מבנים אלגבריים 2, 80446 — בכי לקראת מבחן

9 באוגוסט 2025

תוכן עניינים

1 מלא הגדרות ונגזרותיהן 3
1.1 הרחבות אלגבריות 3
1.2 שדות סגורים אלגברית 3
1.3 חבורת האוטומורפיזמים של הרחבת שדות 3
1.4 שדה פיצול של פולינום 4
1.5 הרחבות ספרביליות 4
1.6 הרחבות נורמליות 5
1.7 רזולטנטה, cubic resolvent, רזולטנטה וכד' 5
2 איך נעה מפרקת 6
3 טריקים שטריקים 7
4 דוגמאות 8
4.1 דברים עם כמויות 8
4.2 איך מוצאים שדה פיצול של פולינום מעל $\mathbb{F}_p$ 8
4.3 מגדלים 8
4.4 מלא חבורות גלואה 9
4.5 שדות ביניים 12
4.6 שדות פיצול 15
4.7 פולינומים סימטריים 16
5 דברים שחשוב לזכור למבחן 17
5.1 חבורות מסדרים קטנים 17
5.2 תתי־חבורות של חבורות סימטריות 17
5.3 קוסינוסים וסינוסים טובים 18
5.4 פולינום ציקלוטומיים בסיסיים 18
5.5 נוסחאות לפולינומים ציקלוטומיים 18
6 משפטים להוכחה במבחן 19
6.1 תנאים שקולים להרחבה נוצרת סופית 19
6.2 לכל שדה קיים סגור אלגברי 20
6.3 שדה המרוכבים הוא סגור אלגברית 21
6.4 על פרובניוס ושדות סופיים מחזקות p 22
6.5 כל הרחבה ספרבילית סופית היא פרימיטיבית 23
6.6 משפט ארטין 24
6.7 התאמת גלואה 25
6.8 הלמה השנייה של גאוס 26
6.9 טענה 8.4.2 ברשומות של מיכאל 27
6.10 טענה על הרחבות ציקלוטומיות תחת תנאי יפה 28

1 מלא הגדרות ונגזרותיהן

1.1 הרחבות אלגבריות

הגדרה 1.1 (איבר אלגברי, איבר טרנסצנדנטי): בהינתן הרחבה E/F ו־$\alpha \in E$, נגיד ש־α **אלגברי** מעל F אם קיים $f(t) \in F[t]$ כך שמתקיים $f(\alpha) = 0$, אחרת נגיד ש־α נקרא **טרנסצנדנטי** מעל E.
אם $\mathrm{char}(E) = 0$ אז $\alpha \in E$ אלגברי או טרנסצנדנטי אם הוא אלגברי או טרנסצנדנטי מעל $\mathbb{Q}$.
נשים לב לתנאי טוב עבור אלגבריות:

$$\alpha \text{ אלגברי מעל } F \iff [F(\alpha) : F] < \infty$$

הגדרה 1.2 (פולינום מינימלי): **הפולינום המינימלי** של α של m_α מעל שדה הוא הפולינום המתוקן בעל המעלה המינימלית בתוך שדה הפולינומים שלנו שמאפס את α.
כדי להראות שפולינום הוא מינימלי, צריכה להתקיים השלשה הבאה:

1. $f_{\alpha/F}(\alpha) = 0$
2. f פולינום מתוקן
3. f אי־פריק

הגדרה 1.3 (הרחבה אלגברית): הרחבת שדות E/F נקראת **אלגברית** אם כל $\alpha \in E$ הוא אלגברי מעל F (אחרת ההרחבה נקראת **טרנסצנדנטית**).

הגדרה 1.4 (הרחבה נוצרת סופית): הרחבה E/F נקראת **נוצרת סופית** אם קיימים $\alpha_1, \cdots, \alpha_k \in E$ כך שמתקיים $E = F(\alpha_1, \cdots, \alpha_k)$

משפט 1.1 (תנאים שקולים להרחבה נוצרת סופית): תהיי E/F הרחבת שדות אז הבאים שקולים

1. E/F סופית
2. E/F נוצרת סופית ואלגבריות
3. $E = F(\alpha_1, \cdots, \alpha_k)$ כאשר $\alpha_1, \cdots, \alpha_k$ אלגבריים

טענה 1.1 (אריתמטיקה של אלגבריים):

1. אם α, β אלגבריים מעל F ו־$\beta \neq 0$ אז גם $\alpha \cdot \beta, \alpha \pm \beta, \frac{\alpha}{\beta}$ אלגבריים מעל F
2. אם α, β אלגבריים מעל F אז $\deg(\alpha+\beta) \leq \deg(\alpha) \cdot \deg(\beta)$ (זה נובע מהדרגה של הרזולטנטה)
3. אם $K/F, L/K$ הרחבות אלגבריות של שדות אז גם L/F הרחבה אלגברית

הגדרה 1.5 (הרחבה פרימיטיבית): הרחבה E/F נקראת הרחבה **פרימטיבית/פשוטה** אם היא נוצרת על־ידי איבר אחד, והאיבר הזה ייקרא **האיבר הפרימיטיבי** של ההרחבה.

1.2 שדות סגורים אלגברית

הגדרה 1.6 (שדה סגור אלגברית (algebraically closed)):
שדה F **סגור אלגברית** אם לכל פולינום ממעלה גדולה מ־1 ב־$F[x]$ יש שורש ב־F (כלומר, אם השדה סגור אלגברית אז כל פולינום ניתן לפירוק).
אם f פולינום מתפרק לגורמים לינאריים נגיד שהוא **מתפצל לחלוטין**.

הגדרה 1.7 (סְגוֹר אלגברי (algebraic closure)): השדה E הוא **סְגוֹר אלגברי** של F אם E/F הרחבה אלגברית ו־E סגור אלגברית.

1.3 חבורת האוטומורפיזמים של הרחבת שדות

הגדרה 1.8: חבורת האוטומורפיזמים של הרחבת שדות

L/K הרחבת שדות

$$\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \forall x \in K \; \sigma(x) = x\}$$

טענה 1.2 (חבורת האוטומורפיזמים של הרחבות אלגבריות פשוטות):

1. אם $L = K(\alpha)$ הרחבת שדות פשוטה אז כל $\sigma \in \mathrm{Aut}(L/K)$ נקבע לחלוטין על־ידי $\sigma(\alpha)$
2. $L = K(\alpha)$ הרחבת שדות אלגברית פשוטה ו־$m_\alpha \in K[x]$ הפולינום המינימלי של α מעל K, אז
   1. לכל $\sigma \in \mathrm{Aut}(L/K)$ התמונה $\sigma(\alpha)$ היא שורש מתוך L של הפולינום המינימלי m_α
   2. לכל β שורש של m_α ב־L קיים ויחיד $\sigma \in \mathrm{Aut}(L/K)$ כך ש־$\sigma(\alpha) = \beta$
3. L/K הרחבה אלגברית פשוטה אז $|\mathrm{Aut}(L/K)| \le [L : K]$ ויש שיוויון אם ורק אם הפולינום המינימלי m_α מתפצל לגורמים לינאריים **שונים** ב־L

הגדרה 1.9 (שורש יחידה פרימיטיבי מסדר n): יהי $2 \le n \in \mathbb{N}$. **שורש יחידה פרימיטיבי מסדר n** הוא שורש יחידה שלכל $1 \le m < n$ מתקיים $\xi^m \neq 1$.

טענה 1.3 (חבורת האוטומורפיזמים של הרחבות צקלוטומיות): ניקח K שדה ו־$\overline{K}$ הסגור האלגברי שלו.

עבור $\mathbb{N} \ni n \ge 2$, **שורש יחידה פרימיטיבי מסדר n** בתוך $\overline{K}$ הוא $\xi \in \overline{K}$ שמקיים $\xi^n = 1$ אבל $\xi^m \neq 1$ לכל $1 \le m < n$.

נניח שיש $\xi \in \overline{K}$ שורש יחידה פרימיטיבי מסדר n וניקח $L = K(\xi)$, הרחבה זאת נקראת **הרחבה ציקלוטומית**.

1. כל אוטומורפיזם $\sigma \in \mathrm{Aut}(L/K)$ שולח את ξ לאיבר מהצורה ξ^a עם $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ (חבורת היחידות/כפלית של החוג $\mathbb{Z}/n\mathbb{Z}$)
2. $\mathrm{Aut}(L/K) \simeq G \le (\mathbb{Z}/n\mathbb{Z})^\times$

1.4 שדה פיצול של פולינום

הגדרה 1.10 (שדה פיצול): יהי $f \in K[x]$. שדה ההרחבה L/K ייקרא **שדה פיצול** של f אם

1. f מתפצל ב־L (מתפרק לחלוטין לגורמים לינאריים)
2. L מינימלי עם תכונה זו ביחס להכלת שדות (אם $K \subseteq L' \subseteq L$ ו־f מתפצל כבר מעל L' אז $L' = L$)
3. שדה פיצול של פולינום הוא יחיד עד־כדי איזומורפיזם

1.5 הרחבות ספרביליות

הגדרה 1.11 (שורש פשוט): נאמר ש־$\alpha = \alpha_i \in L$ הוא **שורש פשוט (simple root)** של f אם הוא מופיע בידיוק פעם אחת בפיצול.
כלומר, $(t-\alpha) \mid f$ אבל $(t-\alpha)^2 \nmid f$.

הגדרה 1.12 (שורש מרובה): נאמר ש־$\alpha = \alpha_i \in L$ הוא **שורש מרובה (multiple root)** של f אם הוא מופיע בפיצול לכל הפחות פעמיים.
כלומר אם $(t-\alpha)^2 \mid f$.

הגדרה 1.13 (פולינום ספרבילי): הפולינום $f \in K[t]$ נקרא **ספרבילי/פריד** אם אין לו שורשים מרובים בשדה ההרחבה L בו הוא מתפצל.

טענה 1.4 (תנאים לספרביליות):

1. פולינום הוא ספרבילי אם ורק אם $\gcd(f, f') = 1$
2. בשדה ממציין 0 כל פולינום אי־פריק הוא ספרבילי
3. אם α הוא שורש של f אז α שורש מרובה של f אם ורק אם $f'(\alpha) = 0$

הגדרה 1.14 (איבר ספרבילי): $\alpha \in L$ ייקרא **ספרבילי/פריד** מעל K אם הפולינום המינימלי שלו מעל K הוא ספרבילי.

הגדרה 1.15 (הרחבה ספרבילית): הרחבה L/K שכל איבריה ספרביליים תקרא **הרחבה ספרבילית**.

טענה 1.5 (טענות על הרחבות ספרביליות):

1. בשדה ממציין 0, כל הרחבה אלגברית היא הרחבה ספרבילית
2. ספרביליות היא תכונה טרנזטיבית – אם L/K הרחבה ספרבילית ו־$K \subseteq M \subseteq L$ הוא שדה ביניים אז $L/M, M/K$ הן הרחבות ספרביליות
3. אם אנחנו במציין $p \neq 0$ ו־$\gcd([L:K],p)=1$ אז L/K הרחבה ספרבילית
4. תנאים שקולים לספרביליות
   1. ההרחבה L/K היא ספרבילית
   2. יש קבוצת יוצרים של L מעל K שכל איבריה ספרביליים
   3. כל קבוצת יוצרים של L מעל K מורכבת מאיברים ספרביליים
5. פיצול של פולינום ספרבילי הוא הרחבה ספרבילית
6. כל הרחבה סופית פרידה היא פרימיטיבית

1.6 הרחבות נורמליות

הגדרה 1.16 (הרחבת שדות נורמלית): הרחבת שדות אלגברית L/K נקראת **נורמלית** אם כל פולינום אי־פריק מעל K עם שורש ב־L מתפצל לחלוטין ב־L.

בדומה לכך שנורמליות של חבורות זו לא תכונה טרנזטיבית, גם נורמליות של הרחבות איננה טרנזטיבית (יש מקרים תחת תנאים מסויימים שכן, כמו לדוגמה שאם L/K הרחבה נורמלית סופית ו־M שדה ביניים אז גם L/M הרחבה נורמלית)

1.7 רזולטנטה, cubic resolvent, רזולטנטה וכד'

הגדרה 1.17 (cubic resolvent): אם f פולינום ספרבילי ואי־פריק מדרגה 4 מעל שדה K ממציין שונה מ־2 ונניח ש־L שדה פיצול של f.

אנחנו יודעים ש־$G := \mathrm{Gal}(L/K)$ פועלת טרנזטיבית על שורשי f והיא איזומורפית לתת־חבורה טרנזטיבית של S_4.

נסמן $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ את השורשים של f ונגדיר

$$\left\{ \underbrace{\alpha_1\alpha_2+\alpha_3\alpha_4}_{:=\beta_1}, \underbrace{\alpha_1\alpha_3+\alpha_2\alpha_4}_{:=\beta_2}, \underbrace{\alpha_1\alpha_4+\alpha_2\alpha_3}_{:=\beta_3} \right\}$$

אז **cubic resolvent** של f הוא $R_f = \prod_{i=1}^{3}(x-\beta_i)$ והוא אינווריאנטי תחת G ולכן הוא $R_f \in K[x]$

2 איך נעה מפרקת

1. **ל'זנדר**

הגדרה 2.1 (סמל לז'נדר): יהי p מספר ראשוני ($p \neq 2$) ו־$a \in \mathbb{Z}$, אז

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod p \\ 1 & a \not\equiv 0 \pmod p \wedge a \equiv x^2 \pmod p \ (\text{זר ל־} a \text{ והוא שארית ריבועית מודלו } p) \\ -1 & a \not\equiv 0 \pmod p \wedge a \not\equiv x^2 \pmod p \ (\text{זר ל־} a \text{ ואינו שארית ריבועית מודלו } p) \end{cases}$$

למה 2.1: נניח ש־p ראשוני אי־זוגי.

1. כדי לבדוק אם לפולינום ריבועי ax^2+bx+c מעל שדה $\mathbb{F}_p$ יש פירוק, מספיק לבדוק אם סמל לז'נדר $\left(\frac{b^2-4ac}{p}\right)$ הוא 1 או -1.
אם הוא 1, זה אומר שיש ב־$\mathbb{F}_p$ שורש ל־b^2-4ac ואפשר להשתמש בנוסחת השורשים (שנותנת גם פירוק לפולינום מהצורה $a \cdot (x-r) \cdot$ $(x-s)$ כאשר a המקדם המוביל ו־r, s השורשים).
2. כדי לבדוק עבור פולינום מהצורה x^2-c, מספיק לבדוק את סמל לז'נדר $\left(\frac{c}{p}\right)$ (שאומר לנו האם יש פיתרון למשוואה $x^2 = c \pmod p$)

משפט 2.1 (משפט ההדדיות הריבועית): אם p, q ראשוניים אי־זוגיים, מתקיים

.1
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

.2
$$\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

.3
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

היתרון של השיטה – אם גילינו שיש ערך שעבורו סימן ל'זנדר הוא -1 אז לא צריך לעבוד יותר וזה לא מתפרק.
משפט ההדדיות עוזר מאוד לדברים סימטריים.

