש a'_1 של $g_\varphi = \tilde{\varphi}(g)$ ומגדירים הומומורפיזם:
 $\varphi : F[\lambda] \rightarrow L$ לפי,

¹כל אידיאל של שדה הוא 0 או כל השדה

$$\sum \beta_i \lambda^i \rightarrow \sum \beta_i (a'_1)^i \text{ , הגרעין מכיל } \sum \beta_i \lambda^i \rightarrow \sum \beta (a'_1)^i$$

הגרעין מכיל את $F[\lambda]g$ ולכן נותן הומו:

$$F[a_1] \cong F[\lambda]/F[\lambda]g \rightarrow L$$

n שדה E , $f = (\lambda - a_1)h$ פיצול של h מעל K לכן אפשר לפי אינדוקציה על n

להמשיך φ_1 להומומורפיזם. ■

אני מצרף כעת את תרגול 5, בו חזרנו על הוכחת משפט זה וראינו דוגמא

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

למה 0.11 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 $L \xrightarrow{x \mapsto b} F[a]$ ו $F[x] \xrightarrow{\hat{\psi}} L[x]$

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

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

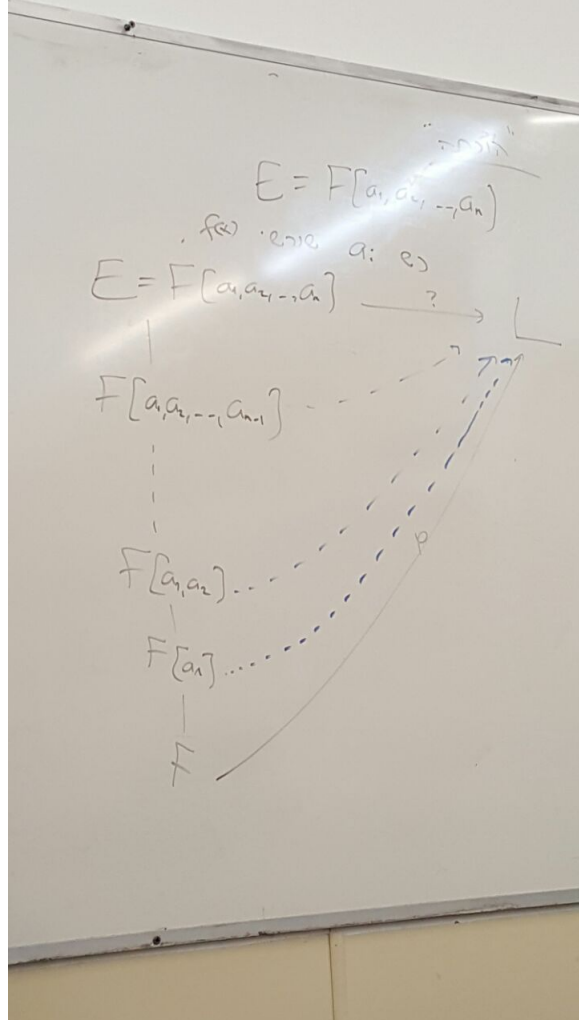
כמה הומומורפיזמים יש מ $F[a] \rightarrow L$?

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

משפט 0.12 נתון $\varphi : F \rightarrow L$ ו $f(x) \in F[x]$ כך ש $\hat{f}(x)$ מתפצל מעל L . (ב L 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 $F[a_1]$: $F[a_1][x] \ni f_{a_2}(x)$. ניקח שורש $b_2 \in L$ 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 $x^2 - 2$.
 $\hat{\varphi}(x^2 - 2) = x^2 - 2$ ולכן $\sqrt{2}$ ולכן $\sqrt{2}$ ללכת ל $\pm\sqrt{2}$.
נבחר $\sqrt{2} \mapsto -\sqrt{2}$
 זה מגדיר $\varphi_1 : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{C}$ 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 $\mathbb{Q}[\sqrt{2}, -\sqrt{2}] = \mathbb{Q}[\sqrt{2}]$ הוא $x^2 - 3$.
 $\hat{\varphi}_2(x^2 - 3) = x^2 - 3$ ולכן $\sqrt{3}$ 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 – הרצאה 5

סיכום ההוכחה מההרצאה הקודמת

טענה 0.1 נניח $\varphi : F \rightarrow \tilde{F}$, $\tilde{\varphi} : F[\lambda] \rightarrow \tilde{F}[\lambda]$ איזומורפיזם של שדות, $g \in F[\lambda]$ אי פריק, a_1 שורש של g בתוך שדה E שמכיל את F , L שדה שמכיל את \tilde{F} .
רוצים: $\tilde{\varphi}(a_1)$ ואיזומורפיזם $\varphi_1 : F[a_1] \rightarrow \tilde{F}[\tilde{a}_1]$, $\varphi_1(a_1) = \tilde{a}_1$, שורש של \tilde{g} בתוך L .
פתרון: זה קיים בדיוק עבור כל שורש $\tilde{a}_1 \in L$ של \tilde{g} .

■ **הוכחה:** $F[a_1] \cong F[\lambda]/F[\lambda]g \xrightarrow{\tilde{\varphi}} F[\lambda]/F[\lambda]\tilde{g} \cong \tilde{F}[\tilde{a}_1]$

משפט 0.2 נניח $f \in F[\lambda]$, E שדה הפיצול של F , $\varphi : F \rightarrow \tilde{F}$ איזומורפיזם, $\tilde{F} \subset L$ ו $\tilde{f} = \tilde{\varphi}(f)$ מתפצל בתוך L , אז L מכיל שדה פיצול \tilde{E} של \tilde{F} איזומורפי ל E .
תוספת חשובה למשפט: מספר ההומומורפיזמים (שהם בדיוק האיזומורפיזמים) $E \rightarrow \tilde{E}$ הם ל כלל היותר $[E : F] = [\tilde{E} : \tilde{F}]$ וקיים שוויון אם ורק אם השורשים כל F בתוך E שונים.

הערה 0.3 ברגע שידועים $[E : F] = [\tilde{E} : \tilde{F}]$ אז כל הומומורפיזם $\tilde{\varphi} : E \rightarrow \tilde{E}$ הוא איזומורפיזם (כי $\tilde{p}(E) \subseteq \tilde{E}$ מאותו מימד ולכן על).

הוכחה: ניקח g להיות הפולינום המינימלי של a_1 (ובפרט אי פריק). $\tilde{g}|\tilde{f} \Leftrightarrow g|f$.
 $(\tilde{f} = \tilde{g}\tilde{h} \Leftrightarrow f = gh)$
 נשים לב: כל גורם של פולינום $\tilde{f} = (\lambda - \tilde{a}_1) \cdots (\lambda - \tilde{a}_n)$ גם מתפצל בגלל פירוק יחיד של פולינומים.

נבחר שורש של \tilde{g} שנסמן \tilde{a}_1 (יש חופש עד $\deg \tilde{g}$). נגדיר $\tilde{K} = F[\tilde{a}_1]$, $K = F[a_1]$.
 $[E : K] = \frac{[E:F]}{[K:F] = \deg g} < [E : F]$, לכן לפי אינדוקציה φ_1 ממשיך להומומורפיזם $\tilde{\varphi} : E \rightarrow L$. מספר אופציות להמשיך את φ_1 ל $\tilde{\varphi}$ הוא לכל היותר $[E : K]$.
 שוויון אם ורק אם השורשים של f הם שונים. נגדיר: $\tilde{a}_i = \tilde{\varphi}(a_i)$ ולכן בנינו $\tilde{E} = \tilde{F}[\tilde{a}_1, \dots, \tilde{a}_n]$ שדה הפיצול של \tilde{E} של \tilde{f} בתוך L .
מה מספר האפשרויות ל $\tilde{\varphi}$?

קודם נמשיך את φ_1 ל φ (יש $\deg g$ אפשרויות), לפי אינדוקציה מספר ההמשכים φ_1 ל $\tilde{\varphi}$ הם לכל היותר $[E : K]$, שוויון אם ורק אם השורשים a_1, \dots, a_n של F בתוך E הם שונים. אבל מקבלים המשך מ $\tilde{\varphi}$ לפי קודם לקבל את φ_1 ואז להמשיך ל $\tilde{\varphi}$. לכן

מספר ההומומורפיזמים שממשיכים את φ הם לכל היותר $[K : F][E : K]$ ושוויון כאשר השורשים שונים. ■

מתי שורשים של פולינום שונים?

