

① 13.05.08
תלמידי מתמטיקה

המחברים: דביר ורדי

mennyaka@ma...
@gmail....

המתרגלים: מני אקא

יש אתר ה- laws ויש גם קטגוריית ציון - (ציון זרוע) של עמית!

- Dummit and Foote - Abstract Algebra : ספרות
- James Milne - Galois Theory (web site)
- Ian Stewart - Galois Theory

• (הסעיף) יצא אפיון משוואה ריבועית $Ax^2 + Bx + C$
 יש נוסחה והיא נכונה כל שבה שלם אצל החלק ה- $2A$
 גם ה- $Ax^3 + Bx^2 + Cx + D$ יש נוסחה (צו מספרת).
 מצאו אותה ה- 565. ה- 1560 מצאו נוסחה לפיתרון של
 משוואה ממעלה ראשית ותקצו. במשך הזמן שנים לא הצליחו למצוא
 נוסחה לפיתרון משוואה ממעלה חמישית ואלו הם אלו יקראו
 משוואות ממעלה ח' (תמונה S_n ונראה שהיא $n=5$)
 אי אפשר למצוא נוסחה לפיתרון מכאן גם בא הנושא של
 תמונה פתירה.

• הפיתוח מתחיל וסרטן אצל החלצות לווית (תורה) זשעים היוונים
 במשך הזמן למצוא ניסוח לחוק לווית א-3, אלו מסתבר שזה סתם
 אפס...
 —

תלבויות:

- I שבה הוא תה קומוטטיבי פשוט (סוגר האידיאלים שלו הם אריוואלים)
- II R תה קומוטטיבי אז M אידיאל מקסימלי אנו R/M שבה
 (לה) (לפי) ישירות אמנם (התאמה)
- III R חוג ראשוני, p איבר אי-פסיק, אז (p) אידיאל מקסימלי
 (ה) ציאה הוא $F[X]$ (פולינומים אי-פסיק) של

המונח טאנס: R תחום פריקות יחידה F -! למה שברים
 ו (להכין \mathbb{Z} -! \mathbb{Q}). אז אם פולינום פריק משהו F
 אז הוא פריק משהו R , טומר אם פולינום אי-פריק משהו R
 אז הוא אי-פריק משהו F . (אם להראו פריק (כונן) לריק עדי תנאי)

הגדרה: אם $f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ התחלה היא
 $\text{Content}(f) = c(f) = \gcd(a_0, a_1, \dots, a_n)$

פואמה: $C(2x + 4x^2 + 6) = 2$

$C(\text{פולינום מתיקן}) = 1$

$C(4x + 6x^2) = 2$

המונח טאנס: אם $f \in \mathbb{Z}[X]$ רק ש- $C(f) = 1$ אז
 אם f אי-פריק משהו \mathbb{Z} אז הוא אי-פריק משהו \mathbb{Q} .

פואמה: אם התחלה אינה 1 להראו טאנס.

$f = 7x \in \mathbb{Z}[X]$ פריק $f = 7 \cdot x$ אבל $f = 7x$
 הוא אי-פריק משהו \mathbb{Q} כי 7 הפריק.

סיכום: בהיותו פולינום מתיקן משהו \mathbb{Z} , פולינום שברוא אי-
 פריק משהו \mathbb{Q} ומפריק, פריק משהו \mathbb{Z} .

קריטריון אי-פריקות

(1) תופש שרשים: עבור פולינום ממעלה ≥ 3 p אי-פריק משהו

F אם או שרשים F .

הסבר: α שורש של p אינה $p \mid \alpha - x$ וכן אם יש שורש

אז הוא פריק, ואם הוא פריק אז בהכרח הנגלה של אחד

מהמחלקה הוא ± 1 שיש שורש.

פואמה: $x^3 + x + 1$ אי-פריק משהו $\mathbb{Z}/2\mathbb{Z}$

② שיתוף אנך :

אנך : R חוג $I \triangleleft R$ יחיד (האידיאל הנולד) I
 $R/I[X] \cong R[X]/(I)$ אם $R[X]$ -0

הוכחה : (I) הוא אידיאל ראשוני של $R[X]$ אם I -0

הוכחה : נחמה $R = \mathbb{Z}$, יש הצגה $\mathbb{Z}[X] \rightarrow \mathbb{Z}/I[X]$

שלוקחה את \mathbb{Z} מתקשים מוצגו I , מופקים שהצגה היא
 הפיסק $I[X] = (I)$ ושההצגה היא \mathbb{Z}/I .

טענה : אם $f \in \mathbb{Z}[X]$ פולינום שפיק מותקן אז $f \in \mathbb{Z}/I[X]$
 אם $f \in \mathbb{Z}/I[X]$ אז f מן התקשים מוצגו I שפיק.

הוכחה : אם יש שפיק $f = ab$ (נתן שור a, b יחיד)

מתקנים (\mathbb{Z}) $x^2 - 3x + 2 = x \cdot (x - 2)$ ואז ישו זה f כי
 הוצגו (\mathbb{Z}) הוא את השפיק.

דוגמה : $x^3 + 2x^2 + x + 1 \in \mathbb{Z}[X]$ אי-שפיק \mathbb{Z} כי אם (\mathbb{Z})

מוצגו $\mathbb{Z}/2\mathbb{Z}$ (קטן) $x^3 + x + 1$ שפיק $\mathbb{Z}/2\mathbb{Z}$

③ 20.05.08
ג' מננים

השאלה (חלק) היא: (נתון n) - $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ עבור

p ראשוני. זה הוליווודי-טי-פיק. באופן ישיר לא נראה מה אפשר
לעשות כאן. (הרף משה"ר $(x^n - 1) = (x-1)\Phi_p(x)$ ושיים שמתקיים

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}$$

$$\Rightarrow \Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{1}$$

ואז ישו אצל אשמה מתרחין אינושטין כי $p \mid \binom{p}{i}$ א

אבל $\binom{p}{1} \not\equiv 0 \pmod{p}$. אז $\Phi_p(x+1)$ לא פיק וזה אומר ל-
 $\Phi_p(x)$ אי-פיק.

הוכחה 8

① ראוי שיהיה $(p(x))$ מתחלק את F (אם F אינו פיק) אז אפשר לומר
שהוא מתחלק את F וזהו יש ל- F שום. ההחמטה היא $F[x]/(p(x))$
והיא מתחלק את F .

② (שיים שיש $F \subseteq K$ מתקיים ל- K אחסוהטורי של F)

רצה להסבין את החסוהטורי של $K = F[x]/(p(x))$ כחסוהטורי של F .
(סמן את החסוהטורי של X אוקולו $(p(x))$ \bar{x} . טוען $\theta = X + (p(x))$
(חסוהטורי של $(\bar{x} = X + (p(x)))$)

לדוגמה: $\theta, \theta^2, \dots, \theta^{n-1}$ הם טיפס $n = \deg p$

החמטה: צריך להראות שהקבוצה פורש ונת'ם.

פירט: יהי $K = F[x]/(p(x))$. $a(x) + (p(x)) \in F[x]/(p(x)) = K$. חוקר עם שורות

$a(x) = q(x)p(x) + r(x)$ - $\deg r < \deg p$. סתרה K

מתקיים $r(x) + (p(x)) = a(x) + (p(x))$ - $r(x)$ הוא צורת סניט

ל הקבוצה (צו). שטרב משה"ר $n-1$. היות $r(x) = \sum_{i=0}^{n-1} a_i x^i$ אז

$$(r(x) + (p(x))) = \sum_{i=0}^{n-1} a_i \theta^i$$

נת'ם $\delta = a_0 + a_1 \bar{x} + \dots + a_{n-1} \bar{x}^{n-1}$ - θ חסוהטורי

$$\bar{x}^n = a_0 + a_1 \bar{x} + \dots + a_{n-1} \bar{x}^{n-1} = 0$$

$$\Rightarrow \bar{x}^n = a_0 + a_1 \bar{x} + \dots + a_{n-1} \bar{x}^{n-1} = 0$$

(4)

... $\mathbb{Q}[\sqrt{2}] / (x^2 - 2) = \mathbb{Q}[\sqrt{2}]$ (6)

ההכלאה $\alpha \in K$ היא שדה $F \subseteq K$ - השדה F של

$F(\alpha) = \{ \sum a_i \alpha^i : a_i \in F \}$ - השדה F של α

השדה α - השדה F (השדה הקטן ביותר) של α של K

$F(\alpha) \cong F[x] / (p(x))$ של K -

⑤ 24.05.2008
 ה' תשס"ח

היבט של קריאה: איזה הגדרות (התוצאות) עבר איזם החישוב בתלמוד.

φ

הפולינום המינימלי

K/F הרחבת שדה ויבוי $K \ni \alpha$ אינו אלגברי, כלומר α איננו פולינום מעל F . (תמונה הפולינום מעל F איננה מינימלית) שמאפשר את α . מהיכ הפולינום הילה מתקין.

טענה: לכו פולינום אי-פריק. f פולינום אחר המאפשר את α אחרת α נסמנו $m_{\alpha, F}$.

הוכחה: ברור שהיא אי-פריק. אם $m = fg$ אז $0 = m(\alpha) = f(\alpha)g(\alpha)$

K שדה זמק $f(\alpha) = 0$ או $g(\alpha) = 0$ וזה מסתירה מינימליות.

כעת, יבוי f פולינום שמאפשר את α . (חלק עם לראות)

$f = qm + r \quad \deg r < \deg m$

$0 = f(\alpha) = q(\alpha)m(\alpha) + r(\alpha) = r(\alpha)$

⑥ \Leftarrow מאינמימליות m נובע $r = 0$.

הסקנה: אם $F \subseteq L \subseteq K$ אז $m_{\alpha, L} \mid m_{\alpha, F}$

הסקנה: אם α אלגברי אז $F(\alpha) \cong F[X] / (m_{\alpha, F})$

הוכחה: $F[X] \xrightarrow{x \mapsto \alpha} K$
 $\ker \varphi = (m_{\alpha, F})$

שהי היבוי היא הפולינום המינימלי של α וזה ברור

⑦ $(m_{\alpha, F})$ איננה שרומית

הפולינום המינימלי הוא יחיד כי צדדו של α יחידה מתקין

אסתרה: אם יש לנו פולינום מתוקן שמאפס את α אז הוא מינימלי אם הוא פריק

דוגמה:

(1) $x^2 - 2$ אי פריק מעל \mathbb{Q} ולכן הוא מינימלי מעל \mathbb{Q} .
 נבדוק שיש שורש אחד.

(2) $m_{\mathbb{Q}, \mathbb{Q}(\sqrt{2})}(x) = x - \sqrt{2}$ (כי $\sqrt{2}$ רגור קלטה)

(שים לב ל- $x^2 - 2 \mid x - \sqrt{2}$ (לא - האסתרה היא שונה)

הרחבה ריבועית

K/F וקראת הרחבה ריבועית אם $\alpha = [K:F]$
 ופי $\alpha \in K \setminus F$ אז $F \neq F(\alpha) \subseteq K$ אפוא
 $[F(\alpha):F] = 1, 2$ (כי $F \neq F(\alpha)$ אפוא
 $F(\alpha) = K \iff [K:F] = 2$

מתי נלמד $m_{\alpha, F}$ באופן בלי, אם $K = F[x]/(f)$
 אז $[K:F] = \deg f$ ולכן $\deg m_{\alpha, F} = 2$.
 אם $\text{char } F \neq 2$ אז $m_{\alpha, F} = x^2 + bx + c$ (ניה ל-)

(*) $\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$

נשים לב שאין כאן שום מונח!