2. **קריטריון אייזנשטיין** נניח ש־$\mathbb{Z}[t] \ni f = \sum_{i=0}^{n} a_i t^i$ ו־$p \in \mathbb{N}$ ראשוני כך שמתקיימים הבאים
   1. $p \nmid a_n$
   2. $p \mid a_i$ לכל $0 \leq i < n$
   3. $p^2 \nmid a_0$

   אז f אי־פריק.

   הערה: טריק לאי־פריקות זה לנסות לפעמים עם $x = t - 1$
3. **תנאים לקיום שורש – Rational root theorem**
$f \in \mathbb{Q}[x]$ עם מקדמים שלמים ונסמן $f(x) = a_n x^n + \cdots + a_1 x + a_0$. אם $\frac{r}{s} \in \mathbb{Q}$ שורש של f אז $s \mid a_n, r \mid a_0$
4. **הלמה של גאוס**
עבור פולינום $f(t) = \sum_{i=0}^{n} a_i t^i \in \mathbb{Z}[t]$, $\mathrm{cont}(f) = \gcd(a_0, \cdots, a_n)$ ופולינום הוא פרימיטיבי אם ורק אם $\mathrm{cont}(f) = 1$.
מלמת גאוס הראשונה $\mathrm{cont}(fg) = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$ ו־fg פרימיטיבי אם ורק אם f, g פרימיטיביים.
מלמת גאוס השנייה, f פולינום אי־פריק ב־$\mathbb{Z}[t]$ אם ורק אם f פרימיטיבי ואי־פריק ב־$\mathbb{Q}[t]$
5. **עם הדיסקרמינטה**
פולינום f מדרגה 2 הוא אי־פריק אם הדיסקרמיננטה של הפולינום ככר ריבוע בשדה.

3 טריקים שטריקים

1. כשאני מקבלת ביטוי ξ_n כלשהו, שווה לכתוב אותו מפורשות, כלומר $\xi_n^k = e^{\frac{2\pi i k}{n}} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$ זה לפעמים מפשט מאוד
2. "perfect square" תמיד מסתיים באחת מהספרות $\{0,1,4,5,6,9\}$ אז אם מספרר מסתיים ב־$\{2,3,7,8\}$ הוא לא "perfect square", זה עוזר לקצר בדיקות
3. דיסקרמיננטות
   1. מדרגה 2 – $\Delta = b^2 - 4ac$
   2. מדרגה 3 – $\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$
   3. מדרגה 4 –
4. חבורות גלואה עבור פולינום מדרגה 4 – f פולינום אי־פריק מדרגה 4, D_f הדיסקרמיננטה ו־R_f נסמן את cubic resolvent, $G_f = \mathrm{Gal}(L/K), \mathrm{char}(K) \neq 2$
   1. $G_f = S_4$ אם ורק אם R_f הוא אי־פריק מעל K ו־D_f הוא לא ריבוע ב־K
   2. $G_f = A_4$ אם ורק אם R_f אי־פריק מעל K ו־D_f ריבוע ב־K
   3. $G_f = V$ אם ורק אם R_f מתפצל לחלוטין מעל K (ואז בהכרח D_f ריבוע ב־K)
   4. $G_f = D_4 \vee G_f = C_4$ אם ורק אם ל־R_f יש בידיוק שורש אחד ב־K

4 דוגמאות

4.1 דברים עם כמויות

דוגמה 4.1 (*כמה אוטומורפיזמים יש*): אם $p>0$ ראשוני, אז עבור $n\in\mathbb{N}$ מתקיים $\mathrm{Aut}\left(\mathbb{F}_{p^n}\right)\cong\mathbb{Z}/n\mathbb{Z}$

4.2 איך מוצאים שדה פיצול של פולינום מעל $\mathbb{F}_p$

דוגמה 4.2: בדרך־כלל זה שאלות מהסגנון $t^8-1\in\mathbb{F}_7[t]$ ורוצים שדה פיצול מעל $\mathbb{F}_7$.
אנחנו רוצים להרחיב את $\mathbb{F}_7$ כדי ששורש יחידה פרימיטיבי מסדר 8 יהיה בו, אז חייב להתקיים ש־8 מחלק את הסדר של החבורה הכפלית שהיא מסדר 7^n-1, אז נמצא את ה־n המינימלי כך ש־$8\mid 7^n-1$

$$7^1-1\underset{\mathrm{mod}\,8}{\equiv}6,\ 7^2-1=48\underset{\mathrm{mod}\,8}{\equiv}0$$

ולכן שדה הפיצול הוא $\mathbb{F}_{49}$.

4.3 מגדלים

דוגמה 4.3: תהיינה $F\subseteq E\subseteq K$ הרחבות סופיות.

1. אם E/F ו־K/E ספרביליות אזי גם K/F ספרבילית – **הטענה נכונה.**
הרחבה ספרבילית = כל איבר בהרחבה הוא ספרבילי, כלומר הפולינום המינימלי של כל איבר כזה הוא פולינום ספרבילי (אין לו שורשים מרובים בשדה ההרחבה) מעל שדה הבסיס.
מהיות E/F הרחבה ספרבילית נובע כי כל $\alpha\in E$ ספרבילי ומהיות K/E הרחבה ספרבילית נובע כי כל $\beta\in K$ ספרבילי מעל E.
נזכר שהרחבה היא ספרבילית אם ורק אם דרגת ההרחבה שווה לדרגת הספרביליות, כלומר מתקיים

$$[K:F]_s=[K:E]_s\cdot[E:F]_s=[K:E]\cdot[E:F]$$

לו לא היה נתון שההרחבות סופיות, זה כמובן לא היה עובד: נניח ש־K/E, E/F לאו דווקא הרחבות סופיות אך עדיין ספרביליות. ניקח $\alpha\in K$ ונניח כי $a_0,\cdots,a_n\in\in E$ הם המקדמים של הפולינום המינימלי של α מעל E ואז ההרחבה $F(\alpha,a_0,\cdots,a_n)/F$ זו הרחבה סופית ונגדיר

$$M:=F(\alpha,a_0,\cdots,a_n)\cap E$$

אז $M\subseteq E$ ו־M/F היא הרחבה ספרבילית והפולינום המינימלי של α מעל M זהה לפולינום מעל E ולכן ספרבילי, ואז $F(\alpha,a_0,\cdots,a_n)/F$ היא הרחבה ספרבילית מהמקרה הסופי שהוכחנו.

2. אם K/F ספרבילית אז גם E/F ו־K/E הן הרחבות ספרביליות –**הטענה נכונה.**
נראה ש־K/E הרחבה ספרבילית: ניקח $\alpha\in K$ ואז f הפולינום המינימלי של α מעל F ו־g הפולינום המינימלי מעל E. מההנחה, f ספרבילי.
מצד שני, $f\in E[x]$ ו־$f(\alpha)=0$ ולכן $g\mid f$.
נסתכל על השורשים של f ו־g ב־$\overline{E}$ (הסגור האלגברי). מהיות f ספרבילי נובע שאין לו שורשים כפולים. אבל $g\mid f$ ולכן השורשים של g הם חלק מהשורשים של f ולכן ל־g אין שורשים כפולים ב־$\overline{K}$ ולכן g ספרבילי.
ההרחבה E/F נובעת ישירות מהגדרת ההרחבה הספרבילית.

3. אם E/F ו־K/E נורמליות אז K/F נורמלית – הטענה **לא נכונה.** נבנה הרחבות נורמליות $F/K,L/F$ כך שההרחבה L/K לא נורמלית.
נבחר $K=\mathbb{Q},F=\mathbb{Q}\left(\sqrt{2}\right),L=\mathbb{Q}\left(\sqrt[4]{2}\right)$.
אנחנו כבר יודעים ש־$F/K=\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ היא נורמלית (הרחבה ריבועית היא נורמלית) וגם $L/K=\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ היא איננה נורמלית כי הפולינום המינימלי של ההרחבה הוא x^4-2 ולא כל השורשים נמצאים בהרחבה $(i\sqrt[4]{2},-i\sqrt[4]{2})$.
נטען כעת שההרחבה $L/F=\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)$ היא נורמלית.
נסתכל על הפולינום $x^2-\sqrt{2}$ הוא אי־פריק מעל $\mathbb{Q}\left(\sqrt{2}\right)$ ושורשיו הם $\pm\sqrt[4]{2}\in\mathbb{Q}\left(\sqrt[4]{2}\right)$ וזו בידיוק ההגדרה לנורמליות (כי הוא מתפצל לחלוטין עכשיו ב־L), ולכן L/F הרחבה נורמלית.

4. אם K/F נורמלית אז גם E/F ו־K/E נורמלית – **הטענה לא נכונה.**
השדה K הוא שדה פיצול מעל F של איזה פולינום $f\in F[x]$. בפרט, $f\in E[x]$ ו־K הוא בהכרח גם שדה הפיצול של f מעל E ולכן K/E נורמלית.
אבל E/F לא נורמלית! ניקח $F=\mathbb{Q},E=\mathbb{Q}\left(\sqrt[3]{2}\right),K=\mathbb{Q}\left(\sqrt[3]{2},\xi_3\right)$. K/F היא נורמלית כשדה פיצול של x^3-2 אבל E/F איננה נורמלית כי $\sqrt[3]{2}$ הוא שורש של x^3-2 אבל אין לו את ההצמדה המורכבת (K/E כן נורמלית כהרחבה מדרגה 2).

דוגמה 4.4: אם E/F ו־K/E הרחבות אלגבריות אז גם K/F היא הרחבה אלגברית.
יהי $\beta \in K$, בגלל ש־K/E הרחבה אלגברית אז β אלגברי מעל E ולכן יש $g(x) \in E[x]$ כך ש־$g(\beta) = 0$.
$g(x)$ הוא עם מקדמים מ־E, כלומר $g(x) = \sum_{i=0}^{n} a_0 x^i = a_0 + a_1 x + \dots + a_n x^n$ כאשר לכל $0 \leq i \leq n$ מתקיים $a_i \in E$.
מכך שההרחבה E/F אלגברית, נובע כי לכל $0 \leq i \leq n$ מתקיים ש־a_i הוא אלגברי מעל F, כלומר יש $f_i(x) \in F[x]$ כך שמתקיים $f_i(a_i) = 0$.
כלומר, a_0 אלגברי מעל F ומתקיים $f_0(a_0) = 0$ ולכן ניתן לבטא את a_0 על־ידי איברים מ־F ולהחליף את a_0 ב־$g(x)$ בביטוי החדש.
לפולינום שנוצר על־ידי החלפות אלו נקרא $h(x) \in F[x]$ כך שמתקיים $h(\beta) = 0$, כלומר β אלגברי מעל F.
β כמובן הייתה בחירה שרירותית ולכן הטענה נכונה לכל $\beta \in K$, כלומר K/F היא הרחבה אלגברית.

דוגמה 4.5: תהיי E/F הרחבת שדות אלגברית ו־$\alpha, \beta \in E$. נסמן ב־m_α^F, m_β^F את הפולינומים המינימליים של α, β מעל F בהתאמה.
1. אם $m_\alpha^F = m_\beta^F$ נראה שלא בהכרח מתקיים ש־$F(\alpha) = F(\beta)$. ניקח $F = \mathbb{Q}$ ו־$\alpha = \sqrt[3]{2}$ ו־$\beta = \beta = \xi_3 \alpha$, $\alpha \neq \beta$ אבל $m_\alpha^F = m_\beta^F$ כי הם שורשים של הפולינום המינימלי $x^3 - 2$.
כמובן שלא מתקיים $F(\alpha) = F(\beta)$ כי $F(\alpha) \subseteq \mathbb{R}$ אבל $F(\beta) \subseteq \mathbb{C}$ (ובפרט $F(\beta) \nsubseteq \mathbb{R}$).
2. אם $m_\alpha^F = m_\beta^F$ נראה שבהכרח מתקיים $F(\beta) \simeq F(\alpha)$. נסמן $m = m_\alpha^F = m_\beta^F$, יש F־הומומורפיזם $F[x] \to F(\alpha)$ כך ש־$x \mapsto \alpha$ ולכן הגרעין הוא (m) ואז $F(\alpha) \simeq F[x]/(m)$.
באותו אופן נקבל $F[x]/(m) \simeq F(\beta)$ אז בהכרח $F(\beta) \simeq F(\alpha)$ כלומר יש F־הומומורפיזם $F(\alpha) \to F(\beta)$ כך ש־$\alpha \mapsto \beta$.
3. אם $m_\alpha^F \neq m_\beta^F$ נראה שלא בהכרח מתקיים ש־$F(\beta) \not\simeq F(\alpha)$.
ניקח $F = \mathbb{Q}$ ואת $\alpha = \sqrt{2}$ ולכן $F(\alpha) = \mathbb{Q}\left(\sqrt{2}\right)$ ו־$m_\alpha^F = x^2 - 2$ וניקח $\beta = 1 + \sqrt{2}$ ולכן m_β^F יהיה

$$x = 1 + \sqrt{2} \iff x - 1 = \sqrt{2} \iff (x-1)^2 = 2 \iff x^2 - 2x - 1 = 0$$

ולכן $m_\beta^F = x^2 - 2x - 1$ ומתקיים $F(\beta) = \mathbb{Q}\left(1 + \sqrt{2}\right)$ אבל נשים לב ש־$F(\beta) \simeq F(\alpha)$ כי כל איבר ב־$F(\alpha)$ הוא מהצורה $a + \sqrt{2}b$ עבור $a, b \in \mathbb{Q}$ וכל האיבר ב־$F(\beta)$ הוא מהצורה $a + b\left(1 + \sqrt{2}\right)$ עבור $a, b \in \mathbb{Q}$ אז מספיק שנבחר $c = a + b \in \mathbb{Q}$.

4.4 מלא חבורות גלואה

דוגמה 4.6: כל שדה פיצול שיש לו 4 שורשים שהם רק מחליפים סימן ביניהם אז החבורת גלואה היא תת־חבורה מסדר 8 של S_4 ויכולה להיות רק D_4 כי היא פועלת טרנזיטיבית על השורשים.
זה בעצם המסקנה מתרגיל 8 שאלה 2 עבור L שדה הפיצול של הפולינום $x^4 - 7x^2 + 7 \in \mathbb{Q}[x]$ וראינו שהשורשים שלו הם $\pm\sqrt{\frac{7 \pm \sqrt{21}}{2}}$.