הגדרה 0.4 איבר $a \in K$ ספרבילי מעל F אם אין שורש כפול של f_a . פולינום הוא ספרבילי אם אין לו שורש כפול. כלומר, אם $f = (\lambda - a_1) \cdots (\lambda - a_n)$ אז a_1, \dots, a_n שונים.

נגזיר נגזרת של פולינום

- אינפי של תינקות: נגזיר $f = \sum \alpha_i \lambda^i$, נגזיר $f' = \sum i \alpha_i \lambda^{i-1}$.
- תרגיל: $(f+g)' = f' + g'$, $(\alpha f)' = \alpha f'$, $(fg)' = fg' + gf'$.

טענה 0.5 פולינום f ספרבילי $\Leftrightarrow f$ זר ל' f .

הוכחה: (\Leftarrow) נוכיח בדרך השלילה. נכתוב $f = (\lambda - a)^2 g$, $f' = 2(\lambda - a)g + (\lambda - a)^2 g'$, $\lambda - a$ מחלק את f ו' f ולכן הם אינם זרים. (\Rightarrow) נניח $\lambda - a$ מחלק את f ו' f , $f' = (\lambda - a)g$, $f = (\lambda - a)^2 |f|$, $f' = (\lambda - a)g' + g$, $(\lambda - a)^2 |f| \Leftarrow (\lambda - a) |g| \Leftarrow$ ■

השלמה להוכחה

טענה 0.6 נניח $F \subset K$, $f, g \in F[\lambda]$, אז f, g זרים מעל F $\Leftrightarrow f, g$ זרים מעל K .

הוכחה: (\Rightarrow) ברור.

(\Leftarrow) נכתוב $pf + qg = 1$ עבור $p, q \in F[\lambda]$ ברור ש $p, q \in K[\lambda]$ לכן f, g זרים מעל K . ■

מסקנה 0.7 פולינום $f \neq 0$ לא קבוע ואי פריק הוא ספרבילי אם ורק אם $f' \neq 0$.

הוכחה: $\deg f' = \deg f - 1$ ו $1 < \deg f$ לכן אם $f' \neq 0$, כל גורם משותף של f ו' f הוא גורם של f ולכן שווה ל' f , אבל הוא מחלק את f ו' f בגלל ש $\deg f' < \deg f$ כי f אי פריק, ולכן $f' = 0$. ■

הגדרה 0.8 האמפיין של F , $\text{char}(F)$ הוא ה $m > 0$ הקטן ביותר כך ש $m \cdot 1 = 0$. אם אין m כזה אז $\text{char}(F) = 0$.

הערה 0.9 יש הומומורפיזם $\psi : \mathbb{Z} \rightarrow F$ ע"י $1 \mapsto 1, m \mapsto m \cdot 1$, $\ker \psi = p\mathbb{Z}$ איזוהו מספר p . $\psi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} \subset F$ לכן $\mathbb{Z}/p\mathbb{Z}$ תחום שלמות לכן φ ראשוני. הוכחנו ש $\text{char}(F)$ מספר ראשוני.

מסקנה 0.10 $\Leftrightarrow char(F) = 0$ כל פולינום אי פריק מעל F הוא ספרבילי ועבור $f = \sum \alpha_i \lambda^i$ אי פריק הוא אי-ספרבילי $\Leftrightarrow p|i$ עבור כל i כך ש $p = char(F) \neq 0$, כלומר f בצורה $\sum \alpha_j (\lambda^p)^j$ (נכתוב $i = pj$).

דוגמא

למעל $F = \mathbb{Z}/2\mathbb{Z}$, $char(f) = 2$, $f(0) = \lambda^2 + 1$, $f(0) = 1$, $f(1) = 1 + 1 = 0$, $f' = 2\lambda = 0$
אבל! $f = (\lambda + 1)^2$ ולכן פריק.

הגדרה 0.11 שדה מושלם (*perfect*) אם כל פולינום אי פריק מעליו הוא ספרבילי.

דוגמאות

1. \mathbb{Q} (או לחלופין כל שדה ממאפיין 0)

2. כל שדה סופי

הגדרה 0.12 E/F הרחבת גלואה אם E שדה פיצול של פולינום סופי.

הגדרה 0.13 חבורת גלואה, המוסמנת $Gal(E/F)$ כי קבוצת כל האוטומורפיזמים של E שקובעים את F ($F \cong \tilde{F}$), כאשר הפעולה היא הרכבת אוטומורפיזמים.

הערה 0.14 המשפט שהוכחנו אומר שאם E/F הרחבת גלואה, אז $|Gal(E/F)| = [E : F]$

תורת גלואה – הרצאה 6

הגדרה 0.1 הרחבת גלואה של E/F הוא שדה פיצול של פולינום ספרבילי מעל F ($f \in F$)
($F[\lambda]$ ואז $\text{Gal}(E/F) = \{\sigma \in \text{Aut}(E/F)\}$).

הערה 0.2 $|\text{Gal}(E/F)| = [E : F]$ כאשר E/F הרחבת גלואה.

הגדרה 0.3 נתון חבורת אוטומורפיזמים G של E . נגדיר:
 $E^G := \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}$

טענה 0.4 E^G הוא שדה

הוכחה: $\alpha_1, \alpha_2 \in E^G$ אז $\sigma(\alpha_1) = \alpha_1$ ו $\sigma(\alpha_2) = \alpha_2$ $\Leftrightarrow \sigma(\alpha_1^{-1}) = \sigma(\alpha_1)^{-1} = \alpha_1^{-1}$
 $\sigma(\alpha_1 \pm \alpha_2) = \sigma(\alpha_1) \pm \sigma(\alpha_2) = \alpha_1 \pm \alpha_2$
 $\sigma(\alpha_1 \alpha_2) = \sigma(\alpha_1) \sigma(\alpha_2)$
לכן E^G סגור ל הופכי, כפל ו \pm ולכן שדה. ■

טענה 0.5 נניח E/F הרחבת גלואה ו $G = \text{Gal}(E/F)$ אז $E^G = F$

הוכחה: $F \subseteq E^G \subseteq E$ לכן: $[E : E^G][E^G : F] = [E : F] = |G|$
אבל נתון ש E שדה פיצול של פולינום $f \in F[\lambda]$ לכן E שדה פיצול של f מעל E^G
לכן $|G| = [E : E^G]$
לכן $E^G = F \Leftrightarrow [E^G : F] = 1, [E : E^G] = [E : F]$ ■

הגדרה 0.6 נניח E/F שדות, אומרים ש $a \in E$ איבר ספרבילי מעל F אם הפולינום
המינימלי $f_a \in F[\lambda]$ של a הוא פולינום ספרבילי.

הגדרה 0.7 E/F הוא הרחבה נורמלית אם לכל $a \in E$, f_a מתפצל ב E (כלומר, מכפלה
של גורמים ליניארים)

¹כל אוטומורפיזם σ של E כך ש $\sigma|_F = 1$

למה 0.8 נניח G חבורת אוטו' של E ו $a \in E$ אז $(\lambda - \sigma(a)) \in E^G[\lambda]$ $\prod_{\sigma \in G, \text{different}}$

הוכחה: נגדיר $g = \prod_{\sigma \in G} (\lambda - \sigma(a))$, נגדיר $\hat{\sigma} : E[\lambda] \rightarrow E[\lambda]$ ע"י:

$$\hat{\sigma} \left(\sum b_i \lambda^i \right) = \sum \sigma(b_i) \lambda^i$$

$$\hat{\sigma}(g) = \hat{\sigma} \left(\prod_{\tau \in G} (\lambda - \tau(a)) \right) = \prod_{\tau \in G} \hat{\sigma}(\lambda - \tau(a)) = \prod_{\tau \in G} (\lambda - \sigma(\tau(a))) = \prod_{\tau \in G} (\lambda - \tau(a)) = g$$

נכתוב: $g = \sum b_i \lambda^i$

$$\sum b_i \lambda^i = g = \hat{\sigma}(g) = \sum \sigma(b_i) \lambda^i$$

$$\forall \sigma \in G, \forall i \sigma(b_i) = b_i \Leftarrow$$

$$\forall i, b_i \in E^G \Leftarrow$$

$$g \in E^G \Leftarrow$$

■

המשפט היסודי (הראשון) של תורת גלואה

נניח $[E : F] < \infty$, התנאים הבאים שקולים:

1. E/F גלואה

2. $F = E^G$ לאיזושהי חבורת אוטומורפיזמים G של E (אז אפשר לקחת $G = \text{Gal}(E/F)$)

3. E/F הרחבה ספרבילית (כלומר, כל איבר של E ספרבילי) ונורמלית

הוכחה:

(1) \Rightarrow (2) הוכחנו.