$K = F(\alpha) = F(\sqrt{b^2 - 4c})$ אסתרה:

הוכחה:

(*) נוסח נ- (א)

$2\alpha + b = \pm \sqrt{b^2 - 4c}$ (ב)

(ג)

אם הרחבה ריבועית מתקבלת ממספר שורש ריבועי!

(ניה שיש) $K/F, L/K$ אז הרחבה
 $[L:F] = [L:K][K:F]$

6) K is a field $[K:F] = p$ or ∞ (infinite)
 (a) K/F is a simple extension (exists $\alpha \in K$ such that $K = F(\alpha)$)

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt[4]{2})$: Example

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$

(b) $m_{\alpha, F(\alpha)} = x^3 - \sqrt{2}$ \leftarrow
 (The minimal polynomial of α over $F(\alpha)$)

Let $\alpha_1, \dots, \alpha_k$ be the roots of the minimal polynomial of α over F .

Let $F(\alpha, \beta) = F(\alpha)(\beta)$.

Let $n = [F(\alpha):F]$ and $d = [F(\alpha)(\beta):F(\alpha)]$.

$n = m_{\alpha, F}$ and $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$

Let $d = \deg m_{\beta, F(\alpha)}$ and $1, \beta, \beta^2, \dots, \beta^{d-1}$

Let $\alpha_i \in F(\alpha)$ and $\beta_j \in F(\alpha)(\beta)$.

$a_i \in F(\alpha) \quad a_0 + a_1 \beta + a_2 \beta^2 + \dots + a_{d-1} \beta^{d-1}$

Let $b_j \in F$ and $a_i = b_0 + b_1 \alpha + b_2 \alpha^2 + \dots + b_{n-1} \alpha^{n-1}$

$b_j \in F \quad a_i = b_0 + b_1 \alpha + b_2 \alpha^2 + \dots + b_{n-1} \alpha^{n-1}$

(The set of all $\alpha^i \beta^j$ is a basis for $F(\alpha, \beta)$ over F)

$F(\alpha, \beta) = \sum_{i=0}^{n-1} \sum_{j=0}^{d-1} c_{ij} \alpha^i \beta^j$

Let $c_{ij} \in F$ and $\{ \alpha^i \beta^j : 0 \leq i < n, 0 \leq j < d \}$ is a basis for $F(\alpha, \beta)$ over F .

Let $[F(\alpha, \beta) : F(\alpha)] = d$ and $[F(\alpha) : F] = n$.

$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)] [F(\alpha) : F] = [F(\alpha, \beta) : F]$

Let $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$: Example

Let $m_{\sqrt{3}, \mathbb{Q}(\sqrt{2})} = x^2 - 3$ \leftarrow $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$

$$\mathbb{Q}(\sqrt{2}) = \{0, 1, \sqrt{2}, \sqrt{2}\}$$

$$\mathbb{Q}(\sqrt{3}) = \{0, 1, \sqrt{3}, \sqrt{3}\}$$

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{0, 1, \sqrt{2}, \sqrt{3}, \sqrt{6}, \sqrt{6}\} \leftarrow$$

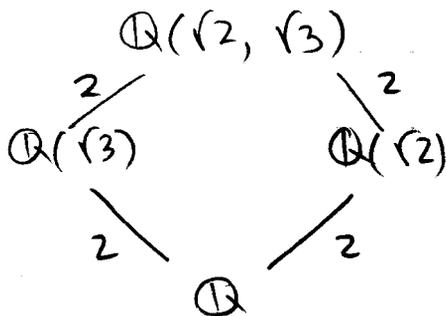
Ⓣ 3.6.08
ג' מתנים

אפשר להגיד את תרגום 3 ו-3 יום שלישי ה- 13⁰⁰ (כיתה לבחורה)

שדה הפיצול ושדה סגורים אחרים

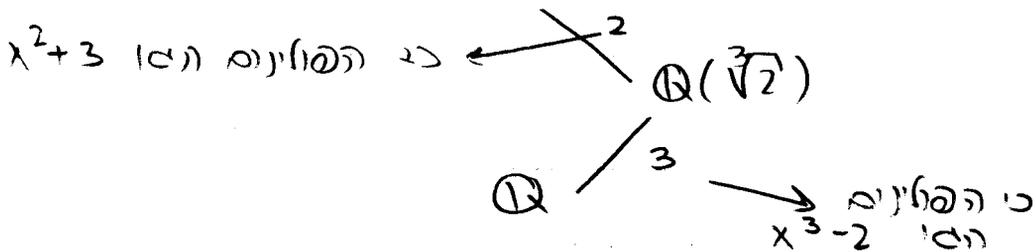
פירמוניג

- Ⓛ $x^2 - 2 \in \mathbb{Q}$ לא מתפצל ב- \mathbb{Q} אלא ב- $\mathbb{Q}(\sqrt{2})$. שדה הפיצול שלו הוא $\mathbb{Q}(\sqrt{2})$
- Ⓜ $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}$ לא מתפצל ב- $\mathbb{Q}(\sqrt{2})$ (תרגום קו- $\mathbb{Q}(\sqrt{2}) \not\subseteq \mathbb{Q}(\sqrt{3})$)
- Ⓝ $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ הוא שדה הפיצול של $x^2 - 2$ ו- $x^2 - 3$. אומרו, אומרו
המחצה הוא:

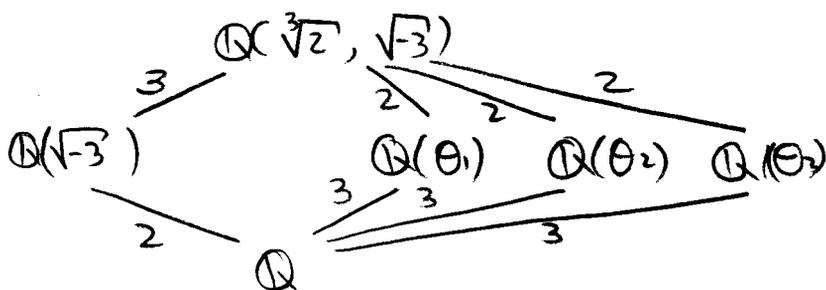


- Ⓛ $x^3 - 2 \in \mathbb{Q}$ לא מתפצל ב- \mathbb{Q} אלא ב- $\mathbb{Q}(\sqrt[3]{2})$. השורשים הם $\theta_1 = \sqrt[3]{2}$, $\theta_2 = \sqrt[3]{2} \left(\frac{-1 + i\sqrt{3}}{2} \right)$, $\theta_3 = \sqrt[3]{2} \left(\frac{-1 - i\sqrt{3}}{2} \right)$

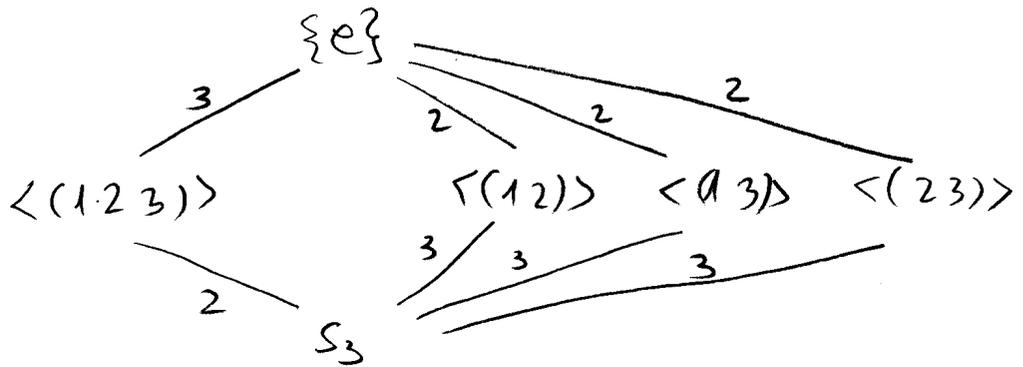
אין מחצה ב- $\mathbb{Q}(\theta_1)$ הוא שדה הפיצול של $x^3 - 2$ ב- \mathbb{R} .
אם $\sqrt{3} \in \mathbb{Q}(\theta_1)$ אז השורשים האחרים הם נוספים את $\sqrt{3}$ אז
אז יהיה נקרא $\mathbb{Q}(\theta_1, \sqrt{3}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$



סוף יש לנו את המחצה הוא:



מתחבר שאין עוד שדה בין $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$ וזה נובע מהחלפה הפס בתורת החבורה:



שדה: שדה הפיצול של x^3-2 הוא ממעלה 6 (למתלם...)

סדרה: שדה הפיצול של פולינום ממעלה n הוא ממעלה $n!$ היות $n!$ הורחה: ראש נוסף שורש ראשוני, נוסף הדרסה ממנה זה ה'גור n (שוויון ראש הפולינום אי-פסיק) נוסף שורש שני d_2 וקבל הדרסה ממנה זה ה'יותר ו- n כי הפולינום המניאלי מחוץ או הפולינום המחקרי וכן הלאה...

שורשי היתרה = שדה הפיצול של x^n-1

תלכורתם שורשי היתרה ה- n הם $e^{\frac{2\pi i k}{n}}$ $k=0,1,2,\dots,n-1$ זוהי חבורה (רמלי) ציקלית. יצר של החבורה נקרא שורש פרימיטיבי ומסומן ξ . מספר היוצרות הוא $\varphi(n)$ (פונקציית φ של אוילר)

הצדקה $\mathbb{Q}(\xi_n)$ לכו שדה הפיצול של x^n-1 וזו וקראו לה שדה החלרות (ציקלוטומי) ה- n .

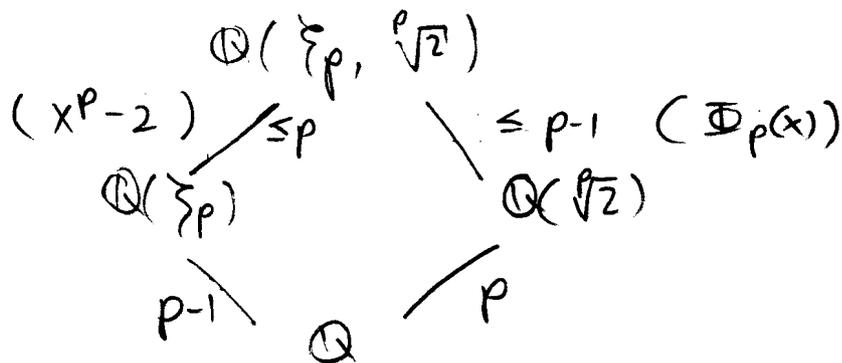
כא $p=n$ ראשני (רצה) את $\mathbb{Q}(\xi_p)$

$$\frac{x^p-1}{x-1} = \Phi_p(x) = x^{p-1} + x^{p-2} + \dots + 1$$

או-פסיק אפק המעלה היא $p-1$; $\Phi_p(x)$ זהו הפולינום המניאלי של ξ_p .

ף

(8) $\sqrt[2]{\sum_{i=1}^p i}$ ותיים
 ותמונה - $x^p - 2$ מתל \mathbb{Q} . השורשים שלו הם
 עבור $i = 0, 1, \dots, p-1$. שדה הפיצול חייב להכיל את
 פרימיטיב $\sum_{i=1}^p i$.
 (טו) שדה הפיצול הוא



נניח ששדה הפיצול הוא K . אז מילתנו חייבת לתק את p ואת
 $\mathbb{Q}(\sum_{i=1}^p i, \sqrt[2]{\sum_{i=1}^p i})$ וכן מילתנו לפחות $p(p-1)$ אכן מילתנו
 היא 6 היור $p(p-1)$ אכן לה המניחים.