דוגמה 4.7: עבור $p \neq 3$ ראשוני נגדיר K_p שדה הפיצול של הפולינום $x^9 - 1$ מעל $\mathbb{F}_p$.
נמצא את כל חבורות גלואה האפשריות $G\left(K_p/\mathbb{F}_p\right)$: ראשית, שדה הפיצול הוא יחיד עד־כדי איזומורפיזם וידוע ש־$K_p = \mathbb{F}_p(\xi_9)$, ולכן מטענה שראינו על חבורות גלואה של הרחבות ציקלוטומיות מתקיים $\mathrm{Gal}\left(K_p/\mathbb{F}_p\right) \simeq (\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$.
זו חבורה מגודל 6 וגם $\varphi_{\text{אויילר}}(9) = 6$ ולכן המחלקים האפשריים של חבורה מסדר 6 הם $\{1, 2, 3, 6\}$ אז $\mathrm{ord}_9(p) \in \{1, 2, 3, 6\}$.
אנחנו רוצים למצוא את ה־n המינימלי כך ש־$\mathbb{F}_{p^n}$ מכיל את ξ_9, אז זה בידיוק ה־n המינימלי כך ש־$9 \mid (p^n - 1)$ כאשר $n \in \{1, 2, 3, 6\}$ ו־$p \neq 3$ ראשוני. אז
1. עבור $9 \mid \left(p^1 - 1\right)$ נבחר $p = 19$ שראשוני ואז $19 - 1 = 18 \underset{\text{mod } 9}{\equiv} 0$ כלומר $19 \underset{\text{mod } 9}{\equiv} 1$
2. עבור $9 \mid \left(p^2 - 1\right)$ נשים לב ש־$p = 2$ לא מתאים, עבור $p = 5$ נקבל $25 \underset{\text{mod } 9}{\not\equiv} 1$ אז לא מתאים, עבור $p = 7$ נקבל $49 \underset{\text{mod } 9}{\not\equiv} 1$ אז גם לא מתאים, עבור $p = 9$ כמובן שלא מתאים, $p = 11$ אז $11^2 = 121 \underset{\text{mod } 9}{\not\equiv} 1$ וגם $13^2 = 169 \underset{\text{mod } 9}{\not\equiv} 1$ ועבור $p = 17$ נקבל $17^2 \underset{\text{mod } 9}{\equiv} 1$ כלומר $p = 17$ מקיים את מה שרצינו
3. עבור $9 \mid \left(p^3 - 1\right)$ ברור ש־$p \neq 2$ ואז עבור $p = 5$ נקבל $125 - 1 = 124 \underset{\text{mod } 9}{\not\equiv} 0$ ועבור $p = 7$ נקבל $7^3 = 343 \underset{\text{mod } 9}{\equiv} 1$ אז $p = 7$
4. עבור $9 \mid \left(p^6 - 1\right)$ אם נבחר $p = 2$ נקבל $2^6 = 64 \underset{\text{mod } 9}{\equiv} 1$

דוגמה 4.8: נוכיח שחבורת גלואה של $f(x) = x^3 - 27x + 60 \in \mathbb{Q}[x]$ היא איזומורפית ל־S_3.
ראשית, מקריטריון אייזנשטיין עם $p = 3$ נובע ש־$f(x)$ הוא פולינום אי־פריק מעל $\mathbb{Z}[t]$ ונחשב

$$\mathrm{cont}(f) = \gcd(1, -27, 60) = \gcd(\gcd(1, -27), 60) = \gcd(1, 60) = 1 \Longrightarrow \text{פרימיטיבי } f$$

מהלמה השנייה של גאוס כל פולינום פרימיטיבי ואי־פריק ב־$\mathbb{Z}[x]$ הוא אי־פריק ב־$\mathbb{Q}[x]$ ולכן f אי־פריק ב־$\mathbb{Q}[x]$ (מיותר כי קריטריון אייזנשטיין רלוונטי גם לכל UFD).
הוא ספרבילי כי $f'(x) = 3x^2 - 27$ ומתקיים $f'(x) = 0 \iff x^2 = 9 \iff x \in \pm 3$, אבל $f(3) = 3^3 - 27 \cdot 3 + 60 = 6 \neq 0,\ \ f(-3) = 114 \neq 0$ וראינו ש־x הוא שורש מרובה אם הוא מאפס את הנגזרת, אז אין לו שורשים מרובים.
מהרזולטנטה והדיסקרמיננטה אנחנו יודעים שמתקיים לפולינום מדרגה 3 לפי שאלה במטלה 9

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

במקרה שלנו $a = 1, b = 0, c = -27, d = 60$ ולכן

$$\Delta = 0 + 4 27^3 - 0 - 27 \cdot 60^2 + 0 = -18468 \Longrightarrow |\Delta| = 18468$$

לפי למה 8.5.2 בסיכומי הרצאות של מיכאל, $G_f \simeq A_3$ אם ורק אם $D_f \in \mathbb{Q}$ הוא ריבוע ב־$\mathbb{Q}$ ואחרת $G_f \simeq S_3$.
כדי לקבוע אם האם הוא ריבוע נצטרך לפרק לראשוניים (כי מספר הוא ריבוע שלם אם ורק אם הוא מכפלה של ראשוניים עם חזקות זוגיות).
ראשית 18468 הוא מספר זוגי ובפרט הוא מתחלק ב־$2^2 = 4$ ולכן $18468 = 4617 \cdot 2^2$.
זה כבר לא מתחלק ב־2 ולכן הראשוני הבא שנבחון זה האם $3 \mid 4817$ ואכן $\frac{4817}{3} = 1539$ וגם הוא מתחלק ב־3 כי $\frac{1539}{3} = 513$, אבל גם זה מתחלק ב־3 כי $\frac{513}{3} = 171$ שגם הוא שוב מתחלק ב־3 ואז $\frac{171}{3} = 57$ שגם מתחלק ב־3 כי $\frac{57}{3} = 19$ שכבר לא מתחלק ב־3.
אז $18468 = 2^2 \cdot 3^5 \cdot 19$ ו־19 הוא ראשוני אז אי־אפשר לפרק יותר.
אז זה בפרט אומר ש־18468 הוא לא ריבוע ב־$\mathbb{Q}$ כי בפירוק שלו לראשוניים יש לנו חזקות אי־זוגיות ולכן מהלמה $G_f \simeq S_3$.

דוגמה 4.9: נמצא את הפולינום המינימלי של $\sqrt{2 + \sqrt{2}}$ ונוכיח שחבורת גלואה שלו איזומורפית ל־$\mathbb{Z}_4$.
ראשית נשים לב שמתקיים

$$x = \sqrt{2 + \sqrt{2}} \iff x^2 = 2 + \sqrt{2} \iff x^2 - 2 = \sqrt{2} \iff \left(x^2 - 2\right)^2 = 2 \iff x^4 - 4x^2 + 2 := f(x)$$

זה אכן פולינום מינימלי כי הוא מתוקן, מתאפס בהצבה של $\sqrt{2 + \sqrt{2}}$ והוא אי־פריק מקריטריון אייזנשטיין עבור $p = 2$.
ניזכר שמעל שדה ממציין 0 כל פולינום אי־פריק הוא ספרבילי ולכן f פולינום ספרבילי אז f ספרבילי וניתן לבחון את Gal_f.
נעזר ברמז ונחשב את $\frac{2}{\sqrt{2+\sqrt{2}}}$.
נסמן $\alpha = \sqrt{2 + \sqrt{2}}$ ונשים לב שמתקיים $\alpha^2 = 2 + \sqrt{2}$ כלומר $\sqrt{2} \in \mathbb{Q}(\alpha)$ אז $\mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}(\alpha)$.
נגדיר $\beta = \sqrt{2 - \sqrt{2}}$ ואז

$$\left(\frac{\sqrt{2}}{\alpha}\right)^2 = \frac{2}{\alpha^2} = \frac{2}{2 + \sqrt{2}} = \frac{2\beta^2}{\alpha^2\beta^2} = \frac{2\left(2 - \sqrt{2}\right)}{\left(2 + \sqrt{2}\right)\left(2 - \sqrt{2}\right)} = \frac{4 - 2\sqrt{2}}{4 - 2} = 2 - \sqrt{2}$$

כלומר $\beta = \sqrt{2 - \sqrt{2}} = \frac{\sqrt{2}}{\alpha}$ וזה בדיוק אומר ש־$\beta \in \mathbb{Q}(\alpha)$.
אז בעצם יש לנו 4 שורשים $\pm\alpha, \pm\beta$ מעל המרוכבים וכל השורשים ב־$\mathbb{Q}(\alpha)$ אז זה שדה פיצול של הפולינום וכן $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
אז כל $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ נקבע לפי לאן הוא שולח את α. נניח כי $\sigma(\alpha) = \beta$, אז

$$\sigma\left(\sqrt{2}\right) = \sigma(\alpha^2 - 2) = \sigma(\alpha)^2 - 2 = \beta^2 - 2 = \left(2 - \sqrt{2}\right) - 2 = -\sqrt{2}$$

$$\sigma(\beta) = \sigma\left(\frac{\sqrt{2}}{\alpha}\right) = \frac{\sigma\left(\sqrt{2}\right)}{\sigma(\alpha)} = -\frac{\sqrt{2}}{\beta} \underset{(\star)}{=} -\alpha$$

כאשר $(\star)$ נובע מכך שמתקיים

$$\alpha\beta = \sqrt{2 + \sqrt{2}}\sqrt{2 - \sqrt{2}} = \left(\left(2 + \sqrt{2}\right)\left(2 - \sqrt{2}\right)\right)^{\frac{1}{2}} = \sqrt{2}$$

כלומר קיבלנו $\sigma^2(\alpha) = -\alpha, \sigma^3(\alpha) = -\beta, \sigma^4(\alpha) = \alpha$ משמע מצאנו איבר שהוא יוצר והוא מסדר 4 ולכן בהכרח $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq \mathbb{Z}_4$ שכן יש רק שתי תתי־חבורות מסדר 4 והן חבורת קליין שאין לה איבר מסדר 4 והיא לא ציקלית.

דוגמה 4.10: יהי $\mathbb{F}$ שדה כך ש־$\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{C}$ ונניח כי $\mathbb{F}/\mathbb{Q}$ הרחבה נורמלית סופית ודרגת ההרחבה $[\mathbb{F}:\mathbb{Q}]$ היא אי־זוגית. נראה כי $F \subseteq \mathbb{R}$.
היות ו־$\mathrm{char}(\mathbb{Q}) = 0$ נובע כי כל הרחבה אלגברית היא ספרבילית, ולכן $\mathbb{F}/\mathbb{Q}$ וההרחבה היא נורמלית וסופית ומהתנאים השקולים לסופיות נובע שהיא הרחבה אלגברית. אז ההרחבה היא גלואה מסדר אי־זוגי.
ניקח $\tau : \mathbb{C} \to \mathbb{C}$ הנתון על־ידי $\tau(z) = \overline{z}$ ואנחנו יודעים שלכל $q \in \mathbb{Q}$, $\tau|_{\mathbb{F}}(q) = q$ כלומר $\tau|_{\mathbb{F}} : \mathbb{F} \to \mathbb{C}$ שיכון שמשמר את $\mathbb{Q}$.
אז בהכרח נובע ש־$\tau|_{\mathbb{F}} \in \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ יחד עם הנורמליות.
אנחנו יודעים שלאוטומורפיזם $\tau|_{\mathbb{F}}$ יש סדר 2 כי $\tau^2 = \mathrm{id}$ ב־$\mathbb{C}$ אבל $[\mathbb{F}:\mathbb{Q}] = |\mathrm{Gal}(\mathbb{F}/\mathbb{Q})|$ שהוא מספר אי־זוגי אז האוטומורפיזם היחידי שיכול להיות מסדר 2 יהיה אוטומורפיזם הזהות, כלומר $\tau|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$.
אז כל הצמדה מורכבת משמרת כל ערך ב־$\mathbb{F}$, כלומר כל ערך ב־$\mathbb{F}$ הוא ממשי אז $\mathbb{F} \subseteq \mathbb{R}$.

4.5 שדות ביניים

דוגמה 4.11: יהי E שדה הפיצול של הפולינום $x^9-1\in\mathbb{Q}[x]$ ונמצא במפורש את כל תתי־השדות של E.
מיחידות שדה הפיצול של הפולינום נובע כי $E=\mathbb{Q}(\xi_9)$ ומתקיים מהגדרת ההרחבה הציקלוטומית

$$[\mathbb{Q}(\xi_9):\mathbb{Q}]=\varphi_{\text{אויילר}}(9)=|\{x\in[1,2,3,4,5,6,7,8]\mid\gcd(x,9)=1\}|=|\{1,2,4,5,7,8\}|=6$$

וממשפט שראינו מתקיים $\mathrm{Gal}(\mathbb{Q}(\xi_9)/\mathbb{Q})\simeq(\mathbb{Z}/9\mathbb{Z})^\times\simeq\mathbb{Z}/6\mathbb{Z}$.
בנוסף, $\Phi_9(x)=x^6+x^3+1$ זה הפולינום המינימלי של 1 $\xi_9^9=1$ ולכן $1+\xi_9^3+\xi_9^6$ ולכן $\xi_9^6=-\xi_9^3-1$, נסמן את הטענה הזאת ב־$(\star)$.
מהתאמת גלואה, יש התאמה חד־חד ערכית ועל בין תתי־החבורות של $G\simeq\mathbb{Z}_6(\simeq\mathbb{Z}/6\mathbb{Z})$ לבין שדות ביניים של ההרחבה.
נשים לב ש־G נוצרת על־ידי σ כאשר $\sigma(\xi_9)=\xi_9^2$ ולכן $G=\{\sigma,\sigma^2,\sigma^3,\sigma^4,\sigma^5,1\}$ והתתי־חבורות הלא טריוויאליות הן $H_1=\{\sigma^2,\sigma^4,1\}$ ו־$H_2=\{\sigma^3,1\}$ (מלגראנז' אלו האופציות היחידות שלא טריוויאליות).
אם σ הוא אוטומורפיזם מסדר 2 על שדה F ו־$z\in F$ אז $u=z+\sigma(z)$ נשמר תחת σ, שכן

$$\sigma(u)=\sigma(z+\sigma(z))=\sigma(z)+\sigma^2(z)=\sigma(z)+z=u$$

ואם τ הוא אוטומורפיזם מסדר 3, אז $v=z+\tau(z)+\tau^2(z)$ גם נשמר תחת τ שכן

$$\tau(v)=\tau(z+\tau(z)+\tau^2(z))=\tau(z)+\tau^2(z)+\tau^3(z)=\tau(z)+\tau^2(z)+z=v$$