(2) \Rightarrow (3)

ניקח $a \in E$. צ"ל: f_a ספרבילי ומתפצל ב E .

נגדיר $g = \prod_{\sigma \in G} (\lambda - \sigma(a)) \in E^G[\lambda] = F[\lambda]$, לפי הלמה a שורש של g .

$f_a | g$ כי f_a הפולינום המינימלי של a .

קל וחומר, f_a ספרבילי ומתפצל בתוך E .

(3) \Rightarrow (1)

נכתוב $E = F[a_1, \dots, a_n]$.

נניח $f_i =$ הפולינום המינימלי של a_i .

ניקח $f =$ מכפלה של f_i שונים.

נשים לב: אם f_i, f_j עם שורש משותף, אז f_i, f_j אינם זרים מעל E .

f_i, f_j אינם זרים מעל F \Leftarrow

אבל הם אינם פריקים מעל F לכן $f_i = f_j$.

לכן כל a_i שורש של f , לפי ההגדרה f מתפרק ל $(\lambda - a_1) \cdots (\lambda - a_n)$ וספרבילי. ■

דוגמה של אי יחידות של f

$$(\lambda^2 - 2)(\lambda^2 - 3) \mathbb{Q}[\sqrt{2}, \sqrt{3}]$$

$$((\lambda - 7)^2 - 18)(\lambda^2 - 6) \mathbb{Q}[3\sqrt{2} + 6, \sqrt{6}]$$

. $G = \text{Gal}(E/F)$ בהנחה $E^G = F$ שאם $E^G = F$ אז בהנחה
 ברור ש $G \subseteq \text{Gal}(E/F)$, לכן
 $|G| \leq |\text{Gal}(E/F)| = [E : F]$
 לשם כך נוכיח את למת ארטיין:

למת ארטיין

אם G חבורת אוטו' של שדה E ו $F = E^G$ אז $|G| \geq [E : F]$,
 (ואז $G = \text{Gal}(E/F) \iff |G| = |\text{Gal}(E/F)|$)

הוכחה: נוכיח שאם $a_1, \dots, a_m \in E$ עבור $m > n = |G|$ אז a_1, \dots, a_m תלויים מעל F .

ניקח את המערכת: $\forall 1 \leq j \leq n \sum_{i=1}^m \sigma_j(a_i) b_i$ כאשר $G = \{\sigma_1, \dots, \sigma_n\}$ (כי b_i קבועים ביחס ל σ_i).

יש פתרונות אי טריוויאליים (b_1, \dots, b_m) לפי אלגברה ליניארית.

לפי שינוי סימון של a_1, \dots, a_n אפשר להניח ש $b_1 \neq 0$

(כלומר, בלי הגבלת הכלליות נניח ש b_1 הוא שאינו מתאפס)

ניקח {הוקטורים (b_1, \dots, b_m) ששורשים של המערכת $V := \{$

$v \in V, v \neq 0$ עם מספר מינימלי של מרכיבים שונים מאפס (כאשר $b_1 \neq 0$).

נחלק את v בסקלר b_1 . לכן נניח $b_1 = 1$.

נוכיח כל $b_i \in F$

[נסיים את ההוכחה כי ניקח $\sigma =$ הזהות בתוך E]

ואז $\sum_{i=1}^m b_i a_i = 0$ ואז נקבל תלות של a_1, \dots, a_m

■

הערה 0.9 נשם לב שאם $(b_1, \dots, b_m) \in V$ אז $(\tau(b_1), \dots, \tau(b_m)) \in V$ לכל $\tau \in G$

$$\sum \sigma_j(a_i) \tau(b_i) = \tau \left(\sum \tau^{-1} \sigma_j(a_i) b_i \right) = \tau(0) = 0$$

לכן $v - \tau(v) \in V$

$$(b_1 - \tau(b_1), b_2 - \tau(b_2), \dots)$$

לפי הגדרת אוטומורפיזם. $\tau(1) = 1$ כי $b_1 - \tau(b_1) = 1 - 1 = 0$

לפי ההנחה על מינימליות של v כל $b_i - \tau(b_i) = 0$ ($\forall \tau \in G$)

\updownarrow

$$b_i = \tau(b_i)$$

הגדרה 0.10 שדה ביניים בתוך E/F הוא שדה L כך ש $F \subseteq L \subseteq E$

המשפט היסודי (השני) של תורת גלואה

יש התאמה חח"ע ועל בין $\{$ שדות הביניים של הרחבות גלואה E/F ותת חבורות של $G = \text{Gal}(E/F)$ לפי $L \mapsto \text{Gal}(E/L), H \mapsto E^H$

תוספת:

ואז: $\text{Gal}(E/L) \triangleleft \text{Gal}(E/F) \Leftrightarrow$ הרחבת גלואה L/F
 $\text{Gal}(L/F) \cong \text{Gal}(E/F)/\text{Gal}(E/L)$

תורת גלואה-הרצאה 7

בשיעור הקודם הוכחנו

1. עבור E/F הרחבת גלואהת אם $E^G = F$ אז $\text{Gal}(E/F) = G$

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

משפט 0.1 יש התאמה 1:1 בין שדות הביניים $F \subset L \subset E$ ותת חבורות של $G = \text{Gal}(E/F)$ לפי $L \mapsto \text{Gal}(E/L)$ ו $H \mapsto E^H$.

הוכחה: צ"ל:

1. $E^{\text{Gal}(E/L)} = L$

2. $\text{Gal}(E/E^H) = H$

אבל אם כותבים F במקום L , H במקום G אז כבר הוכחנו את הטענות האלו במשפט היסודי הראשון ומקבלים את (2). את (1) מקבלים מטענה מלפני שני שיעורים. לסיכום, ההרכבות של ההתאמות הם הזהות בשני הכיוונים ולכן שניהם חח"ע ועל. נשים לב: $E^{H_2} \subseteq E^{H_1} \Leftrightarrow H_1 \subseteq H_2$ ■

הערה 0.2 נניח $F \subseteq L \subseteq E$, אזי $L = E$ $\Leftrightarrow \text{Gal}(E/L) = \{1_E\}$

הערה 0.3 נניח $F \subseteq L \subseteq E$ ו $\tau \in G = \text{Gal}(E/F)$,

$$\tau(L) = \{\tau(a) : a \in L\}$$

גם תת שדה של E .

הוכחה:

$$\tau(a \pm b) = \tau(a) \pm \tau(b)$$

$$\tau(ab^{-1}) = \tau(a)\tau(b)^{-1}$$

נכתוב $H \leq G_2, L = E^H$

$$L = \{a \in E : \sigma(a) = a \quad \forall a \in H\}$$

$$(\tau\sigma\tau^{-1})\tau(a) = \tau\sigma(a)$$

לכן

$$(\tau\sigma\tau)\tau(a) = \tau(a) \Leftrightarrow \sigma(a) = a$$

הוכחנו $a \in E^H$ אממ

$$\tau(a) \in E^{\tau H \tau^{-1}} = \{a \in E : \tau\sigma\tau^{-1}(a) = a \quad \forall \sigma \in H\}$$

■

מסקנה 0.4 $\forall \tau \in G \quad \tau(L) = E^{\tau H \tau^{-1}}$

משפט 0.5 $F \subseteq L \subseteq E$ הרחבת גלואה, אזי L/F הרחבה נורמלית $\Leftrightarrow \text{Gal}(E/L) \triangleleft \text{Gal}(E/F)$ ואז $\text{Gal}(E/F)$

$$\text{Gal}(L/F) \cong \text{Gal}(E/F) / \text{Gal}(E/L)$$

הוכחה: (\Leftarrow) נכתוב $E = \text{Gal}(E/L)$ אם $H \triangleleft G = \text{Gal}(E/F)$ אז $\tau H \tau^{-1} \triangleleft G$ לכן

$$\tau(L) = E^{\tau H \tau^{-1}} = E^H = L$$

כי H נורמלית ולכן סגורה להצמדה. ניקח $a \in L, \tau(a) \in L, \forall \tau \in G$. ניקח

$$f = \prod_{\text{different}} (\lambda - \tau(a))$$

הוכחנו למה שאומרת ש $f \in F[\lambda]$ לכן F מתפצל בתוך L , $L \Leftarrow F$ נורמלי מעל F כי $f(a) = 0$ הפולינום המינימלי מחלק את f לפי הגדרת פולינום מינימלי.