הערה: את המקרה $p=3$ יתר עשינו קודם ואז מילתנו
 הפיצול של $x^3 - 2$ היא 6 וזה לא כהגלל ש- $6=3!$
 אלא כהגלל ש- $6=3 \cdot 2$

⑨ 10.6.08
 פתרון

שאלה 8 גרסא 1:

$$\begin{aligned} F_u[X] / (x^2+1) &\longrightarrow F_u[X] / (y^2+2y+2) \\ \bar{x} &\longmapsto \bar{y}+1 \end{aligned}$$

צייק, והראו שלכל איזומורפיזם.
 (תמונתו) - $F_u[X] \longrightarrow F_u[X] / (y^2+2y+2)$

$$x \longmapsto \bar{y}+1$$

כאשר התקפה של f (ההשגות)

ניתן להראות ש- $\text{Ker } f = (x^2+1)$ - מתקיים

$$x^2+1 \mid p(x) \iff p(y+1) \in (y^2+2y+2)$$

כלומר מתקיים על $y \rightarrow x-1$ (זהו β).

טענה (שנראה בהמשך) שיהיה $\text{Im } f$ סופי של \mathbb{Q} סופי
 מאוגד צדקה הן איזומורפיזם (לא תינתן אלא יחיד)

אכן $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$ (שני סופי) כלומר $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$

תרגיל 3 - אלוט - 19-21

נתונה הרחבה K/F ומציינים "אנחנו אומרים" כרגיל
 חוג שדה של $M_n(F)$ על $n = [K:F]$

$$\begin{aligned} \{1, i\} &\text{ בסיס } \mathbb{C} \text{ על } \mathbb{R} \text{ (מתחבבים)} \\ \mathbb{C} &\xrightarrow{\varphi} M_2(\mathbb{R}) \\ r &\longmapsto m_r \end{aligned}$$

טבלת m_r התקפת הנכס r -י
 $m_r(a) = ra$
 בארבעה סימטריה $m_r: \mathbb{C} \rightarrow \mathbb{C}$
 $a \mapsto ra$

\mathbb{C} של \mathbb{C} על \mathbb{R} (אנחנו אומרים) φ
 כל קומוטטיון של \mathbb{C} על \mathbb{C} - $\text{End}_{\mathbb{R}}(\mathbb{C})$ - מתקיים
 בסיס, $\mathbb{C} = \{1, i\}$

נויג e- $\alpha = a + ib$ $\alpha \in \mathbb{C}$

$$C_{\mathbb{C}}^{[m \times n]}_{\mathbb{R}} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

$$\alpha \cdot 1 = \alpha = a + bi$$

$$\alpha \cdot i = -b + ai$$

כך דובר עם \mathbb{C} נוסד של \mathbb{C} שנתר, את כראו יולאם
מספרים מכלוליים.

דוגמה (חמדה): $M_2(\mathbb{C})$ מהו אגור שגור ריבועיים
של אלוטוריים להלה.

אם זה השתמש בה"צג הלה כבי למצוא פוליומי מנימלי
של איהר.

למה, מהו הפוליומי המנימלי של $a + ib$?

$$\begin{vmatrix} x-a & b \\ -b & x-a \end{vmatrix} = x^2 - 2ax + a^2 + b^2$$

זה הפוליומי האופייני והוא מאפס את המסריצה
האופן של אפתה

$$x^2 - 2ax + (a^2 + b^2) = (x - (a+ib))(x - (a-ib))$$

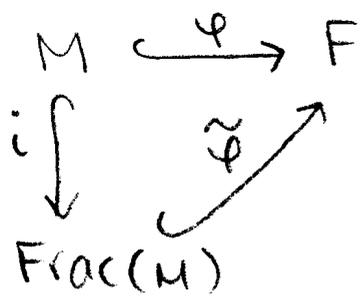
למה הפוליומי האופייני מאפס את $a+ib$.

האופן של איהר אנו הרחבה K/F אז יש ליכון

$$K \subset M_n(F) \quad \alpha \mapsto [m_\alpha] = A_\alpha$$

$p(A_\alpha) = 0$ אם $p(x) \in F[x]$ $\alpha \in K$ $p(\alpha) = 0$ $\alpha \in K$

אם n זו צרג הרחבה אז זה הפוליומי
המנימלי. $p(\alpha) = 0$.



הומומורפזם (אזכור) $\tilde{\varphi} \left(\left[\frac{r}{s} \right] \right) = \frac{\varphi(r)}{\varphi(s)}$
 (ולא ל- $\tilde{\varphi}$ מוגדרות היטב):

- $\frac{r}{s} \sim \frac{r'}{s'} \iff rs' = r's$
- $\varphi(rs') = \varphi(r's)$
 φ שלבון, טובי חתום \iff
- $\varphi(r)\varphi(s') = \varphi(r')\varphi(s)$
 φ הומומורפזם \iff
- $\frac{\varphi(r)}{\varphi(s)} = \frac{\varphi(r')}{\varphi(s')}$
 φ שלבון \iff $s, s' \neq 0$

נבדק משה גם ל- $\tilde{\varphi}$ ה מתקנה חתום.
 יותר (בדיוק) ל- $\tilde{\varphi}$ הומומורפזם של שלבון. (בדיוק) נבדק ל- $\tilde{\varphi}$

$$\tilde{\varphi} \left(\left[\frac{rr'}{ss'} \right] \right) = \tilde{\varphi} \left(\left[\frac{r}{s} \right] \right) \tilde{\varphi} \left(\left[\frac{r'}{s'} \right] \right)$$

אכן זה כן

$$\begin{aligned}
 \tilde{\varphi} \left(\left[\frac{r}{s} \right] \right) \tilde{\varphi} \left(\left[\frac{r'}{s'} \right] \right) &= \frac{\varphi(r)}{\varphi(s)} \cdot \frac{\varphi(r')}{\varphi(s')} = \frac{\varphi(r)\varphi(r')}{\varphi(s)\varphi(s')} = \\
 &= \frac{\varphi(rr')}{\varphi(ss')} = \tilde{\varphi} \left(\left[\frac{rr'}{ss'} \right] \right)
 \end{aligned}$$

מאופן דומה $\tilde{\varphi}$ משמרת גם חיבור.

$\varphi(r) = \frac{\varphi(r)}{\varphi(1)} = \tilde{\varphi} \left(\left[\frac{r}{1} \right] \right) = \tilde{\varphi} \circ i(r)$ $\forall r \in M$
 $\varphi = \tilde{\varphi} \circ i$ \iff



ל'מילים...

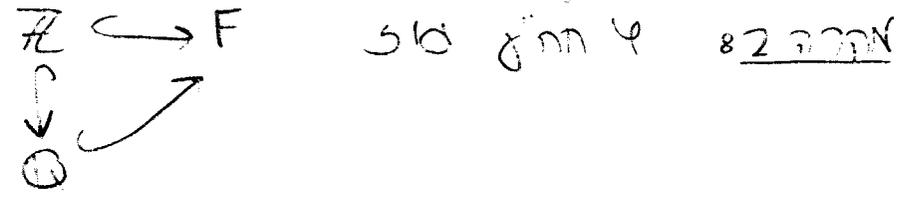
① בנייה שלבון מתחומי שלמות ומשלבות חתומים.

- $\mathbb{Q}[X] = \text{Frac } \mathbb{Q}[X]$ - תחום שלמות
- $\mathbb{Q}[X, Y] = \text{Frac } \mathbb{Q}[X, Y]$ - תחום שלמות
- ה שלבון $F(X)$ (נקודת שלבון הפונקציות הרציונליות) מן F

② שלבון ראשוניים F שלבון נוסטלר מה מתקנה

$$\begin{array}{ccc}
 \varphi: \mathbb{Z} & \longrightarrow & F \\
 n & \longmapsto & n \times 1_F
 \end{array}$$

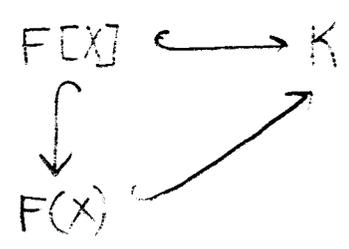
(M) $\text{Ker } \varphi = \{0\}$: 1 תוצאה
 לכל $\varphi \in F$: 2 תוצאה
 $\text{Ker } \varphi = p\mathbb{Z}$: 3 תוצאה
 לכל $p \in \mathbb{Z}$: 4 תוצאה



(0 תוצאה לכל $p \in \mathbb{Z}$) : 5 תוצאה
 Prime Fields : 6 תוצאה
 לכל $\alpha \in K$: 7 תוצאה

$$\begin{array}{ccc}
 \varphi: F[X] & \longrightarrow & K \\
 F & \xrightarrow{\text{id}} & F \\
 x & \longmapsto & \alpha
 \end{array}$$

לכל $F[X]/\text{Ker } \varphi \cong \{ \frac{f(x)}{g(x)} \}$: 8 תוצאה
 לכל $\alpha \in K$: 9 תוצאה



$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : g(\alpha) \neq 0 \right\}$$

(12) 24.06.08
ג' אדר תשס"ח

לפנינו תרגום יומים: - שאלה סופיים - קיים ויפגש

- תתחשבו על F^* (כאן צקא) -

φ

הצבה: אפואנים φ אין שורשים מרוכבים אלא (F, F') -

נתבונן בפולנום $\Phi = x^p - x$ על \mathbb{F}_p , כשה שורשים שונים של Φ

$\alpha_1, \alpha_2, \dots, \alpha_{p-1}$ שורשים, כי אלו שורשים מרוכבים. (נסתים α_{p^n})

אם K שדה הפיצול של Φ הוא $K = \mathbb{F}_p(\alpha_1, \dots, \alpha_{p-1})$.

אז $A = \{\alpha_1, \dots, \alpha_{p-1}\}$ שדה הפיצול הוא קבוצת

כש $\alpha \in A$, $\alpha^p = \alpha$ כי $\alpha \in \mathbb{F}_p$.

אם $\alpha^p = \alpha$ וכן $\beta^p = \beta$ וכו' $\alpha, \beta \in \mathbb{F}_p$.

אם $\alpha, \beta \in A$ אז $(\alpha\beta)^p = \alpha^p \beta^p = \alpha\beta$

אם $\alpha \in A$ אז $(\alpha^{-1})^p = (\alpha^p)^{-1} = \alpha^{-1}$

אם $\alpha, \beta \in A$ אז $(\alpha + \beta)^p = \alpha^p + \beta^p = \alpha + \beta$

כל $\alpha + \beta \in A$. $\Leftarrow A \subseteq K$ שדה. אלא אם $\mathbb{F}_p \subseteq A$

כי \mathbb{F}_p שדה ראשוני $\mathbb{F}_p \subseteq K$ וכן $\mathbb{F}_p \subseteq A$ וכן $A \subseteq K$ וכן $A \subseteq \mathbb{F}_p$

כל K ונתן $A = K$. אז שדה הפיצול של Φ הוא

קבוצת אלו השורשים של Φ .

\Leftarrow שדה הפיצול של Φ הוא מדרגה n על \mathbb{F}_p , n הוא

$n = [K : \mathbb{F}_p]$. אז אם n , המצוי קיים של שדה מדרגה n

על \mathbb{F}_p .

נראה שהיא יותר טובה אם F שדה מדרגה n על \mathbb{F}_p

אם $K \cong F$. אז $F^* = F \setminus \{0\}$ וכן $|F^*| = p^n - 1$.