אז במקרה שלנו, σ^3 היא מסדר 2 ואנחנו מחפשים את האיברים שנשמרים תחת $\sigma^3:\xi_9\mapsto\xi_9^8$ (כלומר, תחת H_2)

$$\xi_9+\sigma^3(\xi_9)=\xi_9+\xi_9^8=\xi_9+\xi_9^{-1}$$
$$\xi_9^2+\sigma^3(\xi_9^2)=\xi_9^2+\xi_9^7=\xi_9^2+\xi_9^{-2}$$
$$\xi_9^3+\sigma^3(\xi_9^3)=\xi_9^3+\xi_9^6=-1$$
$$\xi_9^4+\sigma^3(\xi_9^4)=\xi_9^4+\xi_9^5$$
$$\xi_9^5+\sigma^3(\xi_9^5)=\xi_9^5+\xi_9^4$$

בסיס של ההרחבה הוא $\{1,\xi_9,\cdots,\xi_9^5\}$ ואנחנו רוצים לבטא את $f_1=\xi_9+\xi_9^{-1}=\xi_9+\xi_9^8, f_2=\xi_9^2+\xi_9^7$ בעזרת איברי הבסיס.
אז מ־$(\star)$ נקבל

$$\xi_9^8=\xi_9^2\cdot\xi_9^6=\xi_9^2(-\xi_9^3-1)=-\xi_9^5-\xi_9^2,\qquad\xi_9^7=\xi_9^6\cdot\xi_9=\xi_9(-\xi_9^3-1)=-\xi_9^4-\xi_9$$

כלומר הצלחנו לבטא את f_1,f_2 לפי איברי הבסיס שלנו. אז נכתוב

$$f_1=\xi_9+\xi_9^{-1}=\xi_9+\xi_9^8=\xi_9-\xi_9^5-\xi_9^2$$
$$f_2=\xi_9^2+\xi_9^{-2}=\xi_9+\xi_9^7=\xi_9^2-\xi_9^4-\xi_9$$
$$f_3=-1(\xi_9^6+\xi_9^3=-1,\ \xi_9^{-3}=\xi_9^6)$$

נרצה למצוא את התלות הלינארית ביניהם, כלומר

$$f_1+f_2=(\cancel{\xi_9}-\xi_9^5-\cancel{\xi_9^2})+(\cancel{\xi_9^2}-\xi_9^4-\cancel{\xi_9})=-\xi_9^5-\xi_9^4$$

ובגלל ש־f_1,f_2 נשמרים תחת σ^3 אז גם $f_1+f_2=-\xi_9^5-\xi_9^4$ נשמרים תחת σ^3 ונשים לב שמתקיים $\xi_9^5=\xi_9^{-4}$.
כלומר, שדה השבת מכיל את כל הקומבינציות הסימטריות $\xi_9^k+\xi_9^{-k}$, אז שדה השבת משמר את האיברים שנשארים במקום על־ידי $\xi_9\mapsto\xi_9^{-1}$ ולכן מהתאמת גלואה זה מתאים לתת־שדה מדרגה 3 (כי החבורה מסדר 2) ומהתלות ביניהם נסיק שתת־הרחבה מדרגה 3 תהיה $\mathbb{Q}(\xi_9+\xi_9^{-1})$.
נעשה את אותו התהליך עבור $\sigma^2:\xi_9\mapsto\xi_9^4,\sigma^4:\xi_9\mapsto\xi_9^7$ ואז האיברים שנשארים במקום תחת H_1

$$\xi_9+\sigma^2(\xi_9)+\sigma^4(\xi_9)=\xi_9+\xi_9^4+\xi_9^7=0$$
$$\xi_9^2+\sigma^2(\xi_9^2)+\sigma^4(\xi_9^2)=\xi_9^2+\xi_9^8+\xi_9^5=0$$
$$\xi_9^3+\sigma^2(\xi_9^3)+\sigma^4(\xi_9^3)=\xi_9^3+\left(\xi_9^3\right)^4+\left(\xi_9^3\right)^7=\xi_9^3+\xi_9^{12}+\xi_9^{21}\underset{\bmod 9}{=}\xi_9^3+\xi_9^3+\xi_9^3=3\xi_9^3$$

נשים לב $\xi_9^3=\left(e^{\frac{2\pi i}{9}}\right)^3=e^{\frac{2\pi i}{3}}=\xi_3$ ואנחנו כבר יודעים $\Phi_3(x)=x^2+x+1$ וכן $\varphi_{\text{אויילר}}(3)=|\{x\in[1,2]\}\mid\gcd(x,3)=1|=|\{1,2\}|=2$, כלומר, $\mathbb{Q}(\xi_3)\subseteq\mathbb{Q}(\xi_9)$ וזו הרחבה מדרגה 2.

דוגמה 4.12: נמצא באופן מפורש את כל תתי־שדות של $\mathbb{Q}(\xi_8)$.
נשים לב ש־$\xi_8^8 = 1$ והפולינום המינימלי יהיה $\Phi_8(x) = x^4 + 1$ ולכן $\xi_8^4 = -1$ וממשפט שראינו מתקיים

$$[\mathbb{Q}(\xi_8) : \mathbb{Q}] = |\{x \in \{1,2,3,4,5,6,7\} \mid \gcd(x,8) = 1\}| = |\{1,3,5,7\}| = 4$$

$$\mathrm{Gal}(\mathbb{Q}(\xi_8)/\mathbb{Q})) \simeq (\mathbb{Z}/8\mathbb{Z})^\times = \{1,3,5,7\}$$

יש בדיוק 2 חבורות מסדר 4 והן החבורה הציקלית $\mathbb{Z}_4$ וחבורת קליין, אבל G לא חבורה ציקלית כי אין אף איבר שהוא מסדר 4, ולכן

$$\mathrm{Gal}(\mathbb{Q}(\xi_8)/\mathbb{Q})) \simeq (\mathbb{Z}/8\mathbb{Z})^\times = \{1,3,5,7\} \simeq V_4 \simeq C_2 \times C_2$$

אנחנו יודעים שלחבורת קליין יש 3 תתי־חבורות לא טריוויאליות כולן מסדר 2 והן כולן מתאימות להרחבות מדרגה 2 בגלל המשפט על היחס בין תתי־חבורות והדרגה של ההרחבה.
אנחנו מחפשים את האיברים שנשארים במקום עבור אוטומורפיזמים מסדר 2, ונשים לב שמתקיים

$$\sigma_k(\xi_8) = \xi_8^k \Longrightarrow \begin{cases} \sigma_3^2(\xi_8) = \sigma_3(\xi_8^3) = \xi_8^9 \underset{\bmod 8}{\equiv} \xi_8 \\ \sigma_5^2(\xi_8) = \sigma_5(\xi_8^5) = \xi_8^{25} \underset{\bmod 8}{\equiv} \xi_8 \\ \sigma_7^2(\xi_8) = \sigma_7(\xi_8^7) = \xi_8^{49} \underset{\bmod 8}{\equiv} \xi_1 \end{cases}$$

אז תתי־חבורות של חבורת קליין במקרה זה יהיו $H_1 = \{1, \sigma_3\}, H_2 = \{1, \sigma_5\}, H_3 = \{1, \sigma_7\}$.
ננסה כמו בפעם הקודמת לבדוק את המקרים הסימטריים, כלומר $\xi_8^i + \sigma_k(\xi_8^i) = \xi_8^i + \xi_8^{ik}$ עבור $i \in \{1,2,3\}$ ועבור $k \in \{3,5,7\}$:

$$\boldsymbol{\sigma_3 : \xi_8 \mapsto \xi_8^3} :$$

$$\xi_8 + \sigma_3(\xi_8) = \xi_8 + \xi_8^3, \qquad \xi_8^2 + \sigma_3(\xi_8^2) = \xi_8^2 + \xi_8^6 = \xi_8^2(1 + \xi_8^4) = 0, \qquad \xi_8^3 + \sigma_3(\xi_8^3) = \xi_8^3 + \xi_8$$

$$\boldsymbol{\sigma_5 : \xi_8 \mapsto \xi_8^5} :$$

$$\xi_8 + \sigma_5(\xi_8) = \xi_8 + \xi_8^5 = \xi_8(1 + \xi_8^4) = 0, \qquad \xi_8^2 + \sigma_5(\xi_8^2) = \xi_8^2 + \xi_8^2 = 2\xi_8^2, \qquad \xi_8^3 + \sigma_5(\xi_8^3) = \xi_8^3 + \xi_8$$

$$\boldsymbol{\sigma_7 : \xi_8 \mapsto \xi_8^7} :$$

$$\xi_8 + \sigma_7(\xi_8) = \xi_8 + \xi_8^7, \qquad \xi_8^2 + \sigma_7(\xi_8^2) = \xi_8^2 + \xi_8^6 = \xi_8^2(1 + \xi_8^4) = 0, \qquad \xi_8^3 + \sigma_7(\xi_8^3) = \xi_8^3 + \xi_8^5$$

מהמקרה הראשון נקבל ש־$\xi_8 + \xi_8^3$ נשמר תחת σ_3 ונשים לב

$$\xi_8 + \xi_8^3 = e^{\frac{2\pi i}{8}} + \left(e^{\left(2\pi \frac{i}{8}\right)}\right)^3 = e^{\frac{\pi i}{4}} + e^{\frac{3\pi i}{4}} = \cos\left(\frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{4}\right) + \cos\left(\frac{3\pi}{4}\right) + \sin\left(\frac{3\pi}{4}\right) =$$

$$\frac{\sqrt{2}}{2} + \frac{i\sqrt{2}}{2} - \frac{\sqrt{2}}{2} + \frac{i\sqrt{2}}{2} = i\sqrt{2}$$

מהמקרה השני נקבל ש־$2\xi_8^2 = \xi_8^2 + \xi_2$ נשמר תחת σ_5 ונשים לב

$$\xi_8^2 = e^{\frac{4\pi i}{8}} = e^{\frac{\pi i}{2}} = \cos\left(\frac{\pi}{2}\right) + i \sin\left(\frac{\pi}{2}\right) = 0 + i = i$$

מהמקרה השלישי נקבל ש־$\xi_8 + \xi_8^7$ נשמר תחת σ_7 והפעם

$$\xi_8 + \xi_8^7 = e^{\frac{2\pi i}{8}} + \left(e^{\left(2\pi \frac{i}{8}\right)}\right)^7 = e^{\frac{\pi i}{4}} + e^{\frac{7\pi i}{4}} = \cos\left(\frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{4}\right) + \cos\left(\frac{7\pi}{4}\right) + \sin\left(\frac{7\pi}{4}\right) =$$

$$\frac{\sqrt{2}}{2} + \frac{i\sqrt{2}}{2} + \frac{\sqrt{2}}{2} - \frac{i\sqrt{2}}{2} = \sqrt{2}$$

אז בסך־הכל מצאנו $\mathbb{Q}(i), \mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}\left(i\sqrt{2}\right)$ שדות ביניים, ומהתאמת גלואה אנחנו יודעים שזה בדיוק כולם.

דוגמה 4.13: נמצא את כל השדות ביניים של ההרחבה $\mathbb{Q}(\xi)$ כאשר $\xi = e^{\frac{2\pi i}{7}}$.
ראשית ניזכר $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ אז

$$\xi^6 + \xi^5 + \xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0 \Longrightarrow \xi^6 + \xi^5 + \xi^4 + \xi^3 + \xi^2 + \xi = -1(\star)$$

בנוסף, ממשפט שראינו מתקיים

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = |\{x \in \{1, \cdots, 6\} \mid \gcd(x, 7) = 1\}| = |\{1, 2, 3, 4, 5, 6\}| = 6$$
$$\Longrightarrow G \coloneqq \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \simeq (\mathbb{Z}/7\mathbb{Z})^{\times} = \{1, 2, 3, 4, 5, 6\} \simeq \mathbb{Z}_6$$

אנחנו צריכים למצוא g כך שיתקיים $\{1, 2, 3, 4, 5, 6\} = \{g^0, g^1, g^2, g^3, g^4, g^5\} \bmod 7$.
אז $g = 1, g = 2$ לא מתאימים. נבחן את $g = 3$ ונקבל

$$3^1 \underset{\bmod 7}{\equiv} 3, 3^2 = 9 \underset{\bmod 7}{\equiv} 2, 3^3 = 27 \underset{\bmod 7}{\equiv} 6, 3^4 = 81 \underset{\bmod 7}{\equiv} 4, 3^5 = 243 \underset{\bmod 7}{\equiv} 5$$

אז $\langle\sigma\rangle$ עם $\sigma(\xi) = \xi^3$ הוא יוצר של החבורה שלנו וניתן להבין ככה בצורה קלה יותר את תתי־החבורות של G: מלבד הטריוויאלית הגדולה והקטנה, תת־חבורה מסדר 3 תהיה $\langle\sigma^2\rangle$ ותת־חבורה מסדר 2 תהיה $\langle\sigma^3\rangle$ שמהתאמת גלואה יביאו שדות ביניים מדרגות 2 ו־3 בהתאמה. ונשים לב שעם המחזוריות של פונקציות סינוס וקוסינוס מתקיים

$$\sigma^3(\xi) = \left(\xi^3\right)^3 = \xi^{27} \underset{\bmod 7}{\equiv} \xi^6 = \xi^{-1}$$

כלומר, $\sigma^3 : \xi \mapsto \xi^{-1}$ ונשים לב שבאותו אופן גם $\xi^5 = \xi^{-2}, \xi^4 = \xi^{-3}$ $(\star\star)$ ומתקיים

$$\sigma^3\left(\xi + \xi^{-1}\right) = \sigma^3(\xi) + \sigma^3(x)^{-1} = \xi^{-1} + \left(\xi^{-1}\right)^{-1} = \xi^{-1} + \xi$$

כלומר $\mathbb{Q}\left(\xi + \xi^{-1}\right) \subseteq \mathrm{Fix}\left(\langle\sigma^3\rangle\right)$ אבל מטעמי גודל נסיק שיש הכלה גם בכיוון השני: אם נגדיר $t \coloneqq \xi + \xi^{-1}$ אז מ־$(\star)$ נקבל

$$t_1 = t, t_2 = \xi^2 + \xi^{-2}, t_3 = \xi^3 + \xi^{-3} \Longrightarrow (\star) = t_1 + t_2 + t_3 = -1$$
$$t_1 t_2 + t_1 t_3 + t_2 t_3 = \left(\xi + \xi^{-1}\right)\left(\xi^2 + \xi^{-2}\right) + \left(\xi + \xi^{-1}\right)\left(\xi^3 + \xi^{-3}\right) + \left(\xi^2 + \xi^{-2}\right)\left(\xi^3 + \xi^{-3}\right)$$
$$= \xi^3 + \xi^{-1} + \xi + \xi^{-3} + \xi^4 + \xi^{-2} + \xi^2 + \xi^{-4} + \xi^5 + \xi^{-1} + \xi + \xi^{-5} \underset{(\star),(\star\star)}{=} \sum_{i=1}^{5} 2\xi^i = -2$$
$$t_1 t_2 t_3 = \left(\xi + \xi^{-1}\right)\left(\xi^2 + \xi^{-2}\right)\left(\xi^3 + \xi^{-3}\right) = \left(\xi^3 + \xi^{-1} + \xi + \xi^{-3}\right)\left(\xi^3 + \xi^{-3}\right) = \xi^6 + \xi^0 + \xi^2 + \xi^{-4} + \xi^4 + \xi^{-2} + \xi^0 + \xi^{-6}$$
$$\underset{\substack{\xi^{-6} = \xi, \\ (\star\star)}}{\equiv} 1 + 1 + \xi + \xi^2 + \xi^3 + \xi^4 + \xi^5 + \xi^6 \underset{\substack{(\star), \\ \xi + \xi^2 + \xi^3 + \xi^4 + \xi^5 + \xi^6 = -1}}{=} 1 + 1 - 1 = 1$$