(אפשר להגיד מההוכחה ש L/F נורמלי $\Leftrightarrow \tau(L) = L \quad \forall \tau \in G$)

(\Rightarrow) נניח L/F הרחבה נורמלית.

צ"ל: $\tau \in G$ לכל $\tau H \tau^{-1} = H$.

$\tau(a)$ הוא שורש של הפולינום המינימלי של a כי $\tau(a)$ שורש $\hat{t}(f) = f$ כי $f \in f[\lambda]$.

נתון ש f מתפצל ל $f = \prod (\lambda - a_i)$, $a_i \in L$, לכן פירוק יחיד $\lambda - \tau(a)$ הוא אחד
 מה $\lambda - a_i$, לכן $\tau(a) = a_i \in L$. הוכחנו $\tau(L) = L$,
 $E^{\tau H \tau^{-1}} = \tau(L) = L = E^H$

$$\tau H \tau^{-1} = \text{Gal}(E/E^{\tau H \tau^{-1}}) = \text{Gal}(E/E^H) = H \quad \forall \tau \in G, H \triangleleft G$$

מסקנה מההוכחה עד כאן:

$$\forall \tau \in G \quad \tau(L) = L \Leftrightarrow \text{הרחבה נורמלית } L/F$$

$$\text{Gal}(L/F) \cong \text{Gal}(E/F)/\text{Gal}(E/L)$$

נרצה להשתמש במשפט נתר (משפטי האיזומורפיזם) בכך שנמצא הומו' מ $\text{Gal}(E/F)$ ל $\text{Gal}(L/F)$ שגרעינו $\text{Gal}(E/L)$. נגדיר:

$$\Phi : \text{Gal}(E/F) \rightarrow \text{Gal}(L/F)$$

ע"י

$$\Phi(\sigma) = \sigma|_L$$

כאשר $\sigma|_L$ אוטו' של L כי הוכחנו $\sigma(L) = L$.

$$\ker \Phi = \{\sigma \in G : \sigma|_L = 1_L\} = \text{Gal}(E/L)$$

לכן Φ נותן שיכון

$$\text{Gal}(E/F)/\text{Gal}(E/L) \xrightarrow{\sim} \text{Gal}(L/F)$$

אבל

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

לכן

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

כלומר Φ על. ■

שדות סופיים

זוכרים:

משפט 0.6 אם E שדה סופי אז $\text{char}(E) = p > 0$ ראשוני, וקיים שיכון $\mathbb{Z}/p \hookrightarrow E$,
|E| = p^t בסיס אז b_1, ..., b_t.

הוכחה: $E = \left\{ \sum_{i=1}^t m_i b_i : m_i \in \mathbb{Z}/p \right\}$. בוחר t פעמים.
סה"כ $p^t = p \cdot \dots \cdot p$.

משפט 0.7 אם E שדה סופי ו $|E| = p^t$ אז $E/\{0\}$ חבורה ולכן $a^{p^2-1} = 1$ $\forall a \neq 0$
(לגרנז')
 $\forall a \ a^{p^t} = a \iff$

משפט 0.8 $E/\{0\}$ חבורה צקלית

הוכחה: בקורסים קודמים. משתמשים במשפט היסודי של חבורות אבליות.

למה 0.9 כל איבר של E הוא שורש של הפולינום $f = \lambda^{p^t} - \lambda$, לכן E שדה פיצול של
הפולינום f מעל \mathbb{Z}/p .
 $f' = p^t \lambda^{p^t-1} - 1 = -1 \neq 0$ כי ספרבילי כי $-1 \neq 0$

הוכחנו: $E/\mathbb{Z}/p$ הרחבת גלואה. מהו $G = \text{Gal}(E/\mathbb{Z}/p)$?

0.10 הגדרה ההומומורפיזם של פרובניוס הוא $\sigma_p : E \rightarrow E$ המוגדר ע"י:

$$\sigma_p(a) = a^p$$

הוכחה: נראה שזה אכן הומומורפיזם.

$$\sigma_p(ab) = (ab)^p = a^p b^p = \sigma_p(a) \sigma_p(b)$$

$$\sigma_p(a+b) = (a+b)^p = a^p + b^p = \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} = a^p + b^p = \sigma_p(a) + \sigma_p(b)$$

לכן σ_p הומו,

$$\sigma_p(a)^t = (a^p)^{p \cdot \dots \cdot p} = a^{p^t} = a$$

$$a_p^t = 1_E$$

■ לכן σ_p אוטומורפיזם ו $o(\sigma_p) | t$

$$o(\sigma_p) = t \quad \text{טענה 0.11}$$

הוכחה: אם $o(\sigma_p) = m | t$ אז $a^{p^m} - a = 0$ לכל m . כלומר, כל איבר של E שורש של הפולינום $\lambda^{p^m} - \lambda$ לכן E בכל p^t שורשים של פולינום מדרגה p^m , לכן

$$t = m \Leftrightarrow t \leq m \Leftrightarrow p^t \leq p^m$$

■

מסקנה 0.12 $\langle \sigma_p(t) \rangle$ תת חבורה של G מסדר t .

הוכחה: נגדיר:

$$\bar{E} = E^{\langle \sigma_p^t \rangle} \leq E$$

הוא בדיוק השורשים של $\lambda^{p^t} - \lambda$.

$$E/\mathbb{z}/p$$

הרחבת גלואה עם חבורת גלואה $\langle \sigma_p \rangle$ ואז $|\langle \sigma_p \rangle| = p^t$ ו $|\text{Gal}(\bar{E}/\mathbb{z}/p)| = |\langle \sigma_p \rangle| = p^t$ לכן $|\bar{E}| = p^t$ ולכן $\bar{E} = E$

■

תורת גלואה – הרצאה 8

חזרה

שלוש העובדות המרכזיות לגבי שדות סופיים:

1. אם $K \subseteq E$ שדות סופיים ו $[E : K] = t$ אז $|E| = |K|^t$. למשל, אם $K = \mathbb{Z}/p\mathbb{Z}$ ו $p = \text{char}(E)$ אז $|E| = p^t$.

2. אם $|E| = n = p^t$ אז E שדה פיצול של הפולינום $\lambda^p - \lambda$ ולכן $E/\mathbb{Z}/p$ הרחבת גלואה.

3. במאפיין p , קיים הומו' (פרוביניוס) $\varphi_p : a \mapsto a^p$ ולכן $\varphi_p \in G := \text{Gal}(E/\mathbb{Z}/p)$.

0.1 הערה $E^{\langle \varphi_p \rangle} = \{a \in E : a^p = a\} = \mathbb{Z}/p$ לפי המשפט הכבד לפי טענה קודמת $G = \langle \varphi_p \rangle$ לכן

$$|\varphi_p| = [E : \mathbb{Z}/p] = t$$

0.2 הערה

$$E^{\langle \varphi_p^m \rangle} = [a | a^{p^m} = a]$$

0.3 הערה תת החבורות של $\langle \varphi_p \rangle$ הם בדיוק $\langle \varphi_p^m \rangle$ כאשר $m|t$. לכן, תת השדות של E הם בדיוק $\{a : a^{p^m} = a\}$ עבור $m|t$ כלשהו.