תמונה רפואית ומהמשק (נראה שגם צקא) - אז אם $\alpha \neq 0$,

אז $\alpha^{p^n - 1} = 1$, $\alpha \in F^*$, $\alpha^{p^n} = \alpha$

אם $\alpha \in F$ אז $\alpha^{p^n} = \alpha$ שדה של Φ . הפרט, $\alpha \in \mathbb{F}_p$

אם שורש של Φ . מכיון של Φ יש שורשים שונים (וכן

על F הוא שדה הפיצול של Φ על \mathbb{F}_p . אוניברסל שדה הפיצול

(עמוד F - Φ) וקרא $F \cong H$.

מסקנה: קיים שדה M סדר p^n (קראונו n - סדר) וזה יחיד עד כדי איזומורפיזם.

משפט: יהי F שדה של n (או צוקא סופי) ותהי $G \subseteq F^*$ תת-חבורה רגולר סופית. אז G ציקלי.

למה: תהי G חבורה קומוטטיבית סופית של n יש לה כיוון n איברי מסדר n . אז G ציקלי.

* (ובעזרת המשפט כי איברי מסדר n ב- F^* הם שורשי של הפולינום $x^n - 1$ אז F שדה מסק n של תורת האלה.

יש שני הוכחות למה:

• הוכחה 1: תשלמש בקומוטטיביות ומשפט אגנה לחבורות קומוטטיביות סופיות

• הוכחה 2: לאתניה קומוטטיביות ותשלמש רק במשפט סאו (אם n מספר ראשוני אז חייבים קומוטטיביות, אם n מתקרב לאנו F שדה ונפרט קומוטטיביות)

הוכחה 1: נניח $n = p^r$ ונניח G אינה ציקלי. אז מספר כוונות p רק p - $|G| = p^r$ יש שני אמצעים ציקליים $C_p \times C_p$. הם אחד מהם יש לפחות p איברי מסדר p ואם יש לפחות p^2 איברי מסדר p , מסתבר (למה?).

הוכחה 2: נניח $|G| = p_1^{e_1} \dots p_r^{e_r}$ ונניח A_1, \dots, A_r גמי חבורות p_i -סלוא. אז $|A_i| = p_i^{e_i}$. נסמן $e_i = n_i$.

ציקלי, נסמן $p_i = p$, $e_i = n_i$. אז אם A_i לא ציקלי $p^n = |A_i| \leq 1 + p + p^2 + \dots + p^{n_i-1} + \dots + p^{n-1} < p^n$
למספר איברי מסדר n_i $\sum_{i=1}^r p^{n_i-1} = 1 + \dots + p^{n-1}$
וכן סתירה. A_i ציקלי.

(13) נסו ל- A_i נורמליות. צייק אהוביה שיש רק תבורת p_i -
 סוגה אחר לב i . (נסו n - $k+1$ אר מספר
 זה תבורת p -סוגה של $|G|$ (כי מספר זה
 תבורת p -סוגה מזהו p היה L). (נסו L - $k=0$.
 כאה יוצרים יש אהוביה צייקויה מספר $p^n - p^{n-1}$ -
 (תלבט להם) אהוביה של p -סוגה אהוביה אהוביה
 יוצרות - תהיה אהוביה, מספרה $p^n - p^{n-1}$
 $(1+kp)(p^n - p^{n-1})$
 ומספר לה היה לב תהיה p^n אהוביה $k=0$.
 $A_i \triangleleft A_j$ נורמליות. $A_i \cap A_j = 1$ אהוביה $j \neq i$
 $A_1 A_2 \dots A_r = G \triangleleft A_j$ אהוביה אהוביה
 אהוביה האהוביה הסגור $A_1 \dots A_r$ צייקויה.

(14) $C_m \times C_n \cong C_{mn}$ אהוביה $(m,n)=1$

אהוביה: F/\mathbb{F}_p תהיה אהוביה סגורה. אהוביה F אהוביה סגורה,
 אהוביה קיים $\alpha \in F$ - $\mathbb{F}_p(\alpha) = F$
 אהוביה: ניקח α אהוביה יוצר של F^* אהוביה $\mathbb{F}_p(\alpha) \subseteq F$

(15) אהוביה: $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ אהוביה α אהוביה $n \dots$

80/7/08
ג'מנים

צומאות ומחבורות גלואה והצגות של אישכ גלואה

תלכורתם K/F הרחבת גלואה
 $|Aut(K/F)| = [K:F]$
 $F = K^{Aut(K/F)}$
 מאקרה לה מסומנים
 $Aut(K/F) = Gal(K/F)$
 K/F הרחבה ספיקולרית ונורמלית
 K היא שדה פיצול של פולינום ספיקולרי $f(x) \in F[x]$

① $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ שדה הפיצול של $x^2 - 2$ אך גלואה.
 $Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{Id, \sigma\}$ נצטט שני, $\sigma(\sqrt{2}) = -\sqrt{2}$ ואלה
 הם הסקולריות אך יש שני \mathbb{Q} -אוטומורפיזמים

② הרחבה ריבוסית היא הרחבת גלואה - סצורה צומה
 ה- F -אוטומורפיזמים (היחידים של $F(\sqrt{D})/F$ הם הלחות!
 $\sqrt{D} \rightarrow -\sqrt{D}$ ולכן שדה הפיצול של $x^2 - D$
 הוא אפוא אטואגם של $F = F(\sqrt{D})^{Aut(F(\sqrt{D})/F)}$. ב האיברים
 מקובלים ע' הלחות. אך בייק אבדוק א טוקסס ע' הפיצול
 (ניה ע $- \sqrt{D} = \sigma(a + b\sqrt{D}) = a + b(-\sqrt{D}) = a - b\sqrt{D}$ כאלו ע \sqrt{D} ,
 נסיס נקס ע $- b = b \iff b = 0$
 אך שדה הלחות הוא F

③ $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. מהם ה- \mathbb{Q} -אוטומורפיזמים? איפה הלחות
 הם מהצורה $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ אך אם יוצאים את
 תמונת $\sqrt[3]{2}$ יוצאים את תמונת האיבר. $\sqrt[3]{2}$ שורש של
 הפולינום האי-ספיק $x^3 - 2$ אך חייב להיות שיש אישה אחרת
 של $x^3 - 2$ ע' ב הומומורפיזם אבל או שורשים אחרים
 ה- $\mathbb{Q}(\sqrt[3]{2})$ האחרים הם אחרים. אך $Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{Id\}$
 אבל $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ אך זו לא הרחבת גלואה.

הערות: זהו ייתר למדוק זה לא טרנסוסיבי - הרחבת אלמנטים של הרחבת אלמנטים אינה בהכרח אלמנטרל. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$

④ $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ גלואה כי היא שדה הפיצול של $(x^2-2)(x^2-3)$
 $\Leftrightarrow |\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = 4$ - ארבע האוטומורפיזמים?
 (סתם ז'אן הוורכים היוצרים?)

$\left. \begin{matrix} \sqrt{2} \rightarrow \sqrt{2} \\ \sqrt{3} \rightarrow \sqrt{3} \end{matrix} \right\} \Rightarrow \text{Id}$ אלה האוטומורפיזמים
 כג שווים של פולינום

$\left. \begin{matrix} \sqrt{2} \rightarrow -\sqrt{2} \\ \sqrt{3} \rightarrow \sqrt{3} \end{matrix} \right\} \Rightarrow \sigma$ חייב אחר לשווים של
 אתו פולינום. $\sqrt{2}$ שווים של x^2-2 ואם

$\left. \begin{matrix} \sqrt{2} \rightarrow \sqrt{2} \\ \sqrt{3} \rightarrow -\sqrt{3} \end{matrix} \right\} \Rightarrow \tau$ בהכרח $\sqrt{2}$ הולך ל- $\sqrt{2}$
 או ל- $-\sqrt{2}$.

$\left. \begin{matrix} \sqrt{2} \rightarrow -\sqrt{2} \\ \sqrt{3} \rightarrow -\sqrt{3} \end{matrix} \right\} \Rightarrow \sigma\tau = \tau\sigma$ נ"ל עבור $\sqrt{3}$
 מאחר שב ארבעה

האוטומורפיזמים האלה שונים אלה הם נלמס!
 נבין את התמונה של $\text{Gal}(K/F)$ ($K = \mathbb{Q}(\sqrt{2}, \sqrt{3}), F = \mathbb{Q}$)

כא שייג, נבין איך \mathbb{Q} אוטומורפיזם פועל על איבר \mathbb{Q} ,
 איבר \mathbb{Q} הוא מפתח $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$

אם σ יוצרים ז'אן הולכים $\sqrt{2}, \sqrt{3}$ יוצרים הם.

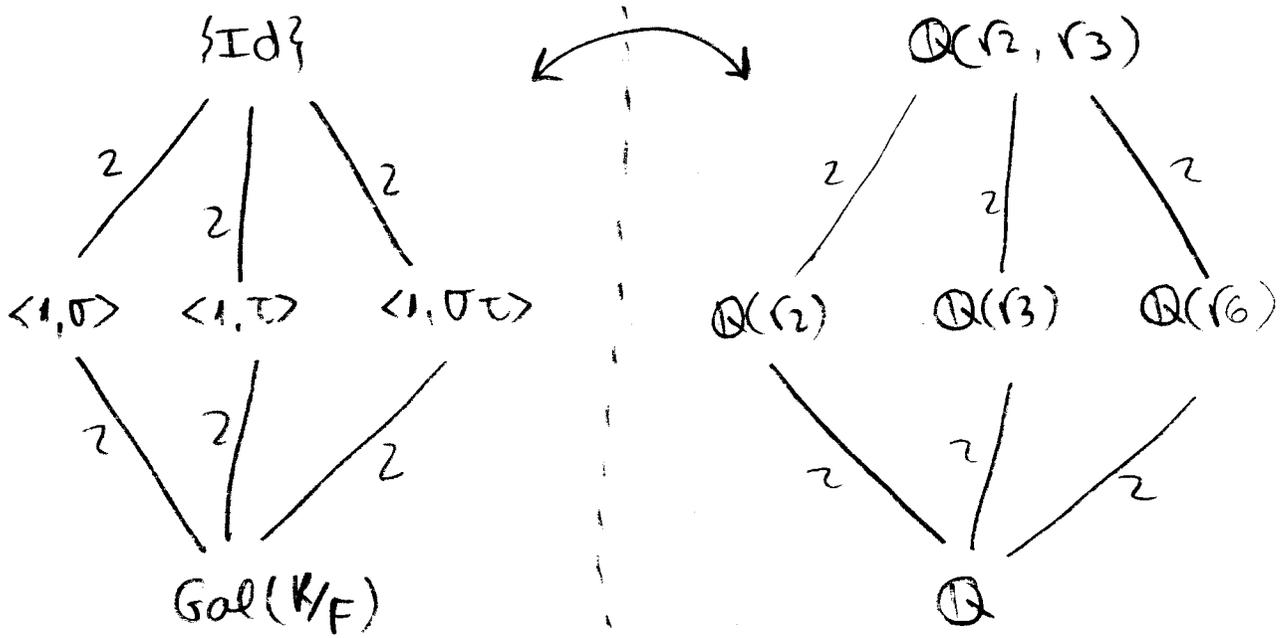
נשים לב ל- $\sigma^2 = \tau^2 = (\sigma\tau)^2 = \text{id}$. $\sigma\tau$ ממש $\text{Gal}(K/F) \cong \mathbb{Z}_2^2$

התמונה היא ציקליה מסדר 4 (Klein 4-group).