כלומר באמצעות הפולינומים הסימטריים נקבל את הפולינום $x^3 + x^2 - 2x + 1$ והוא פולינום אי־פריק מעל $\mathbb{Q}$:
באמצעות Rational root theorem שורשים אפשריים הם ± 1 והוא לא מתאפס לאף־אחד מהם.
אז זה פולינום אי־פריק מדרגה 3 והוא הפולינום המינימלי של $\mathbb{Q}(t_1, t_2, t_3)/\mathbb{Q}$ ומההומומורפיזם שראינו, נובע שההרחבה $\mathbb{Q}\left(\xi + \xi^{-1}\right)/\mathbb{Q}$ היא הרחבה מדרגה 3.
נשאר לעשות את אותו התהליך עבור $\sigma^2(\xi) = \left(\xi^3\right)^2 = \xi^9 \underset{\bmod 7}{\equiv} \xi^2 = \xi^{-5}$, כלומר $\sigma^2 : \xi \mapsto \xi^2$ ואכן

$$\sigma^2\left(\xi + \xi^2 + \xi^4\right) = \sigma^2(\xi) + \sigma^2(\xi)^2 + \sigma^2(\xi)^4 = \xi^2 + \xi^4 + \xi^8 \underset{\bmod 7}{\equiv} \xi + \xi^2 + \xi^4$$

כלומר שוב $\mathbb{Q}\left(\xi + \xi^2 + \xi^4\right) \subseteq \mathrm{Fix}\left(\langle\sigma^2\rangle\right)$ וצריך להראות ש־$\left[\mathbb{Q}\left(\xi + \xi^2 + \xi^4\right) : \mathbb{Q} = 2\right.$ וזה יסיים.
נגדיר $\eta = \xi + \xi^2 + \xi^4, \eta' = \xi^3 + \xi^5 + \xi^6$ ומתקיים

$$\eta + \eta' \underset{(\star)}{=} -1,\ \eta\eta' = \sum_{i \in 1,2,4} \sum_{j \in 3,5,6} \xi^{i+j} = \xi^4 + \xi^6 + \xi^0 + \xi^5 + \xi^0 + \xi + \xi^0 + \xi^2 + \xi^3 \underset{(\star)}{=} 3 + (-1) = 2$$

ובאותו אופן מהפולינומים הסימטריים נקבל

$$(x - \eta)(x - \eta') = x^2 - (\eta + \eta')x + 2 = x^2 + x + 2$$

הוא הפולינום המינימלי והוא אי־פריק כי הדיסקרמיננטה שלו היא לא ריבוע ב־$\mathbb{Q}$ $\left(\Delta = b^2 - 4c = 1 - 8 = -7 \notin \mathbb{Q}^2\right)$, הפולינום מדרגה 2 ולכן $[\mathbb{Q}(\eta) : \mathbb{Q}] = \left[\mathbb{Q}\left(\xi + \xi^2 + \xi^4\right) : \mathbb{Q}\right] = 2$ ועל־כן $\mathbb{Q}\left(\xi + \xi^2 + \xi^4\right) = \mathrm{Fix}\left(\langle\sigma^2\rangle\right)$ ומצאנו את כל השדות ביניים.

דוגמה 4.14: נמצא את כל השדות ביניים של ההרחבה $\mathbb{Q}\left(\sqrt{5},\sqrt{i}\right)/\mathbb{Q}$.
מהאי־תלות של $\sqrt{5}$ ו־i (אחד מורכב והשני ממשי) נוכל להשתמש בטענה על דרגת מגדל הרחבות ולקבל

$$\left[\mathbb{Q}\left(\sqrt{5},i\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{5}\right):\mathbb{Q}\right]\cdot[\mathbb{Q}(i):\mathbb{Q}]2\cdot 2=4$$

ונשים לב ש־$\mathbb{Q}(i)/\mathbb{Q},\mathbb{Q}\left(\sqrt{5}\right)/\mathbb{Q}$ הן גלואה כי הפולינום המינימלי של שתיהן אי־פריק מעל $\mathbb{Q}$ ובגלל שאנחנו במציין 0 כל אי־פריק הוא ספרבילי ולכן גלואה.
כלומר $K=\mathbb{Q}\left(\sqrt{5},\sqrt{i}\right)$ הוא הקומפזיטום של ההרחבות $\mathbb{Q}\left(\sqrt{5}\right),\mathbb{Q}(i)$ ולפי טענה שראינו הוא גלואה (גם תרגיל 17.34 בספר שאלה 3) וההרחבה מדרגה 4.
אז האוטומורפיזמים האפשריים הם $\mathrm{id};\ \sigma:\sqrt{5}\mapsto-\sqrt{5},i\mapsto i;\ \tau:\sqrt{5}\mapsto\sqrt{5},i\mapsto-i;\ \tau\sigma:\sqrt{5}\mapsto-\sqrt{5},i\mapsto-i$ וזה בידיוק המבנה של חבורת קליין.
לחבורת קליין יש בידיוק 3 תתי־חבורות לא טריוויאליות, כולן מסדר 2 וממשפט גלואה יש התאמה חד־חד ערכית ועל בין תתי־חבורות לבין שדות ביניים.
אז תתי־החבורות הן $\langle\sigma\rangle,\langle\tau\rangle\langle\tau\sigma\rangle$ והן בהתאמה מביאות את השדות $\mathbb{Q}(i),\mathbb{Q}\left(\sqrt{5}\right),\mathbb{Q}\left(i\sqrt{5}\right)$.

4.6 שדות פיצול

דוגמה 4.15: נרצה למצוא את E, שדה הפיצול של x^6-2 מעל $\mathbb{Q}$ ולמצוא מה החבורת גלואה של $E/\mathbb{Q}$.
ראשית, x^6-2 הוא פולינום אי־פריק מקריטריון אייזנשטיין עבור $p=2$ ונשים לב ששורשי הפולינום הזה הם $x=\sqrt[6]{2}\xi_6^k,k\in\{0,1,2,3,4,5\}$ (כי $2=2\cdot e^{i\cdot 0}$ ולכן שורש הוא מהצורה $z_k=r^{\frac{1}{n}}\cdot e^{\frac{i(\theta+2\pi k)}{n}}$ עבור $r=2,\theta=0,n=6$ ולכן יש חלק מרוכב לשורש).
היות ו־$\sqrt[6]{2},\xi_6$ הם בלתי־תלויים לינארית (כי $\xi_6=e^{\frac{2\pi i}{6}}=e^{\frac{\pi i}{3}}=\cos\left(\frac{\pi}{3}\right)+i\sin\left(\frac{\pi}{3}\right)=\frac{1}{2}+\frac{i\sqrt{3}}{2}$ ולכל הפחות, $i\notin\mathbb{Q}\left(\sqrt[6]{2}\right)$ ואנחנו יודעים ש־$\left(\mathbb{Q}(\xi_6)=\mathbb{Q}\left(i,\sqrt{3}\right)\right)$ אז שדה הפיצול הוא השדה שיכיל את כלל השורשים, כלומר $E=\mathbb{Q}\left(\xi_6,\sqrt[6]{2}\right)$ וזו הרחבה מדרגה 12 בגלל כפליות מגדל ההרחבות, ולכן גם חבורת גלואה היא חבורה מסדר 12. נסמן $\alpha=\sqrt[6]{2},\xi=\xi_6$ ואז כל השורשים שם $\alpha\xi^k$ עבור $k\in\{0,1,2,3,4,5\}$.
מהתאמת גלואה, אנחנו יודעים שכל $\sigma\in\mathrm{Gal}(E/\mathbb{Q})$ מקיים

$$\alpha\mapsto\xi^k\alpha,\ k\in\{0,1,2,3,4,5\},\ \xi\mapsto\xi^\ell,\ \ell\in(\mathbb{Z}/6\mathbb{Z})^\times=\{1,5\}$$

כאשר עבור ℓ זה נובע ממה שראינו על הרחבות ציקלוטומיות, כי אחרת אנחנו כבר יודעים שהם לא משמרים מבנה של אוטומורפיזם.
אז כל σ כזה נקבע על־ידי $\sigma_{(a,b)}:\alpha\mapsto\xi^a\alpha,\xi\mapsto\xi^b$ עבור $a\in\{0,1,2,3,4,5\}$ ו־$b\in\{1,5\}$ וכל אוטומורפיזם כזה צריך לכבד את מבנה השדה, כלומר

$$\sigma(\xi\alpha)=\sigma(\xi)\sigma(\alpha)=\xi^b\cdot\xi^a\alpha=\xi^{a+b}\alpha$$

יש לנו 6 בחירות לאן α נשלח ו־2 בחירות עבור ξ ולכן $\mathrm{Gal}(E/\mathbb{Q})\simeq D_6\simeq C_6\rtimes C_2$, כי כל אוטומורפיזם פועל בצורה של סיבוב ושיקוף על ששת שורשי הפולינום וכלל השורשים נמצאים על מעגל היחידה במישור המרוכב.
נשים לב שלא ייתכן כי החבורה היא C_{12} או $C_6\times C_2$ בגלל שהחבורת גלואה שלנו היא לא אבלית כי סיבוב (מכפלה ב־ξ_6) והצמדה מורכבת $\xi_6\mapsto\xi_6^{-1}$ הן לא פעולות קומוטטיביות.
זה לא יכול להיות A_4 כי A_4 היא חבורה פשוטה ואין לה תת־חבורה נורמלית מסדר 6 אבל אנחנו גם יודעים שיש לחבורת גלואה שלנו תת־חבורה מסדר 6 שהיא גם נורמלית (פעולת הסיבוב גוררת נורמליות).

יש לנו את הפולינום x^3-5 אז $x^3=5$ אז שורשי הפולינום הם $\sqrt[3]{5}\xi_3^k$ עבור $k\in\{0,1,2\}$, כי אם נכתוב $5=5\cdot e^{i\cdot 0}=5\cdot e^0=5$ אז שורש הוא מהצורה $z_k=r^{\frac{1}{n}}\cdot e^{\frac{i(\theta+2\pi k)}{n}}$ עבור $r=5,\theta=0,n=3$.

4.7 פולינומים סימטריים

דוגמה 4.16: יהיו $\alpha_1, \alpha_2, \alpha_3$ שורשי הפולינום $f(x) = x^3 - 5x^2 + x - 2$ ונחשב את $\alpha_1^3 + \alpha_2^3 + \alpha_3^3$.
ראינו הומומורפיזם $g : \mathbb{Q}[t_1, t_2, t_3, x] \to (\mathbb{Q}(s_1, s_2, s_3))[x]$ המוגדר על־ידי $g(l) = l(\alpha_1, \alpha_2, \alpha_3, x)$.
ניקח s_1, s_2, s_3 הפולינומים הסימטריים האלמנטריים ב־$\mathbb{Q}[t_1, t_2, t_3]$. אז

$$f = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) = g((x-t_1)(x-t_2)(x-t_3)) = x^3 - g(s_1)x^2 + g(s_2)x - g(s_3)$$

כאשר

$$g(s_1) = 5, g(s_2) = 1, g(s_3) = 2$$

אנחנו רוצים לבטא את $l = t_1^3 + t_2^3 + t_3^3$ באמצעות s_1, s_2, s_3 ולפי האלגוריתם שראינו בתרגול $l - s_1^3$ כאשר

$$s_1^3 = (t_1+t_2+t_3)^3 = t_1^3+t_2^3+t_3^3 = (t_1^2+t_2^2+t_3^2+2t_1t_2+2t_1t_3+2t_2t_3)(t_1+t_2+t_3)$$
$$= t_1^3 + t_1t_2^2 + t_1t_3^2 + 2t_1^2t_2 + 2t_1^2t_3 + 2t_1t_2t_3 + t_2^3 + t_2t_1^2 + t_2t_3^2 + 2t_2^2t_1 + 2t_2^2t_3 + 2t_1t_2t_3 + t_3^3 + t_3t_1^2 + t_3t_2^2 + 2t_3^2t_1 + 2t_3^2t_2 + 2t_1t_2t_3$$
$$= t_1^3+t_2^3+t_3^3+6t_1t_2t_3+3t_1^2t_2+3t_1^2t_3+3t_2^2t_1+3t_2^2t_3+3t_3^2t_1+3t_3^2t_2 =$$
$$t_1^3+t_2^3+t_3^3+3(t_1^2t_2+t_1^2t_3+t_2^2t_1+t_2^2t_3+t_3^2t_1+t_3^2t_2+2s_3)$$

כלומר

$$l - s_1^3 = -3(t_1^2t_2+t_1^2t_3+t_2^2t_1+t_2^2t_3+t_3^2t_1+t_3^2t_2+2s_3)$$

האיבר המוביל הוא $-3t_1^2t_2$ והוא מתאים עבור

$$-3s_1s_2 = -3(t_1+t_2+t_3)(t_1t_2+t_1t_3+t_2t_3) = -3(t_1^2t_2+t_1^2t_3+t_1t_2t_3+t_1t_2^2+t_1t_2t_3+t_2^2t_3+t_1t_2t_3+t_1t_3^2+t_2t_3^2)$$
$$= -3(t_1^2t_2+t_1^2t_3+t_1t_2^2+t_3t_2^2+t_1t_3^2+t_2t_3^2+3s_3)$$

ואז

$$l - s_1^3 + 3s_1s_2 = 3s_3 = 3(t_1t_2t_3) \Longrightarrow l = \underbrace{s_1^3 - 3s_1s_2 + 3s_3}_{\text{זהות ידועה לסכום חזקות שלישיות}}$$

ולכן

$$\alpha_1^3+\alpha_2^3+\alpha_3^3 = g(l) = 5^3 - 3\cdot 5\cdot 1 + 3\cdot 2 = 125 - 15 + 6 = 116$$