דוגמא

$\lambda^2 + \lambda + 1$ אי פריק מעל $\mathbb{Z}/2$ לכן $\langle \lambda^2 + \lambda + 1 \rangle / \langle \lambda \rangle$ שדה מסדר $2^2 = 4$

משפט 0.4 לכל t ולכל מספר ראשוני p קיים שדה E מסדר p^t
הוכחה: נגדיר \tilde{E} להיות שדה הפיצול של $\lambda^{p^t} - \lambda$ מעל \mathbb{Z}/p . נגדיר

$$E := \tilde{E} \langle \varphi_p^t \rangle$$

נשים לב של $\lambda^{p^t} - \lambda$ הוא ספרבילי כי הנגזרת היא -1 , ולכן כל השורשים של E שונים
 ■ ולכן $|E| = p^t$. בסוף $\tilde{E} = E$ ולכן $\text{Gal}(E/\mathbb{Z}/p) = \langle \varphi_p \rangle$ שמסדר φ_p^t

דוגמא

נכתוב $\lambda^{p^t} - \lambda$ כמכפלת פולינום אי פריקים.
 מצד שני, נניח $g \in \mathbb{Z}/p[\lambda]$ פולינום אי פריק שמחלק את $\lambda^{p^t} - \lambda$ ו $K = \mathbb{Z}/p[\lambda]/\langle g \rangle$.
 כל שורש של g הוא שורש של $\lambda^{p^t} - \lambda$ ולכן אייך ל E .
 $K = E^{\langle \varphi_p^m \rangle} = \{a \in E : a^{p^m} = a\} \Leftarrow K \subseteq E \Leftarrow$ עבור איזשהו m .

דוגמא

$$p = 2, \quad t = 4$$

$$\lambda^{16} - \lambda = \lambda(\lambda + 1)(\lambda^2 + \lambda + 1) \cdot g(x)$$

משיקולי דרגה, $g(x)$ צריך להיות מכפלה של שלושה פולינומים אי פריקים ממעלה 4.
 המועמדים לתפקיד הרם הם:

$$\begin{cases} \lambda^4 + \lambda^3 + 1 \\ \lambda^4 + \lambda^2 + 1 \\ \lambda^4 + \lambda + 1 \\ \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1 \end{cases}$$

אבל, נשמ לב שהפולינום השני הוא בעצם

$$(\lambda^2 + \lambda + 1)^2 = \varphi_2(\lambda^2 + \lambda + 1) = \varphi_2(\lambda^2) + \varphi_2(\lambda) + \varphi_2(1) = \lambda^4 + \lambda^2 + 1$$

לכן, $g(x)$ היא המכפלה של כולם חוץ מהשני, שפריק.

הערה 0.5 פרופסור רואן אוהב לתת תרגילים כאלה במבחן (:

הרחבות ציקלוטומיות

בדרך כלל $\text{char } F = 0$, כי $\lambda^p - 1 = (\lambda - 1)^p$ כאשר $\text{char } F = p$

למת גאוס

אם $f, g \in \mathbb{Q}[\lambda]$ מתוקנים ו $f, g \in \mathbb{Z}[\lambda]$ אז $f, g \in \mathbb{Z}[\lambda]$.

השאלה המרכזית

נניח ρ שורש n -פרימיטיבי של 1 ($\rho^n = 1, \rho^m \neq 1$ לכל $0 < m < n$) אז מה המבנה של $F[\rho]$? במיוחד כאשר $F = \mathbb{Q}$.
ידוע ש

$$\lambda^n - 1 = \prod_{1 \leq k \leq n} (\lambda - \rho^k)$$

סיבה כל p^k שורש של $\lambda^n - 1$ ויש n שורשים כי הם פרמיטיביים, כלומר שונים. לכן, $F[\rho]$ הוא שדה הפיצול של הפולינום $\lambda^n - 1$ מעל F .
נשאלות השאלות:

1. מהו הפולינום המינימלי של ρ ?

2. מהו $\text{Gal}(F[\rho]/F)$? (אז אפשר לחשב את שדות הביניים).

לפי אייזנשטיין (עם הזזה כלשהי, לדוגמה $p(z+1)$ או $p(z-1)$ וכזה), עבור $n = p$ ראשוני הפולינום $\lambda^{p-1} + \dots + 1$ אי פריק ולכן הפולינום המינימלי של ρ כי

$$\lambda^n - 1 = (\lambda - 1)(1 + \lambda + \dots + \lambda^{n-1})$$

נגדיר

$$f_n = \prod_{\substack{(k,n)=1 \\ 0 < k \leq n}} (\lambda - \rho^k)$$

נשים לב: אם $d = (k, n)$ אז $1 = (p^d)^{\frac{n}{d}}$ ו $p^k = (p^d)^{\frac{k}{d}}$ אינו שורש פרימיטיבי של 1.

דוגמא

$$\begin{aligned}f_6 &= (\lambda - \rho)(\lambda - \rho^5) \\f_3 &= (\lambda - \rho^2)(\lambda - \rho^4) \\f_2 &= \lambda - \rho^3 \\f_1 &= \lambda - 1\end{aligned}$$

נשם לב ש

$$\lambda^n - 1 = f_6 f_3 f_2 f_1$$

0.6 טענה

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

הוכחה:

$$\lambda^n - 1 = \prod \lambda - \rho^k = \prod_d \prod_{(k, \frac{n}{d})=1} \lambda - (\rho^d)^k = \prod_{d|n} f_{\frac{n}{d}}$$

■

למה 0.7 $f_n \in F[\lambda]$

הוכחה: נשם לב שאם $\varphi \in \text{Gal}(F^P/F)$ ו' ρ שורש פרימיטיבי של 1 אז $\varphi(\rho')$ גם שורש של 1, כי

$$\varphi(\rho')^n = \varphi(\rho'^n) = \rho(1) = 1$$

ואם

$$\varphi(\rho'^m) = \varphi(\rho')^m = 1$$

אז

$$\#(\rho')^{m=1}$$

עבור $m < n$. לכן,

$$f_n \in \left(F[\rho]^{\text{Gal}(F[\rho]/F)} \right) [\lambda] = F$$

■

ולכן $f_n \in F[\lambda]$, ועבור $F = \mathbb{Q}$ נקבל $f_n \in \mathbb{Q}[\lambda]$

הגדרה 0.8 הנכרא f_n הפולינום הציקלוטומי של p . $\deg f_n = \varphi(n)$ כאשר $\varphi(n)$ הוא מספר אוילר. f_n מתוקן.

טענה 0.9 אם $F = \mathbb{Q}$ אז $f_n \in \mathbb{Z}[t]$ מתוקן.
הוכחה: לפי אינדוקציה על n ,

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

לפי אינדוקציה, עבור כל $d|n$

$$\prod_{\substack{d|n \\ d \neq n}} f_d \in \mathbb{Z}[\lambda]$$

מתוקן.

לכן, לפי למת גאוס $f_n \in \mathbb{Z}[\lambda]$

■

משפט 0.10 f_n אי פריק כאשר $F = \mathbb{Q}$

דוגמא

$$\lambda^6 - 1 = (\lambda - 1)(\lambda + 1)(\lambda^2 + \lambda + 1)f_6 = f_1 f_2 f_3 f_6$$

. $\varphi(6) = 2$, לבדוק ש $f_6 = \lambda^2 - \lambda + 1$

$$\lambda^{12} - 1 = f_1 f_2 f_3 f_4 f_6 f_{12}$$

תורת גלואה- הרצאה 9

ρ_n שורש n -פרמיטיבי של 1 . $F = \mathbb{Q}$.
 הוכחנו ש $F[\rho_n]$ הוא שדה פיצול של $\lambda^n - 1$
 $(\lambda^n - 1)$ ספרבילי כי הנגזרת שלו $n\lambda^{n-1}$ זרה ל $(\lambda^n - 1)$
 נגדיר

$$f_n := \prod_{\substack{0 \leq k \leq n \\ (k,n)=1}} (\lambda - \rho_n^k)$$

הוכחנו: $f_n \in \mathbb{Z}[\lambda]$ מתוקן מדרגת מספר אוילר של n .

משפט 0.1 f_n אי פריק מעל \mathbb{Q}

הערה 0.2 אם $\mathbb{Q} \subset F \subseteq F(\rho_n)$ אז $\deg f < [F(\rho_n) : F]$ ולכן f פריק.

הוכחה: אחרת, $f_n = gh$ עבור פולינומים g, h מתוקנים מדרגה גדולה מ-1, כאשר g אי פריק.

אפשר לקחת $g, h \in \mathbb{Z}[\lambda]$ לפי למת גאוס.

נעיר כי f_n, g, h כולם ספרבילים, כלומר ללא שורשים כפולים.