אם נסתם עליה כחבורה רגלית אז האוטומורפיזם הוא

$\tau \rightarrow (1, -1)$, $\sigma \rightarrow (1, 1)$

15



איהו שלדה הלמה של $\langle 1, \sigma \rangle$? אלה האברים הנצייק σ -
 אלסיר במקום. סומך

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = \sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) =$$

$$= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

קסאנו שווין בין ייצויים של איבר לפי הסים. אק
 שלדה הלמה של $\langle 1, \sigma \rangle$ היא $\{a + c\sqrt{3}\}$
 $b=0$ ו- $d=0$ פר

סאוויו איש שלדה הלמה של $\langle 1, \tau \rangle$ היא $\mathbb{Q}(\sqrt{3})$ ושלדה
 הלמה של $\langle 1, \sigma\tau \rangle$ היא $\mathbb{Q}(\sqrt{6})$ אפ המשט אלה
 הם ב תת השלדה!

החברה א תת החבורה בקיארמה (נורמל) כי הו
 מאינצקס 2. אך ורחבות השלדה המתאימות אלה
 הן נורמליות אמאל להם ספרתיי ההרחבות גם אלואה
 למהאז אומנו של הרחבה מסדר 2 היא נורמליות.

5) שלדה הפיזית של $x^3 - 2$ (מצים הרחבתה) הוא אלואה
 לה אמזש $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) = \mathbb{Q}(\sqrt[3]{2}, \rho)$ טש $\rho = \zeta_3$
 אהן האםלשויל אוטומורפיזם: $\sqrt[3]{2} \rightarrow \rho^2 \sqrt[3]{2}, \rho \sqrt[3]{2}, \sqrt[3]{2}$
 יש 6 אפסתיור!-6 אוטומורפיזמים (סדר ההחברה) $\rho \rightarrow \rho^2$
 (אק אלה א האוטומורפיזמים)

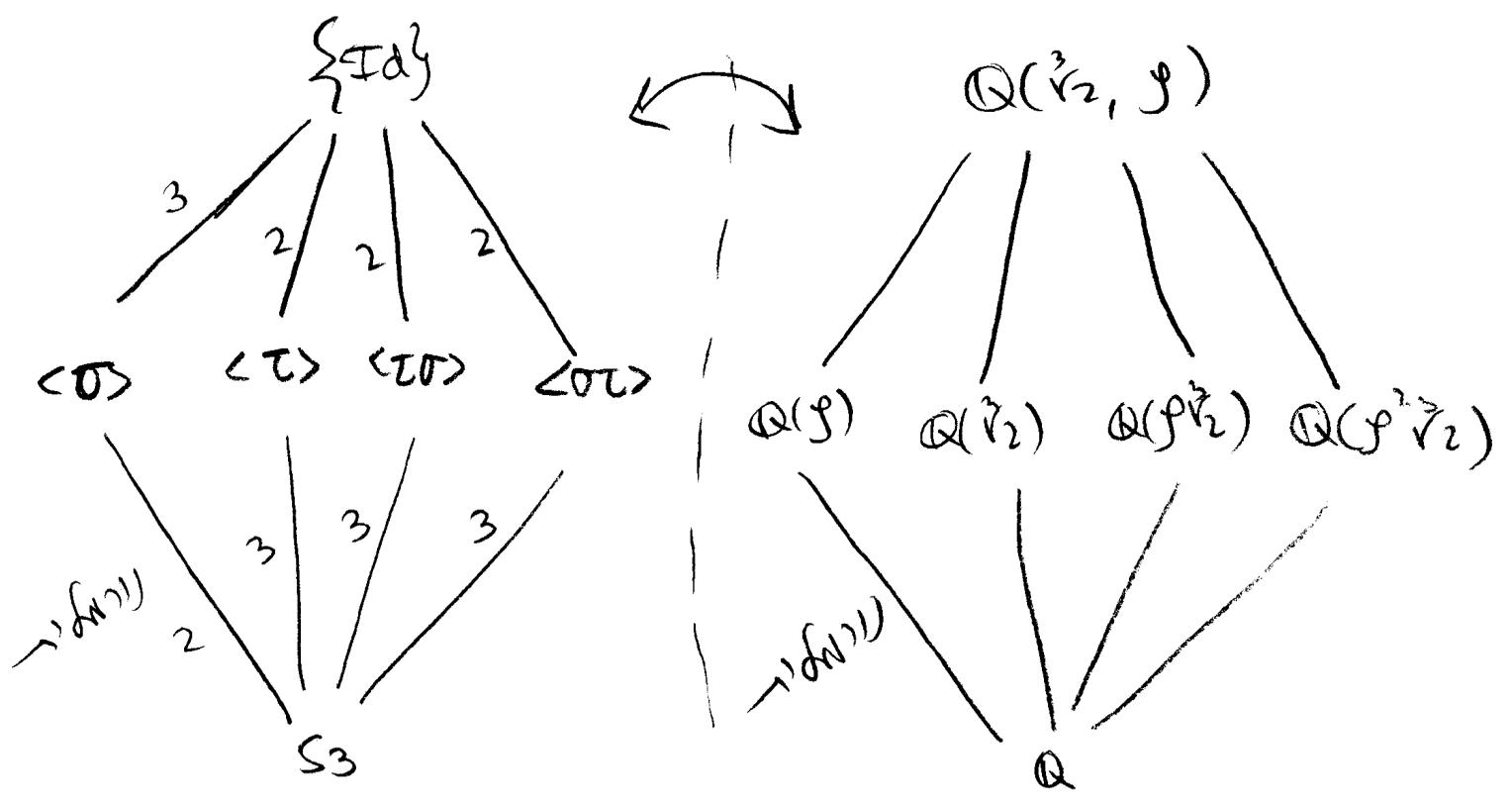
האננה צורה "ג" שיהיה במקסימום אנזיקור ואלו אלקטור

$$\text{Gal}(K/F) \cong S_3 \quad \text{היא האננה האננה}$$

$$\left. \begin{aligned} \sigma(\sqrt[3]{2}) &= \rho\sqrt[3]{2} \\ \sigma(\rho) &= \rho \end{aligned} \right\} \sigma^3 = 1$$

$$\left. \begin{aligned} \tau(\sqrt[3]{2}) &= \sqrt[3]{2} \\ \tau(\rho) &= \rho^2 \end{aligned} \right\} \tau^2 = 1$$

$$\text{Gal}(K/F) \cong S_3 \quad \leftarrow \sigma\tau \neq \tau\sigma$$



פירוק ארבעות איברי

5) ארבעת איברי זה לא סתנזיסים, כיום המסת איברי (המסת איברי זה לא סתנזיסים) -
 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$
 זהו $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ לא איברי כי יש לה רק ארבעה איברי
 אילו הצגה (ה) 4 ...

6) שדות מסויים - טיפו של המסת \mathbb{F}_p^n מסוים n על \mathbb{F}_p
 זהו שדה פיצול של $x^{p^n} - x$ על \mathbb{F}_p המסת $\mathbb{F}_p^n/\mathbb{F}_p$
 איברי. רק $n = |\text{Gal}(\mathbb{F}_p^n/\mathbb{F}_p)|$. נסו לשא ציקלי. הווי
 זה ארבעה איברי מסויים $x \mapsto x^p$. טיפו המסת של
 ארבעה איברי מסויים n . רק זהו זה.

שדה הפיצול של $x^8 - 2$

שדה הפיצול של $x^8 - 2$ שווה ל- $(\mathbb{Q}(\sqrt[8]{2}), \zeta_8)$ וזה
 גם שווה ל- $(\mathbb{Q}(\sqrt{2}, i))$. טיפו של שדה הפיצול זהו
 $\text{N} \leq 16$ [השוויון סגור כי סגור שמיסויים זהו ארבעה איברי מסויים גם
 זה $\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ סגור שמיסויים זהו ארבעה איברי מסויים זהו
 סגור זהו שדה $(\mathbb{Q}(\sqrt{2}, i))$ זהו 16 כי שמיסויים
 זהו זהו הצגה זהו 8 וזה ארבעה איברי של שדה הצגה 2.
 סגור המסת זהו 16.]

נסו: $\theta = \sqrt[8]{2}$ (נתמוך ב-)
 $i \mapsto \pm i$
 $\theta \mapsto \zeta^i \theta$ $i = 0, \dots, 7$

המסת של 16 ארבעה איברי מסויים (זאתו ארבעה איברי מסויים
 של שדה הפיצול.
 $\tau = \begin{cases} \theta \rightarrow \theta \\ i \rightarrow -i \end{cases}$ $\sigma = \begin{cases} \theta \rightarrow \zeta \theta \\ i \rightarrow i \end{cases}$ (צורה) ארבעה איברי מסויים
 ζ σ, τ

$$\xi = \xi_8 = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} = \frac{1}{2}(1+i)\sqrt{2} = \frac{1}{2}(1+i)\theta^4$$

$$\Rightarrow \sigma(\xi) = \frac{1}{2}(1+i)\theta^4 \xi^4 = \xi^5$$

$$\tau(\xi) = \frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} = \xi^7$$

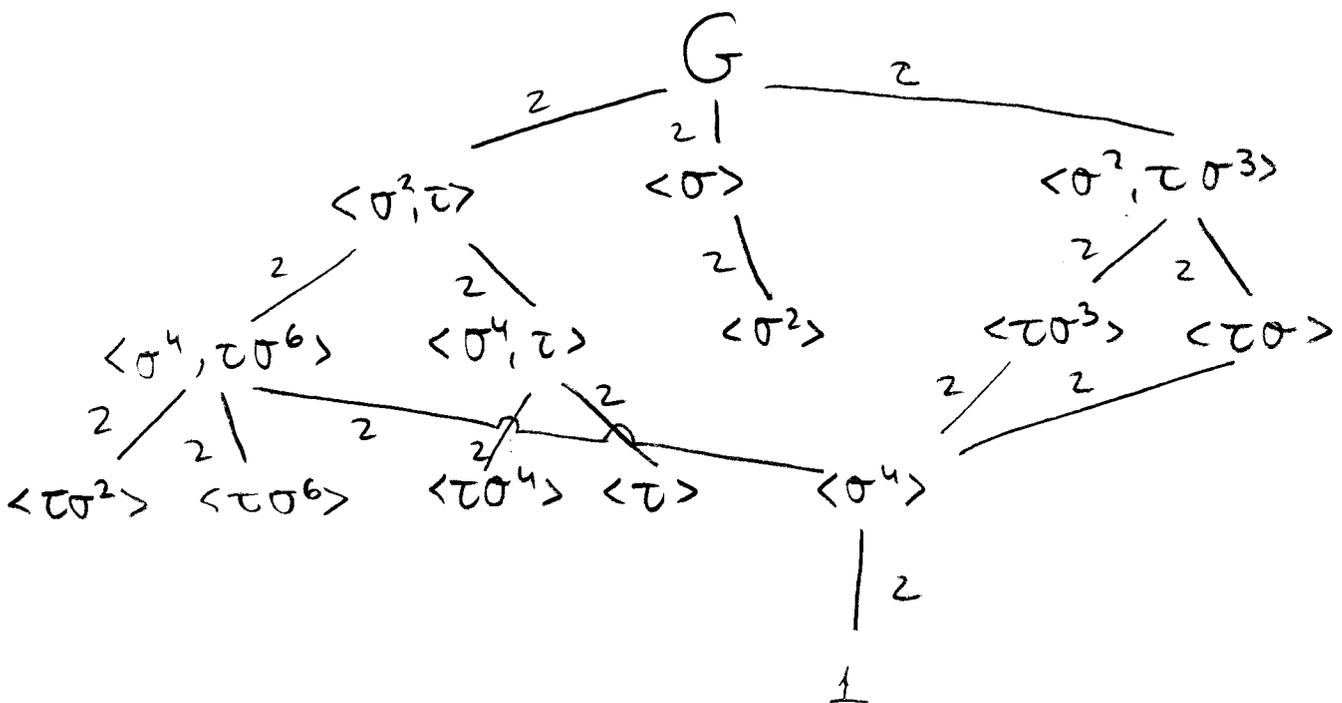
$$1 = \tau^2 = \sigma^8 \quad \text{בורר ש-}$$