5 דברים שחשוב לזכור למבחן

5.1 חבורות מסדרים קטנים

1. חבורות מסדר 2 הן $\mathbb{Z}_2 = S_2 = D_2$ כמובן שציקלית ואבלית
2. חבורות מסדר 3 הן רק $\mathbb{Z}_3 = A_3$ כמובן שציקלית ואבלית
3. חבורות מסדר 4
   1. $\mathbb{Z}_4$ – ציקלית ואבלית
   2. חבורות קליין $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq S_2 \times S_2$ – לא ציקלית, כן אבלית ויש לה 3 תתי־חבורות לא טריוויאליות מסדר 2
4. חבורה מסדר 5 היא רק $\mathbb{Z}_5$ כמובן שציקלית ואבלית
5. חבורות מסדר 6
   1. $\mathbb{Z}_6 \simeq \mathbb{Z}_3 \times \mathbb{Z}_2$ – ציקלית ואבלית
   2. S_3 – לא ציקלית ולא אבלית
6. חבורה מסדר 7 היא רק $\mathbb{Z}_7$ – כמובן שציקלית ואבלית
7. חבורות מסדר 8
   1. $\mathbb{Z}_8$ – כמובן שציקלית ואבלית
   2. $\mathbb{Z}_4 \times \mathbb{Z}_2$ – אבלית
   3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ – אבלית
   4. D_4
8. חבורות מסדר 9
   1. $\mathbb{Z}_9$ – כמובן שציקלית ואבלית
   2. $\mathbb{Z}_3 \times \mathbb{Z}_3$ – אבלית
9. חבורות מסדר 10
   1. $\mathbb{Z}_{10} \simeq \mathbb{Z}_5 \times \mathbb{Z}_2$ – ציקלית
   2. D_5 לא אבלית
10. חבורות מסדר 12
    1. A_4
    2. D_6
    3. $\mathbb{Z}_{12}$

5.2 תתי־חבורות של חבורות סימטריות

1. החבורה S_3
   1. תת־חבורה מסדר 2 היא S_2
   2. תת־חבורה מסדר 3 היא A_3
2. החבורה S_4
   1. תת־חבורה מסדר 3 היא A_3
   2. תתי־חבורות מסדר 4 הן
      1. $\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}_4$ היא תת־חבורה טרנזטיבית
      2. V_4 היא תת־חבורה לא טרנזטיבית אבל היא כן תת־חבורה נורמלית אבל כן אבלית!
   3. תת־חבורה מסדר 6 היא S_3 והיא לא טרנזטיבית
   4. תתי־חבורות מסדר 8
      1. D_4 והיא טרנזטיבית
      2. C_8
      3. $C_4 \times C_2$ אבלית
      4. $C_2 \times C_2 \times C_2$ אבלית
   5. תת־חבורה מסדר 8 היא D_4 והיא טרנזטיבית
   6. תת־חבורה מסדר 12 היא A_4 ונקווה שלא נצטרך את זה בחיים שלנו

5.3 קוסינוסים וסינוסים טובים

1. $\cos\left(\frac{\pi}{2}\right)=0, \sin\left(\frac{\pi}{2}\right)=1$
2. $\cos\left(\frac{3\pi}{4}\right)=\frac{-\sqrt{2}}{2}, \sin\left(\frac{3\pi}{4}\right)=\frac{\sqrt{2}}{2}$
3. $\cos\left(\frac{7\pi}{4}\right)=\frac{\sqrt{2}}{2}, \sin\left(\frac{7\pi}{4}\right)=\frac{-\sqrt{2}}{2}$
4. $\cos\left(\frac{2\pi}{3}\right)=-\frac{1}{2}, \sin\left(\frac{2\pi}{3}\right)=\frac{\sqrt{3}}{2}$
5. $\cos\left(\frac{\pi}{3}\right)=\frac{1}{2}, \sin\left(\frac{\pi}{3}\right)=\frac{\sqrt{3}}{2}$
6. $\cos\left(\frac{\pi}{4}\right)=\frac{\sqrt{2}}{2}, \sin\left(\frac{\pi}{4}\right)=\frac{\sqrt{2}}{2}$

5.4 פולינום ציקלוטומיים בסיסיים

1. $\Phi_1(x)=x-1$
2. $\Phi_2(x)=x+1$
3. $\Phi_3(x)=x^2+x+1$
4. $\Phi_4(x)=x^2+1$
5. $\Phi_5(x)=x^4+x^3+x^2+x+1$
6. $\Phi_6(x)=x^2-x+1$
7. $\Phi_7(x)=x^6+x^5+x^4+x^3+x^2+x+1$
8. $\Phi_8(x)=x^4+1$
9. $\Phi_9(x)=x^6+x^3+1$
10. $\Phi_{10}(x)=x^4-x^3+x^2-x+1$
11. $\Phi_{11}(x)=x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
12. $\Phi_{12}(x)=x^4-x^2+1$

5.5 נוסחאות לפולינומים ציקלוטומיים

1. $x^n-1=\prod_{d|n}\Phi_d(x)$ כאשר $\Phi_n(x)=\prod_{\substack{1\leq k\leq n\\ \gcd(k,n)=1}}\left(x-e^{\left(2\pi i\frac{k}{n}\right)}\right)$
2. עבור n ראשוני, $\Phi_n(x)=\sum_{k=0}^{n-1}x^k$
3. אם $n=2p$ עבור $p\neq 2$ ראשוני, $\Phi_{2p}(x)=\sum_{k=0}^{p-1}(-x)^k$

6 משפטים להוכחה במבחן

6.1 תנאים שקולים להרחבה נוצרת סופית

משפט 6.1: תהיי E/F הרחבת שדות אז הבאים שקולים

1. E/F סופית
2. E/F נוצרת סופית ואלגברית
3. $E = F(\alpha_1, \cdots, \alpha_k)$ כאשר $\alpha_1, \cdots, \alpha_k$ אלגבריים

הוכחה:

$2 \Leftarrow 1$ מהסופיות ברור שמתקיים (מהגדרה)

$$\alpha \text{ אלגברי מעל } F \iff [F(\alpha) : F] < \infty$$

ולכן זו הרחבה אלגברית (בפרט לכל $\alpha \in E$ מתקיים $[F(\alpha) : F] \leq [E : F]$) ולכן $[E : F] = n$ אז $\alpha_1, \cdots, \alpha_n$ זה בסיס של E מעל F ולכן $E = F(\alpha_1, \cdots, \alpha_n)$ ולכן E נוצרת סופית מעל F.

$3 \Leftarrow 2$ אם E/F נוצרת סופית ואלגברית אז יש יש לה קבוצת יוצרים $\alpha_1, \cdots, \alpha_k$ והיות וההרחבה אלגברית בפרט $\alpha_1, \cdots, \alpha_k$ אלגבריים.

$1 \Leftarrow 3$ נסמן $n_1, \cdots, n_k$ הדרגות של $\alpha_1, \cdots, \alpha_k$ בהתאמה, עלינו להראות $[E : F] \leq n_1 n_2 \cdots n_k$.

לכל $1 \leq i \leq k$ נסמן $E_i = F(\alpha_1, \cdots, \alpha_i)$ וכן $E_0 = F$, נשים לב כי אם מתקיים $[E_i : E_{i-1}] \leq n_i$ אז מכפליות הדרגה נקבל

$$[E : F] = [E_k : E_{k-1}] \cdot [E_{k-1} : E_{k-2}] \cdot \cdots \cdot [E_2 : E_1] \cdot [E_1 : E_0] \leq n_k \cdot n_{k-1} \cdot \cdots \cdot n_2 \cdot n_1$$

נזכר ש-$[E_i : E_{i-1}]$ זו הדרגה של הפולינום המינימלי g_i של α_i מעל E_{i-1}, אבל $m_{\alpha_i}(x)$ הוא הפולינום המינימלי של α_i מעל F הוא בפרט פולינום מעל השדה E_{i-1} (שמכיל את F) ומתקיים $g_i \mid m_{\alpha_i}$ ובפרט $[E_i : E_{i-1}] = \deg(g_i) \leq \deg\left(m_{\alpha_i}\right) = n_i$ $\square$

6.2 לכל שדה קיים סגור אלגברי

משפט 6.2: לכל שדה K קיים סגור אלגברי $\overline{K}/K$.

הוכחה: נוכיח תחילה למה:

למה 6.1: נניח כי K שדה ו־L/K הרחבה אלגברית, $\kappa = |K|$. אזי $|L| \le \max\{\kappa, \aleph_0\}$.
לכן, המקרה היחידי שיתקיים $|K| < |L|$ זה כאשר K סופית ו־L בת־מנייה.

הוכחה: נבחן את $K[t]$. קבוצת הפולינומים מדרגה לכל היותר d היא מעוצמה של κ^{d+1}.
אם K אינסופית, אז $\kappa^n = \kappa$ משיקולי עוצמות וזה נכון גם במקרה שבו אנחנו עושים איחוד בן־מנייה של κ, ולכן $|K[t]| = \kappa$.
אם K סופית אזי $|K[t]| = \aleph_0$ (ראינו גם בתורת הקבוצות).
נגדיר העתקה $L \to K[t]$ על־ידי $\alpha \mapsto f_{\alpha/K}$ (כל $\alpha \in L$ ממופה לפולינום המינימלי שלו).
נשים לב שהעתקה זאת ממפה לסיבים סופים (שכן המקור של כל פולינום $f \in K[t]$ מכיל את כל השורשים שלו ב־L), ולכן

$$|L| \le \aleph_0 \cdot \max\{\kappa, \aleph_0\} = \max\{\kappa, \aleph_0\}$$

□

כעת, ניזכר בהגדרה ממבנים 1:

הגדרה 6.1 (סיב): תהיינה A, B קבוצות ו־$f : A \to B$. **סיב (fiber)** של הפונקציה הוא תת־קבוצה של A שהיא קבוצת המקורות של איבר ב־B, כלומר תת־קבוצה מהצורה

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}$$

ניזכר שראינו במבנים 1 שלמת הגרעין (למה 3.13 בספר) אומרת במילים אחרות שהסיבים של הומומורפיזם $\varphi : G \to H$ הם בידיוק המחלקות של הגרעין N ולכן ל־G/N יש מבנה של חבורה.

נבחר $K \subset U$ כך ש־$|U| > \max\{|K|, \aleph_0\}$ (כאשר U מלשון universe).
נבחן את $\mathcal{V}$, קבוצת כל השלשות $(L, +, \cdot)$ משמע קבוצת כל תתי־הקבוצות $K \subseteq L \subset U$ ופעולות $+ : L^2 \to L, \cdot : L^2 \to R$ כך שהפעולות הופכות את L לשדה ואפילו להרחבה אלגברית L/K ובפרט $+_L |_K = +_K, \cdot_L |_K = \cdot_K$.
נסדר באמצעות יחס־סדר חלקי $(L, +, \cdot) \le (F, +, \cdot)$ אם $L \subseteq F$ והפעולות על F מסכימות עם הפעולות על L (משמע F/L הרחבת שדות ולא רק הרחבת קבוצות) ולכן $\mathcal{V}$ היא קבוצה סדורה חלקית.
נניח בנוסף כי $\{(L_i, +, \cdot)\}_{i \in I \subseteq \mathcal{V}}$ שרשרת של שדות ולכן קיים לה חסם עליון $L = \cup_{i \in I} L_i$ (ואכן, כל $a, b \in L$ מוכל ב־L_i עבור i כלשהו, ונגדיר $a +_L b = a +_{L_i} b$ ובאותו אופן נגדיר מכפלה ואז נקבל כי L הוא שדה וכל $a \in L$ מוכל ב־L_i כלשהו ולכן אלגברי מעל K).
לפי הלמה של צורן, קיים איבר מקסימלי $\left(\overline{K}, +, \cdot\right) \in \mathcal{V}$ ונטען כי $\overline{K}$ הוא סגור אלגברי ולכן אלגברי מעל K: נניח שלא כך, ולכן קיימת הרחבה אלגברית לא טריוויאלית $L/\overline{K}$. היות ו־$|L| < |U|$, מהלמה לעיל נובע שקיים שיכון (של קבוצות) $\varphi : L \hookrightarrow U$ שמרחיב את ההכלה $\overline{K} \subset U$ אבל אז $(\varphi(L), +, \cdot)$ הוא האיבר המקסימלי, ב־$\mathcal{V}$ וזו סתירה להנחה כי L חסם־עליון.

6.3 שדה המרוכבים הוא סגור אלגברית

משפט 6.3: השדה $\mathbb{C}$ הוא סגור אלגברית.

הוכחה: נזכר בשתי טענות:

1. לכל $f \in \mathbb{R}[t]$ מדרגה אי־זוגית יש שורש ב־$\mathbb{R}$ – זה נובע ממשפט ערך הביניים: f רציפה ומתקיים $\lim_{t\to\infty} f(t) = \infty, \lim_{t\to-\infty} f(t) = -\infty$ ולכן בפרט יש שורש.
2. השדה $\mathbb{C}$ סגור להוצאת שורש

כעת, נניח שלא כך ולכן יש $L/\mathbb{C}$ הרחבה אלגברית ולכן גם $L/\mathbb{R}$ אלגברית.
היות ו־$\mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$ נובע שכל פולינום אי־פריק הוא ספרבילי ולכן ההרחבה היא ספרבילית ולכן ניקח $L^{\mathrm{gal}}/\mathbb{R}$ ונגדיר $G = \mathrm{Gal}\left(L^{\mathrm{gal}}/\mathbb{R}\right)$.
ניקח $H \leq G$ תת־חבורה 2־סילו ולכן $\{e\} \leq H \leq G$ ונקבל שיש שדה ביניים $L^{\mathrm{gal}}/F/\mathbb{R}$ כאשר $F = \left(L^{\mathrm{gal}}\right)^H$.
אז $[F:\mathbb{R}] = \frac{|G|}{|H|}$ מספר אי־זוגי, זה מכיוון ש־H חבורת 2־סילו ולכן לכל $\alpha \in F$ מתקיים $\deg\left(f_{\alpha/\mathbb{R}}\right)$ אי־זוגי, שכן

$$\deg\left(f_{\alpha/\mathbb{R}}\right) = [\mathbb{R}(\alpha):\mathbb{R}] \mid [F:\mathbb{R}]$$

לכל פולינום כזה יש שורש ב־$\mathbb{R}$ מהטענה הראשונה מתהזכורת ולכן יש ל־f_α שורש ב־$\mathbb{R}$ ולכן $\alpha \in \mathbb{R}$ (אחרת, f_α פריק בסתירה להנחה).
אז $F = \mathbb{R}, H = G$ ולכן $L^{\mathrm{gal}}/\mathbb{R}$ היא הרחבה מסדר זוגי $|G| = 2^n$ ולכן יש סדרה

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G \qquad \left(|G_i| = 2^i\right)$$

מהצד השני, מהתאמת גלואה קיבלנו

$$K_n \supset \cdots \supset K_2 \supset K_1 \supset \mathbb{R} \qquad ([K_i : K_{i-1}] = 2)$$

נניח ש־$n \leq 2$ (בהכרח מתקיים $n \geq 1$ כי $\mathbb{C} \subset L^{\mathrm{gal}}$), אבל זו סתירה כי אז נקבל

$$\mathbb{R} \neq K_1 = \mathbb{R}\left(\sqrt{a}\right)$$

אבל $a \in \mathbb{R}$ ולכן בהכרח $a < 0$ ואז $K_1 = \mathbb{C}$, אבל $C \neq K_2 = \mathbb{C}\left(\sqrt{a+bi}\right)$ אבל זו סתירה לטענה השנייה מהתזכורת, ולכן בהכרח $n = 1 \Rightarrow$ $L = \mathbb{C}$ בסתירה לכך ש־L לא טריוויאלית, כנדרש. □

6.4 על פרובניוס ושדות סופיים מחזקות p

משפט 6.4: לכל ראשוני p ולכל $n \in \mathbb{N}$ קיים שדה $\mathbb{F}_{p^n}$ עם p^n איברים ו־$\mathrm{Aut}_{\mathbb{F}_p}\left(\mathbb{F}_{p^n}\right)$ היא חבורה ציקלית מסדר n והיוצר שלה הוא העתקת הפרובניוס.