השורשים של g ו- h :

$$g : \rho_n^{q_1} \rho_n^{q_2} \dots \rho_n^{q_{i-1}}$$

$$h : \rho_n^{k_1} \rho_n^{q_1} \dots \rho_n^{q_{i-1}}$$

נניח השורשים של f_n הם

$$\rho_n^k : (k, n) = 1$$

נכתוב $k_1 = p_1 \dots p_n$. כל מספר ראשוני p_j זר ל n כי k_1 זר ל n .

$$q_j := \rho_1 \dots \rho_j$$

לכן, קיים l כך ש $\rho_n^{q_{l-1}}$ שורש של g ו $\rho_n^{q_l}$ שורש של h .

$$q_l = \rho_l q_{l-1}$$

נגדיר $p = \rho_n$ שורש של g .

$$\rho_n^{q_l} = \rho_n^{q_{l-1} - \rho_l} = \rho^{p_l}$$

נגדיר $p = \rho_l$ אז ρ שורש של g , ρ^p שורש של h .
 נכתוב עבור התמונה הטבעית $\mathbb{Z} \rightarrow \mathbb{Z}/p$, $\mathbb{Z}[\lambda] \rightarrow (\mathbb{Z}/p)[\lambda]$, לפי $\lambda \mapsto \bar{\lambda}$.
 $\bar{f} = \bar{g}\bar{h}$, $f \mapsto \bar{f}$
 (\bar{f} הוא f כשלקחנו את כל המקדמים מודולו p)
 $h(\lambda^p) = \sum m_i \lambda^{pi} = 0 \iff h = \sum m_i \lambda^i$
 קיבלנו ש $h(\lambda^p)$, g , אינם זרים ב $\mathbb{Z}[\lambda]$.
 נכתוב $\tilde{h} = h(\lambda^p)$
 אם $s = (g, \tilde{h})$ אינו קבוע ב $\mathbb{Z}[\lambda]$, \bar{s} אינו קבוע ב $\mathbb{Z}[\lambda]$ אבל מחלק את \bar{g} ו
 $\bar{\tilde{h}} = \overline{h(\lambda^p)} = \bar{h}^p$

$$\bar{\tilde{h}} = \sum [m_i] \lambda^{pi} = \sum [m_i] (\lambda^i)^p = \sum ([m_i] \lambda^i)^p = \left(\sum [m_i] \lambda^i \right)^p = \bar{h}^p$$

לכן \bar{g} ו \bar{h}^p אינו זרים, לכן $\bar{g} \bar{h}$ אינם זרים (מעל \mathbb{Z}/p) ולכן \bar{f} אינו ספרבילי.
 אבל $\overline{\lambda^n - 1} \mid \overline{f \lambda^n - 1}$ אינו ספרבילי (מעל \mathbb{Z}/p).

$$0 \neq \bar{n} \lambda^{n-1} = (\overline{\lambda^n - 1})'$$

כי p זר ל n כן זר ל $\overline{\lambda^n - 1}$ לכן $\overline{\lambda^n - 1}$ ספרבילי, לכן $\overline{f_n}$ ספרבילי, בסתירה. ■

0.3 מסקנה $\text{Gal}(\mathbb{Q}(\rho_n)/\mathbb{Q}) \cong u_n$.

הוכחה: לכל k זר ל n נגדיר:

$$\sigma_k : \rho \mapsto \rho^k$$

$$\sigma_{k_1} \sigma_{k_2}(\rho) = \left(\rho^{k_2} \right)^{k_1} = \rho^{k_1 k_2} = \sigma_{k_1 k_2}(\rho)$$

לכן $k \mapsto \sigma_k$ הומו'. הוא חח"ע כי אם

$$((k, n) = 1) \quad \rho^k = \rho$$

אז

$$k = 1 \iff k - 1 = 0 \iff \rho^{k-1} = 1$$

$$|\sigma_k|(k, n) = 1| = |u_n|$$

לכן

$$\text{Gal}(\mathbb{Q}(\rho_n)/\mathbb{Q}) = u_n$$

נזכור כי u_n חבורה אבלית ויודעים את המבנה, לכן יודעים כל שדה ביניים בין \mathbb{Q} ל $\mathbb{Q}(\rho_n)$ לפי התאמת גלואה. ■

משפט שטייניץ

הרחבה סופית K/F ספרבילית אם ורק אם יש מספר סופי של שדות בין K ל F

הוכחה: (\Leftarrow)

ניקח $K = F[a_1, \dots, a_n]$

$f_i \in F[\lambda]$ הפולינום המינימלי של a_i .

F = מכפלה של ה f_i בלי כפילויות.

E = שדה פיצול של f

לפי ההגדרה $\text{Gal}(E/F)$ סופית \Leftarrow יש מספר סופי של שדות ביניים בין E ל F . קל

■

וחומר בין K ל F .

הגדרה 0.4 נאמר ששדה F הוא מושלם/תמים (perfect) אם כל הרחבה ממימד סופי של F היא ספרבילית.

דוגמאות

1. אם $\text{char}(F) = 0$ אז F מושלם. (עשינו מזמן)

2. אם $|F| < \infty$ ו $F \subseteq E$ ולכן E שדה פיצול של $\lambda^{|E|} - 1$, ולכן גלואה מעל F .

המשפט היסודי של האלגברה: \mathbb{C} סגור אלגברית

רקע נדרש מתורת החבורות

1. משפט סילו: לכל חבורה G יש תת חבורה p -סילו לכל ראשוני שמחלק את $|G|$.
2. אם $|G| = p^n$ אז G חבורה פתירה (יותר טוב, $|Z(G)| > 1$).

נרצה להוכיח

שכל פולינום אי פריק מעל \mathbb{C} הוא מהצורה $\lambda - \alpha$ כאשר $\alpha \in \mathbb{C}$, כלומר כל פולינום מעל \mathbb{C} מתפצל. במילים אחרות, אם $[K : \mathbb{C}] < \infty$ אז $K = \mathbb{C}$.

הוכחת המשפט

נפצל לשני מקרים.

מקרה ראשון: $K = \mathbb{C}[a] \Leftrightarrow [K : \mathbb{C}] = 2$

כאשר $a^2 \in \mathbb{C}$. אפשר להוכיח ש $a \in \mathbb{C}$ לפי כך שנפתור משוואות. אבל, יותר מהר, אם $a^2 = re^{i\theta}$, אז אפשר לקחת $a = \sqrt{r}e^{i\frac{\theta}{2}} \in \mathbb{C}$, לכן יש שורש בתוך \mathbb{C} .

מקרה שני: אם $[K : \mathbb{R}]$ אי זוגי אז $K = \mathbb{R}$

ניקח $a \in K$, $\deg a | [K : \mathbb{R}]$. לכן הפולינום המינימלי $f_a \in \mathbb{R}[\lambda]$ מתוקן אי זוגי. f_a חותך את ציר ה x לכן יש ל f_a שורש c ב \mathbb{R} . $(\lambda - c) | f_a$ אבל f_a אי פריק לכן $f_a = \lambda - c$

תורת גלואה – הרצאה 10

המשך הוכחת המשפט היסודי של האלגברה

אם $[K : \mathbb{C}] < \infty$ אז $K = \mathbb{C}$

הראנו שתי למות:

1. אין הרחבה ריבועית של \mathbb{C}

2. אין הרחבה אי זוגית של \mathbb{R}

קעת נוכיח את המשפט. נניח שאינו מתקיים וניח $a \in K/\mathbb{C}$. ניקח $f \in \mathbb{C}[\lambda]$ הפולינום המינימלי של a מעל \mathbb{C} . נשם לב לכך ש $f\bar{f} \in \mathbb{R}[\lambda]$ כאשר \bar{f} ההצמדה של הפולינום f . ניקח E שדה הפיצול של $f\bar{f}$ מעל \mathbb{R} . נגדיר $G = \text{Gal}(E/\mathbb{R})$. נסמן ב H תת חבורה 2-סילו של G .

$$[E^H : \mathbb{R}] = \frac{|G|}{|H|}$$

כי $[E : E^H] = |H|$ ומהתאמת גלואה. נעיר שביטוי זה כמובן אי זוגי מהגדרת H , ומלמה $E^H = \mathbb{R}$ ולכן $|H| = 2$. מכאן, נקבל ש $H = G$ לפי התאמת גלואה, אבל H היא חבורה מסדר שהוא חזקה של 2. נגדיר:

$$H_1 = \text{Gal}(E/\mathbb{C}) < H$$

לפי התאמת גלואה.

$$|H_1| = \frac{|H|}{2}$$

גם חזקת 2. לכן, קיים

$$H_1 > H_2 > \dots H_z = \{e\}$$

כאשר לכל i

$$[H_i : H_{i-1}] = 2$$

כלומר

$$|H_2| = \frac{|H_1|}{2}$$

$$[E^{H_2} : \mathbb{C}] = [H_1 : H_2] = 2$$

בניגוד ללמה 1 שאומרת שאין הרבה ריבועיות של \mathbb{C} .
כעת נעבור להוכיח את שתי גולות הכותרת של הקורס: פתרון הבעיות של ימי קדם וההוכחה לכך שלא ניתן למצוא נוסחה לפתרון משוואה ממעלה חמישית ומעלה.