נכזה להנחה ש- $\sigma\tau = \tau\sigma^3$ וזהו קונס אית
 אגני החמונה ותמונה לזו נקראת קווי-זיה צרליו.
 רצוי הראוה ש- $\tau\sigma = \sigma^3\tau$ צדק פשוט אעשה את
 ס החישובים.

$$\sigma \cdot \tau : \begin{cases} \theta \rightarrow \xi\theta \\ i \rightarrow -i \\ \xi \rightarrow \xi^7 \rightarrow \xi^{35} = \xi^3 \end{cases}$$

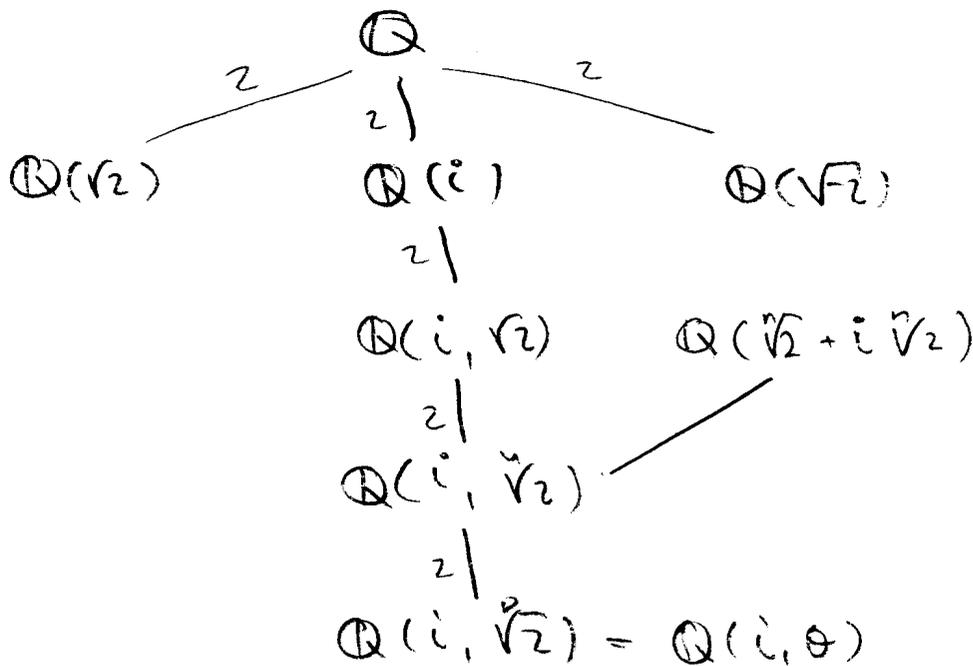
$$\tau \cdot \sigma^3 : \begin{cases} \theta \rightarrow \xi\theta \rightarrow \xi^6\theta \rightarrow \xi^3\theta = \xi^{-1}\theta \rightarrow \xi^7\theta = \xi\theta \\ i \rightarrow -i \\ \xi \rightarrow \xi^3 \end{cases}$$

בשעתם את האוטומורפיזמים צייק אביהר נו אשל $\sqrt{2} = \xi + \xi^7$
 וזה אגבו איתנו...



17

אברהם איתן קיבל את



אנחנו: נבנה שדה גלואה המכיל את שני החסמים

• $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i, \sqrt{2})$

$(\text{Fix}(\langle \sigma \rangle) = \mathbb{Q}(i, \sqrt{2})^{\langle \sigma \rangle})$ (*) $\mathbb{Q}(i) \subseteq \text{Fix}(\langle \sigma \rangle) \subseteq \mathbb{Q}(i, \sqrt{2})$

$[\text{Fix}(\langle \sigma \rangle) : \mathbb{Q}] = 2$ מכאן נראה

• קבוצת גלואה

$\langle \tau \sigma^3 \rangle$ - $\langle \tau \sigma \rangle$ - $\langle \sigma \rangle$ (גורמים אי-מתאימים)

$1, \tau \sigma^3$ הם $\langle \sigma^4 \rangle$ (צייגים) (מחלקות)

$\alpha = (1 + \tau \sigma^3) \theta^2 = \theta^2 + \tau \sigma^3 \theta^2$ זכר. $\theta = \sqrt[4]{2}$ - מסומן

$\tau \sigma^3$ - α מייצג σ^4 • σ^4 - α מייצג $\tau \sigma^3$

$$\begin{aligned} \tau \sigma^3 ((1 + \tau \sigma^3) \theta^2) &= (\tau \sigma^3 + \tau \sigma^3 \tau \sigma^3) \theta^2 = \\ &= (\tau \sigma^3 + \tau \tau \sigma^3 \sigma^3) (\theta^2) = (\tau \sigma^3 + \sigma^4) (\theta^2) = \\ &= \tau \sigma^3 \theta^2 + \theta^2 \end{aligned}$$

• • • אקרום מספרים הרעיון היא להתבונן במסגרת המחלקה

... אנוורטנינג

18) 13/7/08
 מונח

הצגת שדה אי-רציונליים \mathbb{Z} (הצגת שדה אי-רציונליים \mathbb{Z})
 תלכודת של שדה אי-רציונליים. ב שדה אי-רציונליים \mathbb{Z} הוא מהצורה
 ההצגה היחידה של \mathbb{F}_p הצורה n שבו \mathbb{Z} אי-רציונליים.
 $\text{Gal}(\mathbb{F}_p^n / \mathbb{F}_p)$ צורת n שבו \mathbb{Z} אי-רציונליים
 שבו $x \rightarrow x^p$

ב $d | n$ יש n/d אלמנטים (צורת) שבו



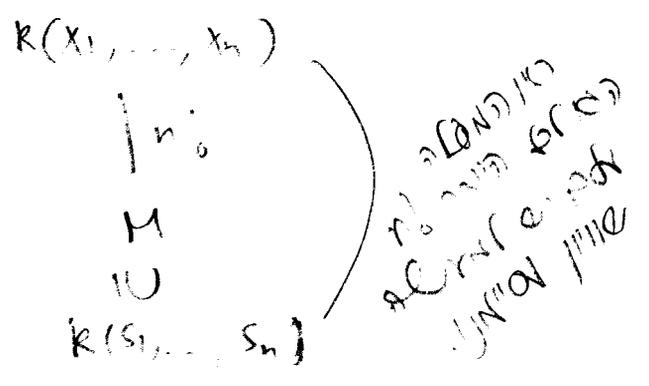
מקיים $\mathbb{F}_{p^n}^{\langle \sigma^d \rangle} = \mathbb{F}_{p^d}$ כי $\sigma^d(\alpha) = \alpha$ II
 שבו $\alpha^{p^d} - \alpha = 0$ I
 $a \in \mathbb{F}_{p^d}$ (כי) $x^{p^d} - x$ \mathbb{F}_{p^d} (הצורה היחידה של \mathbb{F}_{p^d})
 \mathbb{F}_{p^d} - (הצורה היחידה של \mathbb{F}_p) d שבו \mathbb{F}_p II

וכן $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ $m | n$

$f(x) \in \mathbb{Z}[x]$ - אצל \mathbb{Z} הצורה היחידה של \mathbb{Z} (הצורה היחידה של \mathbb{Z})
 $x^n - 2$ \mathbb{Z} (הצורה היחידה של \mathbb{Z})
 שבו (x^n)

דוגמה: $x^4 + 1$ אי-רציונליים \mathbb{Z} (הצורה היחידה של \mathbb{Z})
 $\mathbb{Q} = x^4 + 1$ (הצורה היחידה של \mathbb{Q})
 $(x+1)^4 = (x^2+1)^2 = x^4 + 1$ \mathbb{Z} \mathbb{Q} (הצורה היחידה של \mathbb{Q})
 $p = 1, 3, 5, 7 \pmod{8}$ \mathbb{Z} \mathbb{Q} (הצורה היחידה של \mathbb{Q})
 $(p^m - 1) \mid (x^{p^m} - 1)$ \mathbb{Z} (הצורה היחידה של \mathbb{Z})

(19) השאלה: אילו הפונקציות הרציונליות הסגורות (closed) הן? $k(x_1, \dots, x_n)$
 כל סדרה של פונקציות רציונליות (הן שלמים והן שברים) $k(x_1, \dots, x_n)$ היא
 תת-השדה $k(x_1, \dots, x_n) \subseteq k(s_1, s_2, \dots, s_n)$
 (המתקיים: S_n (המספר הטבעי) $\subseteq k(x_1, \dots, x_n)$)
 בשטח זה תמיד קיימת פונקציה רציונלית, אם כי לא תמיד
 בעלת טווח זהה לזה של הפונקציות הרציונליות הסגורות M .
 $M \subseteq k(x_1, \dots, x_n)$ כי הרכבתם של פונקציות
 $n! = |S_n| = [k(x_1, \dots, x_n) : M]$
 (שמהלך זה הפיכות של הפונקציות) $F(x_1, \dots, x_n)$
 השדה $k(x_1, \dots, x_n)$ הוא סגור $k(s_1, \dots, s_n)$
 ואינו שדה של פונקציות רציונליות $k(x_1, \dots, x_n)$ הוא
 היות $n!$ זוגי.



(20)

$\sigma: t \mapsto t+1$ (\mathbb{N}) g אה g
 הפונקציה $k(t)^{\langle \sigma \rangle} \subseteq k(t)$ היא הפונקציה
 הזאת שהתחבבה על ידי σ .
 $k(t^p - t) \subseteq k(t)^{\langle \sigma \rangle}$ כי $t^p - t \in k(t)^{\langle \sigma \rangle}$ - כי אם $t \in k(t)^{\langle \sigma \rangle}$
 $k(t^p - t) \subseteq k(t)$ אז כל הפונקציות שהן פולינומים
 הם פולינומים.

הרחבות ציקלוטומיות

$\mathbb{Q}(\zeta_n)$ השרדה הציקלוטומיה n-י. $M_{\mathbb{Q}, \zeta_n} = \mathbb{Z}$ אי-שק
 מצדנה $\varphi(n)$. $\mathbb{Z} \subset \mathbb{Q}(\zeta_n)$ כגוף \mathbb{Z} שורש n-י
 פרימיטיבי ויחידה.

באוסטרוורפוליס σ חיים ולוח את ζ_n ושרש פרימיטיבי אחר.