הוכחה: נסמן $q = p^n$ ונתחיל מלהוכיח את קיום השדה $\mathbb{F}_q$: נתבונן ב-$\mathbb{F}_p$ ונגדיר הרחבה K כשדה פיצול של הפולינום $f(t) = t^q - t$ ונראה שיש ב־K בידיוק q איברים: נסמן ב־A את קבוצת השורשים של f ב־K ומתקיים $f' = -1$ ולכן $\gcd(f, f') = 1$ והפולינום f ספרבילי. על־כן, $|A| = q$ ו־A שדה כי אם נסמן $\mathrm{Fr}^q\, x = x, \mathrm{Fr}^q\, y = y$ אז

$$\mathrm{Fr}_q(x+y) = \mathrm{Fr}_q(x) + \mathrm{Fr}_q = x + y \pmod q$$

$$\mathrm{Fr}_{q(xy)} = \mathrm{Fr}_q\, x\, \mathrm{Fr}_q\, y = xy \pmod q$$

וזה מראה ש־A שדה, ולכן $K = A =: \mathbb{F}_q$ הוא שדה וכמובן יחיד עד־כדי איזומורפיזם כשדה פיצול של הפולינום.

נסתכל על ההרחבות שדות $\mathbb{F}_{p^n}/\mathbb{F}_p$, הרחבת שדות סופית מדרגה n.

נראה בתור התחלה $n \leq \left|\mathrm{Aut}_{\mathbb{F}_p}\left(\mathbb{F}_q\right)\right|$, נטען שזו הרחבה פרימיטיבית: $\mathbb{F}_q^\times$ היא ציקלית ויוצר כלשהו שלה יוצר גם את ההרחבה (מהציקליות), כלומר, $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.

אז $\deg_{\mathbb{F}_p}(\alpha) = n$ ולכן יש לו לכל היותר n צמודים מעל $\mathbb{F}_p$.

כל $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}\left(\mathbb{F}_p\right)$ חייב לקחת את α לאחד הצמודים שלנו, $\sigma(\alpha) = \alpha_i$ והוא נקבע ביחידות על־ידי $\sigma(\alpha)$ כי α יוצר, ולכן קיימים לכל היותר n $\mathbb{F}_p$ אוטומורפיזמים שונים.

מצד שני, נשים לב ש־$\mathrm{Fr}_p|_{\mathbb{F}_p} = \mathrm{Id}$ ולכן $\mathrm{Fr}_p \in \mathrm{Aut}_{\mathbb{F}_p}\left(\mathbb{F}_q\right)$.

לכל $0 \leq i < n$ מתקיים $\left(\mathrm{Fr}_p\right)^i = \mathrm{Fr}_{p^i}$ ול־Fr_{p^i} יש בידיוק p^i נקודות שבת, ו־$i < n$ אז יש $\beta \in \mathbb{F}_q$ כך ש־$\mathrm{Fr}_{p^i}(\beta) \neq \beta$ ולכן $\mathrm{Fr}_{p^i} \neq \mathrm{Id}_{\mathbb{F}_{p^s}}$ ולכן הסדר של Fr_p הוא לכל הפחות n.

לכן יש בידיוק n אוטומורפיזמים, וראינו ש־Fr_p יוצר את חבורת ה־$\mathbb{F}_p$ אוטומורפיזמים, כנדרש. $\square$

6.5 כל הרחבה ספרבילית סופית היא פרימיטיבית

משפט 6.5: נניח כי L/K הרחבה סופית ונניח בנוסף שההרחבה פרידה (ספרבילית). אז היא פרימיטיבית (קיים $\alpha\in L$ כך ש־$L=K(\alpha)$ ו־α נקרא **איבר פרימיטיבי**).

הוכחה: תחילה נוכיח למה:

למה 6.2 (משפט האיבר הפרימיטיבי חלק 1): תהיי L/K הרחבה סופית. אז L/K היא הרחבה פרימיטיבית אם ורק אם יש כמות סופית של שדות ביניים.

הוכחה: $\Longleftarrow$ תהיי L/K פרימיטיבית, כלומר $K=L(\alpha)$ ויהי F שדה ביניים. אז $f_{\alpha/F}=\sum_{i=1}^{n}a_it^i$.
יהי $L\subset F\subset E=K(a_0,\cdots,a_n)$ אז $f_{\alpha/F}\in E[t]$ ולכן $f_{\alpha/F}\mid f_{\alpha/E}$ ובפרט הם שווים.
לכן $[L:F]=\deg\left(f_{\alpha/F}\right)=\deg\left(f_{\alpha/E}\right)=[L:E]$ ולכן $E=F$ (כי $[F:E]=\frac{[L:E]}{[L:F]}=1$).
אז $F=K(a_1,\cdots,a_n)$ נקבע ביחידות על־ידי $f_{\alpha/F}$ ואנחנו יודעים ש־$f_{\alpha/K}\mid f_{\alpha/F}$ ולכן יש רק כמות סופית של אפשרויות ל־$f_{\alpha/F}$ (מקסימום $2^{\deg\left(f_{\alpha/K}\right)}=2^{[L:K]}$ כי $f_{\alpha/K}=\prod_{i=1}^{n}(t-\alpha_i)\in\overline{K}[t]$ ואם אני רוצה פולינום שיחלק, צריך לבחור קבוצה כלשהי של שורשים ויש 2^n אפשרויות לכל היותר).
$\Longrightarrow$ נניח שיש כמות סופית של שדות ביניים, $K\subset F_i\subset L$ עבור $1\le i\le m$.
אם K סופי, אז אנחנו יודעים ש־L/K פרימיטיבית, אז נניח ש־K אינסופי ונוכיח באינדוקציה על $[L:K]$:
הבסיס של דרגה 1 הוא טריוויאלי ולכן ניח שהטענה מתקיימת לכל הרחבה מדרגה הקטנה ל־$[L:K]$.
נכתוב $L=K(\alpha_1,\cdots,\alpha_r)$ הרחבה סופית וכן $E=K(\alpha_1,\cdots,\alpha_{r-1})$ (ואז $L=E(\alpha_r),\alpha=\alpha_r$).
נניח בלי הגבלת הכלליות ש־$E\neq L$ (אחרת נזרוק את α_r כי הוא מיותר).
מהנחת האינדוקציה, $E=K(\beta)$ כי ל־K יש רק מספר סופי של תתי־שדות.
ניקח סדרה אינסופית (מההנחה ש־K אינסופי) $c_1,c_2,\cdots\in K$ וניקח $\gamma_i=\alpha+\beta c_i$ (צירופים לינאריים שונים של α,β).
נגדיר $F_j=K\left(\gamma_j\right)$ וקיימים $j\neq\ell$ כך ש־$F_j=F_\ell$ (כי יש כמות סופית של שדות ביניים וכמות אינסופית של איברים).
מתקיים $F_j=F_\ell\ni\frac{\gamma_\ell-\gamma_j}{c_\ell-c_j}=\frac{(\alpha+\beta c_\ell)-(\alpha+\beta c_j)}{c_\ell-c_j}=\beta$ ולכן $\alpha=\gamma_\ell-c_\ell\beta\in F_\ell$ ואז $\alpha,\beta\in F_j$, כלומר

$$L=K(\alpha,\beta)\subset F_j=K\left(\alpha+c_j\beta\right)=K\left(\gamma_j\right)$$

וזה בידיוק אומר ש־L/K פרימיטיבית. $\square$

אם כך, מספיק להוכיח שיש כמות סופית של שדות ביניים: נסתכל על סגור גלואה $L^{\text{gal}}/K=L^{nor}$ (הסגור הנורמלי הוא סגור גלואה כי L/K פרידה) ומספיק להוכיח של־L^{gal}/K יש כמות סופית של שדות ביניים (כי $L\subset L^{\text{gal}}$).
מהתאמת גלואה לכל $K\subset F\subset L^{\text{gal}}$ מתקיים $F=L^{\text{Gal}(L/F)}$ ולכן F נקבע ביחידות על־ידי $\text{Gal}(L/F)\le\text{Gal}(L/K)$ ויש כמות סופית כזאת כי $\text{Gal}(L/K)$ היא חבורה סופית. $\square$

6.6 משפט ארטין

משפט 6.6: L שדה ו־$H \le \mathrm{Aut}(L)$ חבורת אוטומורפיזמים סופית כלשהי, נסמן $F = L^H$. אז L/F הרחבת גלואה ו־$H = \mathrm{Gal}(L/F)$.

הוכחה: יהי $\alpha \in L$ ונגדיר $\mathcal{C}_\alpha = H\alpha = \{\sigma(\alpha)\}_{\sigma \in H}$ ונגדיר $f_\alpha = \prod_{\alpha \in \mathcal{C}_\alpha}(t-\alpha)$.
כל $\sigma \in H$ מחליף גורמים ב־f_α ולכן $\sigma(f_\alpha) = f_\alpha$ כלומר $f_\alpha \in F[t]$ אז $f_{\alpha/F} \mid f_\alpha$ ולכן $f_{\alpha/F}$ הוא פריד מדרגה חסומה על־ידי $|H| \ge |\mathcal{C}_\alpha|$.
נשאר להראות $[L:F] \le |H|$: נניח שלא, אז $[L:F] > |H|$.
L/F אלגברית (כי H סופית ומתנאים שקולים) ופרידה, ולכן יש תת־הרחבה סופית $F \subset E \subset L$ כך שמתקיים $|H| < [E:F] < \infty$ ולכן לפי משפט האיבר הפרימיטיבי $E = F(\alpha)$.
אבל $|H| \le \deg\left(f_{\alpha/F}\right)$ בסתירה להנחה.
אז $[L:F] \le |H|$ וגם $H \le \mathrm{Aut}(L/F)$ אבל תמיד מתקיים $[L:F] \le |\mathrm{Aut}(L/F)|$ ולכן יש שיוויון, אבל שיוויון מתקיים אם ורק אם L/F היא הרחבת גלואה והכל שיוויונות ולכן $H = \mathrm{Gal}(L/F)$, $[L:F] = |H|$. □

6.7 התאמת גלואה

תהיי L/K הרחבת גלואה סופית ונסמן $G = \mathrm{Gal}(L/K)$.
אזי ההעתקות $\mathscr{G}(F) = \mathrm{Gal}(L/F), \mathscr{F}(H) = L^H$ הפוכות אחת לשנייה ומשרות התאמה חד־חד ערכית ועל בין שדות ביניים $L/F/K$ לתתי־חבורות $1 \le H \le G$.

הוכחה: נוכיח כי לכל שדה ביניים $L/F/K$ מתקיים $F = L^{\mathrm{Gal}(L/F)}$.
ברור כי $F \subseteq L^{\mathrm{Gal}(L/F)}$ כי $\mathrm{Gal}(L/F)$ אלו האוטומורפיזמים שמקבעים את F.
ניקח $\alpha \in L/F$ ולכן α פריד מעל F כי L/K פרידה (כי גלואה) ולכן L/F פרידה ו־$\deg_s(\alpha) > 1$ ולכן יש לו צמוד α' מעל F ולכן קיים $\sigma \in \mathrm{Aut}_F(\overline{F})$ כך שיתקיים $\sigma(\alpha) = \alpha'$.
מתקיים $\sigma|_K = \mathrm{Id}_K$ וגם $\sigma(L) = L$ מהיות L/K נורמלית ולכן $\sigma|_L \in \mathrm{Gal}(L/F)$ כי הוא הזהות על F, אבל $\sigma(\alpha) \neq \alpha$ ולכן $\alpha \in L^{\mathrm{Gal}(L/F)}$
ולכן קיבלנו שוויון ומתקיים $F = L^{\mathrm{Gal}(L/F)}$.
אז מתקיים

$$\mathscr{F}(\mathscr{G}(F)) = \mathscr{F}(\mathrm{Gal}(L/F)) = L^{\mathrm{Gal}(L/F)} = F \Rightarrow \mathscr{F} \circ \mathscr{G} = \mathrm{Id}$$

בכיוון השני, נזכר במשפט ארטין:

משפט 6.7 (משפט ארטין): L שדה ו־$H \le \mathrm{Aut}(L)$ חבורת אוטומורפיזמים סופית כלשהי ונסמן $F = L^H$. אז L/F הרחבת גלואה ו־$H = \mathrm{Gal}(L/F)$.

אז ניקח $H \le G$ תת־חבורה ולכן ממשפט ארטין (יחד עם הסופיות!) נקבל

$$H = \mathrm{Gal}(L/L^H) = \mathscr{G}(\mathscr{F}(H)) \Rightarrow \mathscr{G} \circ \mathscr{F} = \mathrm{Id}$$

אז הוכחנו את ההתאמה ונשאר להראות ש־$\mathscr{G}, \mathscr{F}$ הופכות שיכונים:
נניח כי $H' \le H \le G$ תתי־חבורות של G אז $\mathscr{F}(H) = L^H$ אלו כל האיברים ב־L שנשארים במקום על־ידי פעולת H, אבל $H' \subseteq H$ ולכן נובע כי אם איבר נשאר במקום על־ידי H הוא ישאר במקום גם על־ידי H' ולכן $\mathscr{F}(H) \subseteq L^{H'} = \mathscr{F}(H')$.
ניקח שדות ביניים $L/F/F'/K$ אז $\mathscr{G}(F) = \mathrm{Gal}(L/F)$ אלו אוטומורפיזמים המשמרים את F אבל $F' \subseteq F$ ולכן הם גם משמרים הכרח את F', כלומר $\mathscr{F} = \mathrm{Gal}(L/K) \subseteq \mathrm{Gal}(L/F') = \mathscr{G}(F')$, כנדרש. $\square$

הערה: תהיי L/K הרחבת שדות ותהיי $G = \mathrm{Aut}(L/K)$.
לכל שדה ביניים $K \subseteq M \subseteq L$ התאמת גלואה מתאימה את החבורה $\mathscr{G}(M) = \mathrm{Aut}(L/M)$ ולכל תת־חבורה $H \le G = \mathrm{Aut}(L/K)$ מתאימה את **שדה השבת** של H המסומן $\mathscr{F}(H)$ ומוגדר על־ידי

$$\mathscr{H} = \{x \in L \mid \forall \sigma \in H,\ \sigma(x) = x\}$$

כלומר, קבוצת האיברים ב־L שמקובעים על־ידי כל האוטומורפיזמים ב־H (הוא כמובן שדה ומתקיים $K \subseteq \mathscr{F}(H) \subseteq L$)

6.8 הלמה השנייה של גאוס

משפט 6.8: כל פולינום פרימיטיבי $f(x) \in \mathbb{Z}[x]$ שהוא אי־פריק ב־$\mathbb{Z}[x]$ הוא גם אי־פריק ב־$\mathbb{Q}[x]$.