הגדרה 0.1 הרחבה $K \supset F$ היא **שורשת- p** אם $K = F[a]$ כאשר $\alpha = a^p$ (חושבים על a כעל $\sqrt[p]{\alpha}$).

הגדרה 0.2 $L \supset F$ הרחבה **רדיקלית** (p_1, \dots, p_n) אם קיימת סדרת הרחבות שורשיות

$$F = F_0 \subset F_1 \subset \dots \subset F_t = L$$

כך שכל F_i הוא הרחבה שורשית עבור p_{j_i} עבור $j_i \in \{p_1, \dots, p_n\}$ אומרים ש $a \in E$ פתיר לפי רדיקלים אם $F[a]$ מוכל הרחבה רדיקלית L מעל F .

דוגמא

נניח a בעל בנייה מעל \mathbb{Q} , אז קיימת סדרה

$$\mathbb{Q} = F_0 \subset F_1 \subset \dots \subset F_t$$

כך ש $[F_{i+1}, F_i] = 2$ ו $a \in F_t$.
אבל, אם $[K : F] = 2$ ו $\frac{1}{2} \in F$ אז $K = F[\sqrt{a}]$ לאיזשהו $\alpha \in F$.

הוכחה: לפי הנוסחה הריבועית $K = F[a]$ שורש של $\lambda^2 + b\lambda + c$, $a = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$,
 $K = F[\sqrt{b^2 - 4c}]$

ולכן F_t הוא רדיקלי-2 מעל \mathbb{Q} .

האתגר:

איך להפעיל את הרחבות גלואה? (לא דרשנו שזוהי הרחבת גלואה).
 נניח למשל ש K הרחבה רדיקלית של F ונניח K/F ספרבילי (למשל, אם $\text{char } f = 0$).

לוקחים את E להיות הסגור הנורמלי של F , כלומר נכתוב $K = F[a_1, \dots, a_n]$, ונניח f_i הפולנום המינימלי של a_i , אז נרשום

$$f = \prod f_i$$

ללא כפילויות (ע"מ שיהיה ספרבילי). E הוא שדה הפיצול של f .
 צריכים תת שדה E_1 כך ש $\sigma(E_1) = E_1$ לכל $\sigma \in G$, אז E_1/F הוא הרחבת גלואה.

רוצים E_1/F הוא רדיקלי $\{p_1, \dots, p_n\}$ וכן K/F הוא רדיקלי $\{p_1, \dots, p_n\}$.
 נכתוב $F = F_0 \subset F_1 \subset \dots \subset F_t = K$, כאשר $F_{i+1} = F_i[a_{i+1}]$

$$\alpha_i = a_{i+1} \in F_i$$

נכתוב $G = \{\sigma_1, \dots, \sigma_m\}$ כאשר $\sigma_1 = 1_E$.

$$\sigma(F) = F \subset \sigma(F_1) \subset \dots \subset \sigma(F_t) = \sigma(K)$$

$$\sigma(F_{i+1}) = \sigma(F_i)[\sigma(a_{i+1})]$$

$$\sigma(a_{i+1})^{p_{i+1}} = \sigma(a_{i+1}^{p_{i+1}}) = \sigma(\alpha_i) \in \sigma(F_i)$$

$$F \subset F[a_1] = F[\sigma_1(a_1)] \subset \dots \subset K \subseteq K[\sigma_2(a_1)] \subseteq K[\sigma_2(a_1), \sigma_2(a_2)] \subset$$

$$\subset \underbrace{K_{2,3}}_{K[\sigma_2(a_1), \dots, \sigma_2(a_3)]} \subset K_{2,3} \subset \dots \subset K_{2,t} \subset K_{3,1} \subset K_{3,2} \subset \dots \subset K_{3,t} \subset$$

$$\subset \dots \subset E_1 := K_{|G|,t}$$

כאשר סמנו

$$K_{2,i} = K[\sigma_2(a_1), \dots, \sigma_2(a_i)]$$

כל $\sigma_j(a_i) \in E_1$
 כאשר לפי אינדוקציה,

$$K_{j,i} = K_{j-1}[\sigma_j(a_1), \dots, \sigma_j(a_j)]$$

לכל $\tau \in G$, $\tau(E_1)$ מקבלים לפי מגדל שבנוי מ $\tau\sigma_j(a_i)$ אבל $G = \{\tau\sigma_1, \dots, \tau\sigma_m\}$ ולכן מגיעים שוב ל E_1 .

מסקנה 0.3 נקבל מקרה פרטית לפיו אם K/F הרחבה רדיקלית-2 אז E/F גם הרחבה רדיקלית-2.

למעשה, הוכחנו את המשפט הבא:

משפט 0.4 התנאים הבאים שקולים עבור איבר $a \in \mathbb{C}$:

1. a בעל בנייה מעל \mathbb{Q} .

2. a מוכל בהרבה רדיקלית-2 מעל \mathbb{Q} .

3. a מוכל בהרחבת גלואה רדיקלית-2 מעל \mathbb{Q} .

הוכחה: $1 \Leftrightarrow 2$

לפי פתרון של משוואות קו ומעגל (עשינו בתרגול/ש"ב).

$2 \Rightarrow 3$

לפי החישוב שעשינו עכשיו

$3 \Rightarrow 2$ קל וחומר.

■

טענה 0.5 נניח E/F הרחבת גלואה, אז E/F הרחבה רדיקלית-2 $\Leftrightarrow \text{Gal}(E/F)$ חבורה (פתירה) מסדר חזקת 2.

הוכחה:

$$F \subset \underbrace{F_1}_2 \subset \underbrace{F_2}_2 \subset \dots \subset F_t = E$$

$$E^G \subset E^{G_1} \subset E^{G_2} \subset \dots \subset E^{G_t} = E$$

$$[G_i : G_{i+1}] = 2$$

$$G = G_0 \supset G_1 \supset \dots \supset G_t$$

■

פתרונות לשאלות של היוונים

1. אי אפשר לבנות אם $\sqrt[3]{2}$ כי הדרגה שלו היא 3 שאינו חזקת 2, לכן אי אפשר להכפיל את הקובייה.
2. $\cos 20^\circ$ גם מדרגת 3 כי $\frac{1}{2} = \cos 60^\circ$ וממספרי אוילר ניתן לקבל את הנוסחה $\cos^3 \theta - 3 \cos \theta = \frac{1}{2}$ עבור $\theta = 20^\circ$ שמדרגה 3 (מוכיחים שהוא אי פריק לפי אייזנשטיין). לכן, אי אפשר לחלק זווית כללית ל3 לפי בניית.
3. לריבוע מעגל צריך לבנות את $\sqrt{\pi}$, אבל π טרנסנדנטי, אבל זאת לא נוכיח כי זהו משפט קשה (כנראה של לינדשטראוס).
4. ניתן לבנות מצולע n -משוכלל \Leftrightarrow ניתן לבנות את ρ_n , כלומר $|U_n| = 2^t$. לכן ניתן לבנות ריבוע, או מחומש משוכלל, אבל לא מצולע משוכלל בעל 7 צלעות.

תורת גלואה – הרצאה 11

סגור הגלואה (הסגור הנורמלי) של הרחבה ספרבילית

$$K = F[a_1, \dots, a_n]$$

הוא שדה פיצול של

$$f = \prod f_i$$

כאשר מסירים כפילויות מהמכפלה ו f_i הוא הפולינום המינימלי של a_i .
הוכחנו: אם $G = \text{Gal}(E/F)$ אז

$$E = F[\{\sigma_i(a_j) : \sigma_i \in G, 1 \leq j \leq m\}]$$

שימוש

אם K/F הרחבה (p_1, \dots, p_t) רדיקלית אז E/F הרחבה רדיקלית.