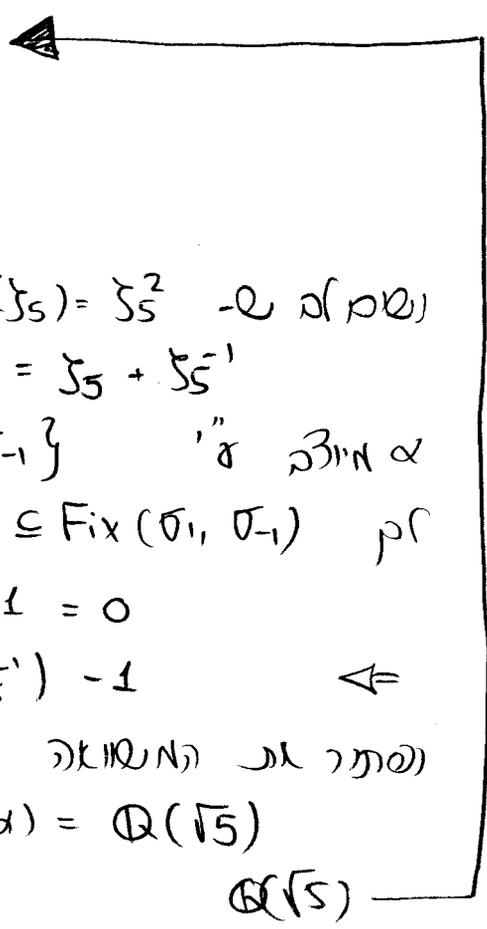
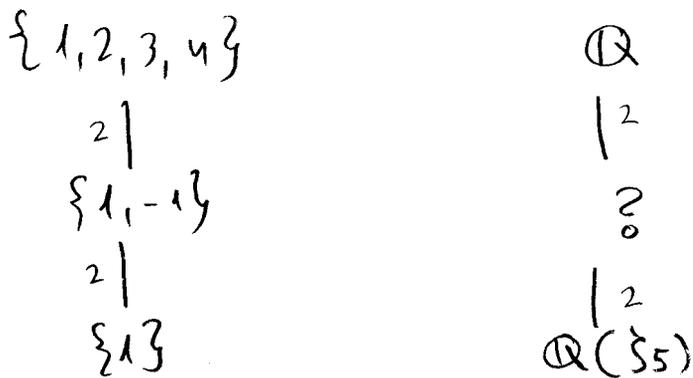
לפי $\sigma(\zeta_n) = \zeta_n^a$ עבור $(a, n) = 1$.

יש איזומורפיזם $(\mathbb{Z}/n\mathbb{Z})^* \rightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

$a \mapsto \sigma_a, \sigma_a(\zeta_n) = \zeta_n^a$

כה הומומורפיזם כי $\sigma_a \circ \sigma_b = \sigma_{ab}$ ברורה לשם זה הפיכה.

צייאאוג: $\mathbb{Q}(\zeta_5)$ היא הרחבת גלואה עם תבורת גלואה
 $\mathbb{Z}/4\mathbb{Z} \cong (\mathbb{Z}/5\mathbb{Z})^*$. לפי מחנה התת-תבורת, יש תת-שרדה אחרת בין
 $\mathbb{Q}(\zeta_5) - \mathbb{Q}$.



נשמר ל- $\sigma_2(\zeta_5) = \zeta_5^2$ יורה ל תבורת גלואה. (תמוך ה-)

$\alpha = 1\zeta_5 + (-1)\zeta_5^{-1} = \sigma_1(\zeta_5) + \sigma_{-1}(\zeta_5) = \zeta_5 + \zeta_5^{-1}$

$\sigma_{-1}(\zeta_5 + \zeta_5^{-1}) = \zeta_5^{-1} + \zeta_5$ כי $\{\sigma_1, \sigma_{-1}\}$ "א מיוזב"

לפי $\mathbb{Q}(\alpha) \subseteq \text{Fix}(\sigma_1, \sigma_{-1})$ נשמר ל- ζ_5 נקיים

$\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$

$0 = \alpha^2 - \alpha - 1 = (\zeta_5^2 + 2 + \zeta_5^{-2}) + (\zeta_5 + \zeta_5^{-1}) - 1$ ←

נפתר את המשואה הנ"ל, ל- $\alpha = \frac{1 \pm \sqrt{5}}{2}$ טומר

$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$ לפי השרדה האמצעי ה

$\mathbb{Q}(\sqrt{5})$

האופן בלוי, $\mathbb{Q}(\sqrt{\pm p}) \subseteq \mathbb{Q}(\zeta_p)$ אתה מסימן אוקרוים
 באלו, והוא : $p \equiv 1 \pmod{4} : +$
 $p \equiv 3 \pmod{4} : -$
 (תרגיל לא קל)

נתבונן ב- $\mathbb{Q}(\zeta_p)$ עבור p ראשוני. לכן, $(\mathbb{Z}/p\mathbb{Z})^*$
 ציקלור. נמצא מסים נחמז אצבז איתנו :
 צום- $\zeta_p^{-2}, \dots, \zeta_p^2, \zeta_p, 1$ מסים א- $\mathbb{Q}(\zeta_p)$
 אכיוון ל- $0 = 1 + \zeta_p + \zeta_p^2 + \dots + \zeta_p^{p-1}$ (נוסח ל-
 $1 - \zeta_p^p = 0$ מסים $\zeta_p^{-1}, \zeta_p^2, \dots, \zeta_p^{p-1}$
 לאה זה מסים נחמז

אכיוון ל- p ראשוני, אלו הציק שרטי היתיבה
 הפרימטיבים מוצטו p ופעולת חבורת גלטה היא
 פרמוטציה על יורם.

תהיו $H < Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. נרצה לתאר את $Fix(H)$.
 נגדיר $\alpha_H = \sum_{\sigma \in H} \sigma(\zeta_p)$

כרור ל- $\alpha \in Fix(H)$ לרתי אם $\tau \in H$
 $\tau(\alpha_H) = \tau(\sum_{\sigma \in H} \sigma(\zeta_p)) = \sum_{\sigma \in H} \tau\sigma(\zeta_p) = \sum_{\psi \in H} \psi(\zeta_p)$

הכל שלב אכיונותימה לר חסר שני סגור
 סטמה.

נרצה ארבות ל- $\mathbb{Q}(\alpha_H) = Fix(H)$. נניח לאן שווין.
 אר $\mathbb{Q}(\alpha_H)$ אתים א- $Fix(H')$ סבור $H \neq H'$.
 אר חספיק אראר של איבר מחול א- H מציב את α_H .
 יקח $\tau \notin H$ ונניח ל-

$\sum_{\sigma \in H} \tau\sigma(\zeta_p) = \tau\alpha_H = \alpha_H = \sum_{\sigma \in H} \sigma(\zeta_p)$
 אר סטמה ל איברי המסו Δ . אר $\tau(\zeta_p) = \sigma(\zeta_p)$
 $\sigma^{-1}\tau = Id \iff \sigma^{-1}\tau(\zeta_p) = \zeta_p \iff \tau = \sigma$
 א"מנו $\tau = \sigma$

(2)

5k . $\mathbb{Q}(\zeta_{13})$ - אסות, $\mathbb{Q}(\zeta_{13})$

$\langle \sigma_2 \rangle = C_{12} \cong (\mathbb{Z}/13\mathbb{Z})^*$

מספר תמורה חתומה	2	3	4	6
יוצר	σ^6	σ^4	σ^3	σ^2
מספר התמורה של שדה	6	4	3	2
יוצר שדה השדה	$\zeta + \zeta^{-1}$	$\zeta + \zeta^3 + \zeta^6$		

$\text{Id } \zeta_{13} + \sigma^6 \zeta_{13} = \zeta + \zeta^{2^6} = \zeta + \zeta^{-1}$

$\zeta + \sigma^4 \zeta + \sigma^8 \zeta = \zeta + \zeta^{2^4} + \zeta^{2^8} = \zeta + \zeta^3 + \zeta^9$

וכן הלאה

periods באמצעות האלה וקראים

$\varphi(n) = \prod_{i=1}^r \varphi(p_i^{e_i})$ $n = p_1^{e_1} \dots p_r^{e_r}$ מספר

$\mathbb{Q}(\zeta_{p_i^{e_i}}) \cong \mathbb{Q}(\zeta_n^{p_1^{e_2} \dots p_1^{e_r}}) \subseteq \mathbb{Q}(\zeta_n)$ 5k

$\mathbb{Q}(\zeta_{p_i^{e_i}}) \subseteq \mathbb{Q}(\zeta_n)$, i כל אחד, i אסות

$\prod \mathbb{Q}(\zeta_{p_i^{e_i}}) \subseteq \mathbb{Q}(\zeta_n)$ \Leftarrow $\mathbb{Q} = \mathbb{Q}(\zeta_{p_i^{e_i}}) \cap \mathbb{Q}(\zeta_{p_j^{e_j}})$

$\prod \mathbb{Q}(\zeta_{p_i^{e_i}}) = \mathbb{Q}(\zeta_n)$ \Leftarrow $\varphi(p_i^{e_i}) = [\mathbb{Q}(\zeta_{p_i^{e_i}}) : \mathbb{Q}]$

$\varphi(p_i^{e_i}) = [\mathbb{Q}(\zeta_{p_i^{e_i}}) : \mathbb{Q}]$ \Leftarrow

$\mathbb{Q} = \mathbb{Q}(\zeta_{p_i^{e_i}}) \cap \mathbb{Q}(\zeta_{p_j^{e_j}})$ \Leftarrow

$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta_{p_1^{e_1}})/\mathbb{Q}) \times \dots \times \text{Gal}(\mathbb{Q}(\zeta_{p_r^{e_r}})/\mathbb{Q})$ \Leftarrow

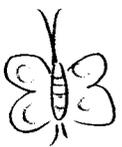
$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \times \dots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^*$

האסות השדה האסות

נראה של תמונה אלמנטרית נותנת אמינות כחבורת גלואה G
 של $\mathbb{Q}(\zeta_n)$. נראה של תמונה אלמנטרית סופית מובילה כחבורת תמונה
 של תמונה מהצורה $(\zeta/p_1)^* \dots (\zeta/p_g)^*$

הוכחה: יקום $G = C_{n_1} \times \dots \times C_{n_k}$. בעזרת משפט
 השלישי של קורסיני (ויתר אחרות)

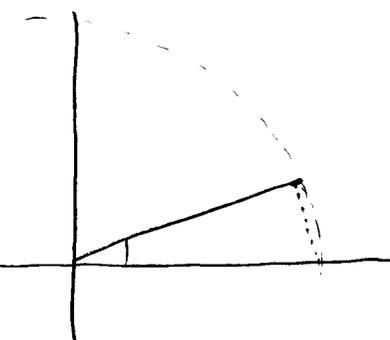
$p_i \equiv 1 \pmod{n_i}$
 $p_k \equiv 1 \pmod{n_k}$
 $n_i \mid p_i - 1$ for $1 \leq i \leq k$



(Dummit & Foote) סעיף 9.2

הנניח n הוא מספר ראשוני ו- ζ_n הוא שורש n -י של היחידה

אילו מצבים נותן אנוני $\mathbb{Q}(\zeta_n)$
 הנייה של מצב $\mathbb{Q}(\zeta_n)$ וצורה של קוהרנט אנוני של \mathbb{Q}
 להשקוף אנוני של \mathbb{R}



אנחנו $\alpha \in \mathbb{R}$ נותן אנוני \mathbb{Q}
 אנוני $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ חלקה של α

(הפסל תנאי של $\mathbb{Q}(\text{Re}(\zeta_n))$ יתקיים -
 יהיה הרחבה מסוג חלקה של \mathbb{Q}

(סיון) $x = \text{Re} \zeta_n = \frac{\zeta_n + \zeta_n^{-1}}{2}$. (הפסל) $\mathbb{Q}(\zeta_n)$ ונקרא

$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\text{Re} \zeta_n)] = 2 \iff \zeta_n^2 - 2x\zeta_n + 1 = 0$

$\mathbb{Q}(\text{Re} \zeta_n) : \mathbb{Q}$ חלקה $\mathbb{Q}(\zeta_n) : \mathbb{Q}$ אנוני

של $2 \iff [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ חלקה של 2 אנוני

$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \prod_{i=1}^g \varphi(p_i^{e_i})$