הוכחה: נזכר בשתי הגדרות

הגדרה 6.2 (תכולה): עבור פולינום $f(t) \in \mathbb{Z}[t]$ (תזכורת: $f(t) = \sum_{i=0}^{n} a_i t^i$) נגדיר **תכולה** של f להיות

$$\mathrm{cont}(f) = \gcd(a_0, a_1, ..., a_n)$$

הגדרה 6.3 (פולינום פרימיטיבי): פולינום $f(t) \in \mathbb{Z}[t]$ יקרא **פרימיטיבי** אם $\mathrm{cont}(f) = 1$.

הערה: לכל פולינום f יש פירוק ב־$\mathbb{Z}[t]$ הנתון על־ידי $f = \mathrm{cont}(f) \cdot f_0(t)$ כאשר $f_0(t)$ הוא פולינום פרימיטיבי.

וניזכר בלמת גאוס הראשונה:

משפט 6.9 (למת גאוס הראשונה): אם $f, g \in \mathbb{Z}[t]$ אזי $\mathrm{cont}(fg) = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$. בפרט, fg פרימיטיבי אם ורק אם f ו־g פרימיטיביים.

הוכחה: מההערה לעיל מתקיים $f \cdot g = \mathrm{cont}(f) \cdot \mathrm{cont}(g) \underbrace{f_0 \cdot g_0}_{\text{פרימיטיביים}}$ ולכן מספיק להוכיח כי $f_0 \cdot g_0$ הוא פרימיטיבי:

נניח שלא ולכן קיים $p \in \mathbb{N}$ ראשוני כך שמתקיים $p \mid \mathrm{cont}(f_0 \cdot g_0)$, אבל $f_0 = \sum_{i=0}^{n} a_i t^i, g_0 = \sum_{j=0}^{m} b_j t^j$ הם פולינומים פרימיטיביים (ולכן לא כל a_i, b_j מתחלקים ב־p) ולכן נוכל לבחור m, n מינימליים כך ש־$p \nmid a_n$ ו־$p \nmid b_m$.
נסתכל על המקדם של $c = \sum_{k=0}^{m+n} a_k b_{m+n-k}$ של t^{m+n} ב־$f_0 \cdot g_0$, נכתוב אותו מפרושות:

$$\underbrace{a_0 b_{m+n} + ... + a_{n-1} b_{m+1}}_{\text{מתחלקים ב־p כי } p|a_k \text{ לכל k<n}} + a_n b_m + \underbrace{a_{n+1} b_{m-1} + ... + a_{m+n} + b_0}_{\text{מתחלקים ב־p כי } p|b_k \text{ לכל k>n}}$$

אבל $a_n b_m$ זר לחלוקה ב־p ולכן $p \nmid c$ וזאת סתירה. $\square$

נוכיח למה שהייתה חלק מלמת גאוס השנייה:

למה 6.3: יהי $f \in \mathbb{Z}[t]$ פולינום לא קבוע. נזכור כי $\mathbb{Q}[t]$ הוא $\mathrm{Frac}(\mathbb{Z})$, שדה השברים של $\mathbb{Z}[t]$.
אם $f = g \cdot h$ פירוק ב־$\mathbb{Q}[t]$ אזי קיים $0 \neq c \in \mathbb{Q}^\times$ כך ש־$c \cdot g, c^{-1} \cdot h \in \mathbb{Z}[t]$ ולכן $f = (c \cdot g) \cdot (c^{-1} \cdot h)$ פירוק ב־$\mathbb{Z}[t]$.

הוכחה: ניקח את הפירוק $f = g \cdot h$ עבור $g, h \in \mathbb{Q}[t]$ וניקח $0 < m, n \in \mathbb{Z}$ כך ש־$m \cdot g, n \cdot h \in \mathbb{Z}[t]$ ואז נקבל פירוק

$$m \cdot n \cdot f = m \cdot g \cdot n \cdot h$$

נסמן $\ell = \mathrm{cont}(f), \alpha = \mathrm{cont}(m \cdot g), \beta = \mathrm{cont}(n \cdot h)$. מלמת גאוס הראשונה נקבל עם כפליות התכולה

$$\mathrm{cont}(m \cdot n \cdot f) = m \cdot n \cdot \ell = \alpha \cdot \beta = \mathrm{cont}(m \cdot g \cdot n \cdot h)$$

אם כך, ניקח $m \cdot n \cdot f = m \cdot g \cdot n \cdot h$ ונחלק ב־$m \cdot n \cdot \ell = \alpha\beta$ ונקבל $\underbrace{\frac{m}{\alpha} \cdot g \cdot \frac{n}{\beta} \cdot h}_{\in \mathbb{Z}[t]} = \frac{m \cdot n \cdot f}{m \cdot n \cdot \ell} = \frac{1}{\ell} \cdot f$ משמע $f = \ell \frac{m}{\alpha} \cdot g \cdot \frac{n}{\beta} \cdot h$. $\square$

נשאר רק להוכיח את הטענה שלנו: נניח כי f אי־פריק ב־$\mathbb{Z}[t]$ ולכן $f = \mathrm{cont}(f) \cdot \frac{f}{\mathrm{cont}(f)}$ פירוק טריוויאלי ונשים לב $\deg\left(\frac{f}{\mathrm{cont}(f)}\right) > 0$ ולכן $\mathrm{cont}(f)$ הפיך ולכן f פרימיטיבי.
נניח ש־f פריק ב־$\mathbb{Q}[t]$ ולכן יש $f = g \cdot h$ כך ש־$\deg(g), \deg(h) > 0$ ולכן מהלמה לעיל נקבל $f = c \cdot g \cdot c^{-1} \cdot h$ עם דרגות גדולות מ־0 ב־$\mathbb{Z}[t]$ משמע הוא פריק בו, וזאת סתירה.

$\square$

6.9 טענה 8.4.2 ברשומות של מיכאל

משפט 6.10: יהי $\mu_n \subset K$,$n \in K^\times$ ו־L/K הרחבה ציקלית, אז קיים $\alpha \in L$ כך שמתקיים $L = K(\alpha)$ ו־$\alpha^n \in K$.

הוכחה: ניזכר בהגדרה

הגדרה 6.4 (חבורת μ_n, חבורת שורשי היחידה מסדר n): עבור K שדה ו־$1 \le n \in \mathbb{N}$ נגדיר

$$\mu_n(K) = \{\xi \in K \mid \xi^n = 1\}$$

$$\mu_\infty(K) = \bigcup_n \mu_n(K)$$

נשים לב ש־$\mu_n(K)$ היא תת־חבורה של $K^\times$ מסדר המחלק את n (וזהי כמובן חבורה אבלית עם כפל).
עבור K שדה ו־$1 \le n \in \mathbb{N}$, אם $x^n - 1$ מתפצל לחלוטין ב־K נסמן $\mu_n = \mu_n(K)$ (שכן היא לא תשתנה תחת הרחבה של K) ונגיד במקרה זה ש־μ_n מתפצל ב־K.

נעבור להוכחה:
מכך שההרחבה ציקלית אנחנו יודעים שההרחבה וסופית ושמתקיים $G = \mathrm{Gal}(L/K) \simeq (\mathbb{Z}/n\mathbb{Z})$ ולכן יש σ שיוצרת את ההרחבה.
נזכר שמהגדרה

$$G = \mathrm{Gal}(L/K) = \mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \forall x \in K\ \sigma(x) = x\}$$

נסתכל על ה־$\sigma : L \to L$ הזאת כאופרטור K־לינארי (כלומר, מכבד את המבנה של K, משמע לכל $a, b \in K$ ולכל $x, y \in L$ מתקיים $(\sigma(ax + by) = a\sigma(x) + b\sigma(y)$).
ניקח את $f_\sigma(t)$ הפולינום המינימלי של σ. היות וההרחבה סופית מדרגה n אז אנחנו יודעים מטעמי סדר שיתקיים $\sigma^n = 1$ ומכך ש־$\mu_n \subset K$, אנחנו מקבלים שהפולינום $t^n - 1$ מתפצל לחלוטין ב־K.
מכך ש־σ הוא אופרטור K־לינארי, מתקיים $\sigma^n - 1 = 0$ ולכן לפולינום $t^n - 1$ יש שורש שהוא σ.
מהגדרת הפולינום המינימלי הוא מחלק גם את $t^n - 1$ (כי σ שורש שלו).
מכך ש־$t^n - 1$ מתפצל לחלוטין ב־K אז הוא מהצורה

$$t^n - 1 = (t - \xi_0)(t - \xi_1) \cdot \dots \cdot (t - \xi_{n-1})$$

ובהכרח השורשים שלו (שורשי היחידה) הם שונים זה מזה, כי $(t^n - 1)' = nt^{n-1}$, אבל השורש היחידי של nt^{n-1} הוא רק עבור $t = 0\ (n \ne 0)$, אז לפי טענה שראינו נובע שאין לו שורשים מרובים ולכן כל השורשים שלו שונים זה מזה, אז כל השורשים שונים זה מזה והפיצול שראינו לעיל הוא פיצול לינארי.
ניזכר שבלינארית ראינו שאופרטור הוא אלכסוני מעל שדה אם קיים בסיס של המרחב הוקטורי שמכיל את כל הוקטורים העצמיים של האופרטור, ובמקרה שלנו זה שקול ללהגיד שהפולינום המינימלי של האופרטור מתפצל לחלוטין מעל השדה – כפי שמצאנו.
לכן יש לנו בסיס של וקטורים עצמיים $\alpha_1, \cdots, \alpha_n$ עבור הערכים העצמיים $\xi_1, \cdots, \xi_n \in \mu_n$ בהתאמה כך שמתקיים $\sigma(\alpha_i) = \xi_i \alpha_i$.
נראה כי ה־ξ_i יוצרים את μ_n: μ_n ציקלית, ולכן גם כל תת־חבורה שלה ציקלית אז $\langle \xi_i, \cdots, \xi_n \rangle = \mu_m$ עבור $m \le n$ ואז $\xi_i^m = 1$ אבל נשים לב שמתקיים אם כך לכל i

$$\sigma^m(\alpha_i) = \xi_i^m \alpha_i = 1 \cdot \alpha_i = \alpha_i$$

ולכן בהכרח $m = n$ ובעצם $\langle \xi_1, \cdots \xi_n \rangle = \mu_n$.
מכך ש־$\xi_1, \cdots, \xi_n$ יוצרים את μ_n והיא חבורה ציקלית לכן נוצרת על־ידי איבר אחד, ξ, נובע שהוא צריך להיות צירוף לינארי שלהם, אז לכל i נתאים את ℓ_i כך שיתקיים $\xi = \prod_{i=1}^n \xi_i^{\ell_i}$, נגדיר $\alpha = \prod_{i=1}^n \alpha_i^{\ell_i}$ ונקבל

$$\sigma(\alpha) = \sigma\left(\prod_{i=1}^n \alpha_i^{\ell_i}\right) = \prod_{i=1}^n \sigma\left(\alpha_i^{\ell_i}\right) \underset{\sigma(\alpha_i) = \xi_i \alpha_i}{=} \prod_{i=1}^n \xi_i^{\lambda_i} \alpha_i^{\ell_i} = \prod_{i=1}^n \xi_i^{\ell_i} \prod_{i=1}^n \alpha_i^{\ell_i} = \xi\alpha$$

במילים אחרות, α הוא וקטור עצמי של הערך עצמי ξ, אבל ξ הוא שורש פרימיטיבי מסדר n, אז הקבוצה $\{\alpha, \xi\alpha, \xi^2\alpha, \cdots, \xi^{n-1}\alpha\}$ היא בעלת n איברים שונים – זאת אומרת ל־α יש n צמודים מעל K ונטען שזה מסיים: נסמן $L = K(\alpha)$, ואם נבחר $a = \alpha^n$ אז עבור כל $\sigma_i \in G$ נקבל

$$\sigma_i(a) = \sigma_i(\alpha^n) = (\sigma_i(\alpha))^n = (\xi_i\alpha)^n = \alpha^n = a$$

וזה בידיוק אומר ש־$a \in L^G = \{x \in L \mid \forall \sigma \in G,\ \sigma(x) = x\}$, אבל זה בידיוק אומר ש־$a \in K$, כי כל איבר ב־$K$ נשמר תחת כל האוטומורפיזמים של G כי G מהגדרתה מכילה את כל האוטומורפיזמים שמשאירים את K במקום. □

6.10 טענה על הרחבות ציקלוטומיות תחת תנאי יפה

משפט 6.11: אם $n \in K^\times$ אז קיים שורש פרימיטיבי $\xi_n \in \overline{K}$ מסדר n, ההרחבה $K(\xi_n)/K$ היא גלואה וישנו שיכון

$$\mathrm{Gal}(K(\xi_n)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

הוכחה: נניח ש-$n \in K^\times$, הפולינום $x^n - 1$ הוא ספרבילי ולכן ל-$\overline{K}$ יש n שורשי יחידה שונים.
ראינו שאם ל-$\overline{K}$ יש n שורשי יחידה שונים זה מזה, אז $\mu_n \cong (\mathbb{Z}/n\mathbb{Z})$, זו חבורה ציקלית ולכן יש לנו שורש יחידה פרימיטיבי ξ_n שיוצר אותה.
$K(\xi_n)/K$ הוא שדה הפיצול של הפולינום שלנו ולכן ההרחבה נורמלית וספרבילית ולכן זו הרחבת גלואה.
כל $\sigma \in G(L/K)$ נקבע ביחידות על־ידי $\sigma(\xi)$ ולכן אנחנו מקבלים שיכון $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}(\mu_n)$ על־ידי $\sigma \mapsto \sigma|_{\mu_n}$.
נגדיר $\lambda : (\mathbb{Z}/n\mathbb{Z}) \to \mathrm{Aut}(\mu_n)$ על־ידי $a \mapsto \sigma_a$ כאשר $\sigma_a(\xi) = \xi^a$ לכל $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ והעתקה הזאת מגדירה את השיכון

$$\mathrm{Gal}(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

$\square$