נזכר גם בהתאמת גלואה:

אם $G = \text{Gal}(E/F)$ ו

$$G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\}$$

אז מגדירים

$$F_j := E^{G_j}$$

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

תכונות של חבורת גלואה $G = \text{Gal}(E/F)$

כאשר E סגור הגלואה של $F[a] = K$ כאשר a אלגברי מדרגה n :

1. קיים הומו'

$$G \hookrightarrow S_n$$

כי כל אוטומורפיזם פועל בתמורה של השורשים a_1, \dots, a_n בתוך E ($a_1 = a$).
למשל,

$$|G| \mid n!$$

לפי משפט לגרנז'.

2.

$$\deg a = [K : F][E : F]$$

3. יותר קונקרטי:

אם $\mathbb{Q} \leq F \leq \mathbb{R}$ אז $E \subseteq \mathbb{C}$ לפי המשפט היסודי של האלגברה. לכן, איבר של G . אם קיים שורש אי ממשי של הפולינום המינימלי של a , אז $|G|$ זוגי.

וכעת לפתרון לשאלת השאלות:

פתרון משוואה בעזרת רדיקלים

רוצים K שהוא רדיקלי $(p_1, \dots, p_t) E \Leftrightarrow$ רדיקלי.
 זה נכון \Leftrightarrow קיים $G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\}$ כך ש $|\text{Gal}(F_{i+1}/F_i)| = p_{j_i}$
 כאשר $p_{j_i} \in \{p_1, \dots, p_t\}$.

דוגמא: הרחבת קומר

נניח $K = F[a]$ כאשר $\alpha = a^p \in F$ ו $\rho_p \in F$

$$\lambda^p - \alpha = \prod_{i=0}^{p-1} (\lambda - \rho_p^i a)$$

$\sigma^j(a) = \rho_p^j a$ או $\sigma(a) = \rho_p a$ כאשר $\text{Gal}(E/F) = \langle \sigma \rangle$

$$\sigma(a^k) = (\rho_p a)^k = \rho_p^k a^k$$

לכן $a \mapsto \rho_p^j a$ נגדיר את σ^j לכן $G = \{1, \sigma, \dots, \sigma^{p-1}\} = \langle \sigma \rangle$

הערה 0.1 נניח $H \subset G$, $a \in E$ אז

$$\sum_{\sigma \in H} \sigma(a) \in E^H$$

משפט 0.2 נניח $a \in E$ ו $\text{Gal}(E/F) = \langle \sigma \rangle$ ו $p \in F$. נגדיר $\rho = \rho_p$, אז

$$\sigma(b) = \rho b$$

עבור איזשהו $b \in E$.

הוכחה:

$$b = a + \rho^{-1}\sigma(a) + \rho^{-2}\sigma^2(a) + \rho^{-3}\sigma^3(a) + \dots + \rho^{p-1}\sigma^{p-1}(a)$$

$$\sigma(b) = \rho a + \sigma(a) + \rho^{-1}(a)\sigma^2(a) + \dots + \sigma^{p-1}(a)$$

(האיבר האחרון הוא כי $\rho^p = 1$)

צ"ל: $b \neq 0$. זה נובע מכך ש ρ שורש p יחידה $\Leftrightarrow \rho^j$ שורש p יחידה. היה אפשר להשתמש ב ρ^j במקום ρ ולקחת

$$n = \sum_{i=0}^{p-1} \rho^{-ji} \sigma^j(a)$$

עבור j כלשהו, ומצליחים אלא אם זה תמיד 0.

$$\begin{pmatrix} 1 & \cdot & \cdot & \cdot & 1 \\ 1 & \rho^{-1} & \cdot & \cdot & \rho^{p-1} \\ 1 & \rho^{-2} & \cdot & \cdot & \rho^{2(p-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \rho^{p-1} & \cdot & \cdot & \rho^{(p-1)(p-1)} \end{pmatrix} \begin{pmatrix} a \\ \sigma(a) \\ \sigma^2(a) \\ \cdot \\ \sigma^{p-1}(a) \end{pmatrix} = 0$$

אבל זוהי מטריצת ונדרמונדה, ואנו יודעים שהדטרמיננטה שלה

$$\det = \prod_{i < j} (\rho^i - \rho^j) \neq 0$$

ולכן הפיך. ■

משפט 0.3 נניח F מכיל שורש p_1, \dots, p_t של 1 אז E/F הרחבה (p_1, \dots, p_t) רדיקלית $\Leftrightarrow G$ חבורה פתירה עם גורמים שהסדר שלהם נמצא ב $\{p_1, \dots, p_t\}$.

הוכחה:
נניח

$$F = F_0 \subset \dots \subset F_n = E$$

נגדיר

$$G_0 = G$$

$$G_i = \text{Gal}(E/F_i)$$

$$G_n = \{e\}$$

אז

$$G = G_0 \supset G_1 \supset \dots \supset G_n$$

$$F_i = E^{G_i}$$

$$[G_i : G_{i+1}] = [F_{i+1} : F_i] = p_{ji}$$

לכן חבורה פתירה G_n
 \Rightarrow

$$G = G_0 \supset \dots \supset G_n = \{e\}$$

כאשר

$$[G_i : G_{i+1}] = p^{j_i}$$

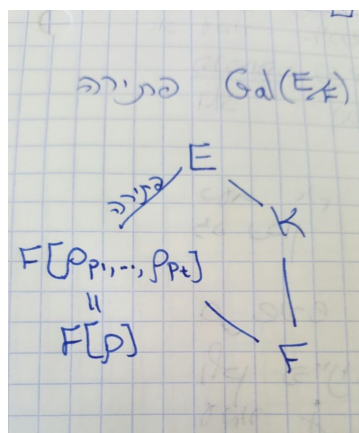
ראשוני.
 אז $F^i = E^{G_i}$

$$[F^{i+1} : F^i] = [G_i : G_{i+1}] = p_{ji}$$

כאשר p_{ji} ראשוני. לכן, הרחבת קומר (שורשית).

■

משפט 0.4 K/F הרחבה שורשית $\Leftrightarrow \text{Gal}(E/F)$ פתירה.



הוכחה:

כאשר זו הרחבה רדיקלית כי $F \ni 1 = \rho_{p_i}^{p_i}$

$$\text{Gal}(F[\rho]/F) \cong U_{p_1 \cdot \dots \cdot p_n}$$

שחבורה אבלית ולכן פתירה.

חבורה G פתירה \Leftrightarrow עבור $N \triangleleft G$, $N = \text{Gal}(E/F[\rho])$ ניקח $N = \text{Gal}(E/F[\rho])$ אז $G/N \cong \text{Gal}(F[\rho]/F)$ אבלית ולכן פתירה, זה אומר ש N פתירה $\Leftrightarrow G$ פתירה. ■

להפריך רדיקליות באופן כללי

צריך $K \supset F$ כאשר $G = \text{Gal}(E/F)$ חבורה שאינה פתירה.

דוגמא מפורסמת

יודעים ש S_n פתירה $\Leftrightarrow n < 5$. זה אומר שאפשר לפתור כל הרחבה $K = F[a]$, כי עבור $\deg a \leq 4$ אז $G \subseteq S_4$ פתירה. רוצים פולינום מינימלי $f \in \mathbb{Q}[\lambda]$ של a מדרגה 5, כאשר $G = S_5$. אנו יודעים ש $|G| \equiv 5 \pmod{5}$ מכיל איבר מסדר 5 לפי משפט קושי.

משפט 0.5 כל איבר מסדר p ביחד עם חילוף יוצר את S_p . צריך פולינום f כאשר G מכיל חילוף. מספיקה דוגמא כאשר חילוף הוא הצמדה.

כלומר, רוצים הצמדה מחליפה שני שורשים וקובעת את האחרים. רוצים 3 שורשים ממשיים של f ו 2 לא ממשיים. קל למצוא פולינום עם שני שורשים ממשיים, שיהיה גם אי פריק. ננסה לבנות לפי אייזנשטיין. ננסה

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

הוא אי פריק,

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

$$\lambda = \pm x, \quad x = \sqrt[4]{\frac{pq}{5}}$$

$$f(-x) = x\left(\frac{pq}{5} + pq\right) + p > 0$$

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

וזה שלילי כאשר $p \ll q$.