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

יקום $\varphi(p^e)$ יהיה חלקה של 2 : אנוני $p=2$ אנוני

$p \neq 2$ אנוני קובצת $n=1$ אנוני p ראשוני : יתקיים חלקה 2

אנוני אנוני אנוני $p=2^{2^n} + 1$ (ראו קורס בתורת המספרים)

23

$$n = 2^k p_1 \dots p_r$$

פר n -בינומית $x^n - x + 1$ אי-פריק
על \mathbb{F}_p כאשר p_i אינן מתחלקים ב- n

ראוהו $x^{p^n} - x + 1 = \varphi(x)$ אי-פריק
על \mathbb{F}_p כאשר $n=1$ ו- $p=2$
אם $\alpha \in \mathbb{F}_{p^n}$ אז $\alpha + \alpha^{p^n} = 0$

$$(\alpha + \alpha)^{p^n} - (\alpha + \alpha) + 1 = \alpha^{p^n} - \alpha + 1 + \frac{\alpha^{p^n}}{\alpha} - \alpha = 0$$

אם $\alpha \in \mathbb{F}_{p^n}$ אז $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$
השדה $\mathbb{F}_p(\alpha)$ מכיל את α ואת α^p
אם $\alpha^p = \alpha + a$ אז $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$

$$(\alpha^p)^{p^n} - \alpha^{p^{n+1}} = (\alpha^{p^n} - \alpha)^p + 1 = (-1)^{p+1} = 0$$

$$\alpha^p = \alpha + a \iff \alpha \in \mathbb{F}_{p^n}$$

$$[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] \leq p \text{ פר } \mathbb{F}_{p^n} \text{ לפי } x^p - x + a$$

אם $\alpha \in \mathbb{F}_{p^n}$ אז $\alpha^p = \alpha + a$ ו- $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$
אם $\alpha \notin \mathbb{F}_{p^n}$ אז $\mathbb{F}_p(\alpha) \neq \mathbb{F}_{p^n}$

$$\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n} \text{ פר } \alpha \in \mathbb{F}_{p^n} \text{ אז } \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$$

$$\mathbb{F}_{p^n} \text{ מכיל את } \mathbb{F}_p \text{ ולכן } \mathbb{F}_p(\alpha) \text{ מכיל את } \mathbb{F}_p$$

הוא \mathbb{F}_{p^n}

$$p = n = 2 \text{ ו-} n = 1 \iff p^n = [\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] = p \cdot n \text{ פר}$$

$\psi: k(t) \rightarrow k(t)$ $\text{char } F = p$ $\psi(t) = t+1$ $\text{Fix}(\psi)$ $\text{Fix}(\psi) = \{k(t) \mid \psi(k(t)) = k(t)\}$

שכ $\frac{f(t)}{g(t)} = \frac{f(t+1)}{g(t+1)}$; $\text{char } F = p$ או

$H(t) = f(t)g(t+1) = g(t)f(t+1) = H'(t)$

$\Rightarrow H(t) = H(t+1) = H(t+2) = \dots$

$\dots H = 0$ פר כמה פונקציות $H = 0$ \Leftarrow

$\psi: k[t] \rightarrow k[t]$ $\text{char } F = p$ $f(t) \rightarrow f(t+1) - f(t)$

$1, t, t^2, \dots, t^p, \dots$ $\text{char } F = p$ $t^p - t \in \text{Fix}(\psi)$

	1	t	t ²	...	t ^p	...
1	0	1	1	...	1	...
t	0	0	2	...	0	...
t ²	0	0	0	...	0	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮
t ^p	0	0	0	...	0	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮

$t^p - t \in \text{Fix}(\psi) \iff t^p - t \in \text{Ker } \psi \iff$

$\Rightarrow \text{Fix}(\psi) = \langle t(t+1)(t+2)\dots(t+p-1) \rangle$ או

$t^p - t$ $\text{Fix}(\psi)$ $\text{Fix}(\langle \psi \rangle) = \text{Fix}(\psi)$ $\text{char } F = p$

$\text{Fix}(\langle \psi \rangle) = \text{Fix}(\psi)$ $\text{char } F = p$

$k(t)/\text{Fix}(\psi)$ $\text{char } F = p$ $k(t)$ $\text{char } F = p$

$k(t^{p-t}) \in \text{Fix}(\psi)$ $\text{char } F = p$ $\text{char } F = p$

$[k(t) : k(t^{p-t})] = p$ $\text{char } F = p$



(25)

$$n \mid \varphi(p^n - 1) \quad : \underline{B}$$

$$! \quad |Gal(\mathbb{F}_{p^n})| = n \quad - \text{על } \mathbb{F}_p \quad = \underline{1770}$$

$$Gal(\mathbb{F}_{p^n}) \leq Aut(\mathbb{F}_{p^n}^*) = Aut C_{p^n-1}$$

$$\varphi(p^n - 1) = |Aut C_{p^n-1}| \quad \text{כל } n \mid \varphi(p^n - 1) \quad \Leftarrow$$

אם n אינו זוגי אז $n \mid \varphi(p^n - 1)$
אם n זוגי אז $n \mid \varphi(p^n - 1)$

11.08.08
 ג' תמוז

הצגת הבעיה

• אנו רוצים לראות כי $x^p - x + a \in \mathbb{F}_p[x]$ מתפרק לגורמים ליניאריים.
 כלומר, $\exists \alpha \in \mathbb{F}_p$ כזה ש- α הוא שורש של $x^p - x + a$.

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

$\forall y \quad y^p = y$

נניח $1 < r < p$ נגד $(x^p - x + a) = (x^r - Ax^{r-1} + \dots)(x^{p-r} + \dots)$

כאן A הוא מספר השורשים של הפולינום $(x^r - Ax^{r-1} + \dots)$ ולכן
 $A = \sum_{j=1}^r (\alpha + i_j) = r\alpha + b$ כן $\pi(x - x_i)$ (הפולינום הממונה)
 נגד $\exists b \in \mathbb{F}_p$ וכן $A \in \mathbb{F}_p$ וכן $\alpha = \frac{A-b}{r} \in \mathbb{F}_p$

כלומר, אם $\alpha \in \mathbb{F}_p$ הוא שורש של $x^p - x + a$ אז גם $\alpha + i \in \mathbb{F}_p$ הוא שורש.
 כלומר, הפולינום מתפרק לגורמים ליניאריים.

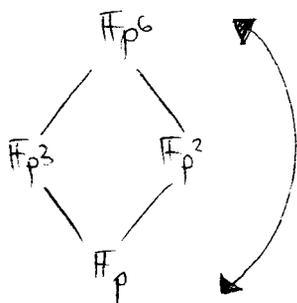
• יהי $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ ויהי $\alpha \in \overline{\mathbb{F}_p}$ הרי $\alpha^p = \alpha$ כלומר $\alpha \in \mathbb{F}_p$.

• תלמיד מוצא כי לאה 2

הוא מנסה להוכיח שהשורשים של $x^p - 1$ הם $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$ כאשר ζ הוא שורש יחידאי.

$$x^{p-1} - 1 = \prod_{x_i \in \mathbb{F}_p^*} (x - x_i) = x^{p-1} + \dots + (-1)^{p-1} \prod_{x_i \in \mathbb{F}_p^*} x_i$$

כלומר $p=2$ אז $-1 = (-1)^{2-1} \prod_{x_i \in \mathbb{F}_2^*} x_i = -1 \cdot 1 = -1$ \triangleleft
 $2 < p$



• מהי המינימום של \mathbb{F}_{p^6} ?

$\text{Gal}(\mathbb{F}_{p^6}/\mathbb{F}_p) \cong C_6$
 המינימום של \mathbb{F}_{p^6} הוא \mathbb{F}_p .
 המינימום של \mathbb{F}_{p^2} הוא \mathbb{F}_p .
 המינימום של \mathbb{F}_{p^3} הוא \mathbb{F}_p .

• מצא את שדה הפיצול של $x^3 + 2x - 2$ אל \mathbb{F}_3 . קל לראות שאין
 או שורש זעק, והוא אי-פסיק. השדה $\mathbb{F}_3[x]/(x^3+2x-2)$ מזהו שדה של
 הפולינום וקונו גם של הרחבת גלואה. אכן היא נורמלית זעק זה שיש שיש את
 זה אומר שיש את \mathbb{F}_3 השורשים. זעק זה שדה פיצול.

• טענה: $\mathbb{F}_p^m \subseteq \mathbb{F}_p^n$ א"א $m \mid n$ ובמקרה כזה
 $\langle \sigma \rangle = \text{Gal}(\mathbb{F}_p^n / \mathbb{F}_p^m) \cong C_{n/m}$
 ואם $\sigma(x) = x^{p^m}$
 (שדה השבת של \mathbb{F}_p^m הוא \mathbb{F}_p)

• ציגיה שהרחבה לא ספרבולית: $\mathbb{F}_p(t^p) \subseteq \mathbb{F}_p(t)$. כאן
 $m_{t, \mathbb{F}_p(t^p)}(x) = x^p - t^p = (x-t)^p$. האכחוכו זעק זה וזהו
 שלו החלקה הנורמלית האפשרית כי $t^k - t^p \neq 0$ אב $k < p$.
 הפולינום הזה לא ספרבולי. t הוא שורש זעק זה וזהו $1 < p$. זה מזה
 זה שדה פיצול של פולינום זעק הרחבה נורמלית.

תכונות גלואה של

• מצא את שדה הפיצול של $f = x^3 + 2x - 2$ אל \mathbb{Q} . זה פולינום
 אי-פסיק לפי קריטריון איינשטיין. שדה הפיצול שלו הוא הרחבת גלואה
 וראה שיש איבר זעק 2 בחבורת גלואה ונסיים.
 יש שורש ממשי אחד α . f כי הוא מצרפה אי-זוגית ומחקים $\sigma(\alpha) = 3\alpha^2 + 2 > 0$
 אז הוא נראה שזה \mathbb{R} . זעק יש שורש יחיד ב- \mathbb{R} . אכן שני השורשים
 ב- \mathbb{C} . (נסו ב- \mathbb{C} את שדה הפיצול אז $\mathbb{C} \subseteq \mathbb{R}$ וזה נמצא
 היא אוטומופיזם מסדר 2. (נסו ב- \mathbb{C}) $[\mathbb{C} : \mathbb{Q}] = 6$. $\mathbb{Q}(\alpha)$ גלואה זעק
 $[\mathbb{Q} : \mathbb{Q}] = |\text{Gal}(\mathbb{C}/\mathbb{Q})| = 2$ שמה מצאנו של איבר זעק 2. מצד שני, אם α
 שורש של f אז $\mathbb{Q}(\alpha) \subseteq \mathbb{C}$. הרחבה מסדר 3 כי f איננו פסיק.
 אכן, $[\mathbb{C} : \mathbb{Q}] = 6$ אבל $[\mathbb{C} : \mathbb{Q}] \leq 3!$ זעק $[\mathbb{C} : \mathbb{Q}] = 6$ זעק
 $\text{Gal}(\mathbb{C}/\mathbb{Q}) = S_3$.

• תורה - $\mathbb{Q}(\sqrt[3]{2})$ לא מזהו זעק זיקסומוני.
 פתרון I: אם $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{m})$ זעק זה אז קיימת $H \subseteq \mathbb{Z}_n^*$
 קב- $\text{Fix}(H) = \mathbb{Q}(\sqrt[3]{2})$. H נורמלית א"א $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ גלואה.
 זו סתירה כי H זו נורמלית כי \mathbb{Z}_n^* אבלי אבל $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ לא גלואה.
 פתרון II: אם $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{m})$ זעק זה הסדר הנורמלי של $\mathbb{Q}(\sqrt[3]{2})$ (סומ)

