מבנים אלגבריים 2, 80446 — בכי לקראת מבחן

23 ביולי 2025

תוכן עניינים

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 m_α של 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)

[נגיד כי 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 $\xi^m \ne 1$.

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 $\xi^m \ne 1$ 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 בדיוק 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

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 $p \ne 0$ 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)

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

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

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 $r \mid a_0$, $s \mid a_n$
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 דוגמאות

3.1 דברים עם כמויות

דוגמה 3.1 (כמה אוטומורפיזמים יש): אם $p > 0$ ראשוני, אז עבור $n \in \mathbb{N}$ מתקיים $\mathrm{Aut}\left(\mathbb{F}_{p^n}\right) \cong \mathbb{Z}/n\mathbb{Z}$

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

דוגמה 3.2: 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 $\mathbb{F}_{49}$.

3.3 הרחבות לא נורמליות ונורמליות

דוגמה 3.3: 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.

3.4 מלא חבורות גלואה

דוגמה 3.4: 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 טרנזטיבית 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 3.5:

4 משפטים להוכחה במבחן

4.1 תנאים שקולים להרחבה נוצרת סופית

משפט 4.1: 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 $[E_i : E_{i-1}] = \deg(g_i) \leq \deg\left(m_{\alpha_i}\right) = n_i$ $\square$

4.2 לכל שדה קיים סגור אלגברי

משפט 4.2: לכל שדה K קיים סגור אלגברי $\overline{K}/K$.

הוכחה: נוכיח תחילה למה:

למה 4.1: נניח כי K שדה ו־L/K הרחבה אלגברית, $\kappa = |K|$. אזי $|L| \leq \max\{\kappa, \aleph_0\}$.
לכן, המקרה היחידי שיתקיים $|L| > |K|$ 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

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

$\square$

כעת, ניזכר בהגדרה ממבנים 1:

הגדרה 4.1 (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 בדיוק 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 $+_K |_K +_L, \cdot_K = |_K \cdot_L$.
נסדר באמצעות יחס־סדר חלקי $(L, +, \cdot) \leq (F, +, \cdot)$ 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 אלגברית 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.

4.3 שדה המרוכבים הוא סגור אלגברית

משפט 4.3: 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־$\operatorname{char}(\mathbb{R})=\operatorname{char}(\mathbb{C})=0$ נובע שכל פולינום אי־פריק הוא ספרבילי ולכן ההרחבה היא ספרבילית ולכן ניקח $L^{\mathrm{gal}}/\mathbb{R}$ ונגדיר $G=\operatorname{Gal}\left(L^{\mathrm{gal}}/\mathbb{R}\right)$.
ניקח $H\le G$ תת־חבורה 2־סילו ולכן $\{e\}\le H\le G$ 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

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

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

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

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

4.4 על פרובניוס ושדות סופיים מחזקות p

משפט 4.4: 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 בדיוק 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 $n \le \left|\mathrm{Aut}_{\mathbb{F}_p}\left(\mathbb{F}_q\right)\right|$, 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 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 $0 \le i < n$ מתקיים $\left(\mathrm{Fr}_p\right)^i = \mathrm{Fr}_{p^i}$ ול־Fr_{p^i} יש בדיוק 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 בדיוק n אוטומורפיזמים, וראינו ש־Fr_p יוצר את חבורת ה־$\mathbb{F}_p$ אוטומורפיזמים, כנדרש. $\square$

4.5 כל הרחבה ספרבילית סופית היא פרימיטיבית

משפט 4.5: 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 4.2 (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 $f_{\alpha/F} = \sum_{i=1}^{n} a_i t^i$.
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 $\frac{\gamma_\ell - \gamma_j}{c_\ell - c_j} \in F_j = F_\ell$ $= \frac{(\alpha+\beta c_\ell)-(\alpha+\beta c_j)}{c_\ell - c_j}$ $\beta =$ ולכן $\beta \in F_\ell$ ואז $\alpha = \gamma_\ell - c_\ell \beta \in F_\ell$, כלומר $\alpha, \beta \in F_j$

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

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

אם כך, מספיק להוכיח שיש כמות סופית של שדות ביניים: נסתכל על סגור גלואה $L^{nor} = L^{\text{gal}}/K$ (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. $\square$

4.6 משפט ארטין

משפט 4.6: L שדה ו־$H \leq \mathrm{Aut}(L)$ 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 $|\mathcal{C}_\alpha| \leq |H|$.
נשאר להראות $[L : F] \leq |H|$: נניח שלא, אז $|H| < [L : F]$.
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 $|H| \leq \deg\left(f_{\alpha/F}\right)$ בסתירה להנחה.
אז $[L : F] \leq |H|$ וגם $H \leq \mathrm{Aut}(L/F)$ אבל תמיד מתקיים $[L : F] \leq |\mathrm{Aut}(L/F)|$ ולכן יש שיוויון, אבל שיוויון מתקיים אם ורק אם L/F היא הרחבת גלואה והכל שיוויונות ולכן $H = \mathrm{Gal}(L/F), [L : F] = |H|$. $\square$

4.7 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 $\sigma\in\mathrm{Aut}_F\left(\overline{F}\right)$ 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 שיוויון 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 4.7 (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

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

אז הוכחנו את ההתאמה ונשאר להראות ש־$\mathscr{F},\mathscr{G}$ 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. $\square$

4.8 הלמה השנייה של גאוס

משפט 4.8: 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 4.2 (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 4.3 (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 4.9 (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 t^{m+n} ב־$f_0 \cdot g_0$, $c = \sum_{k=0}^{m+n} a_k b_{m+n-k}$ 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 4.3: 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.

$\square$

4.9 טענה 8.4.2 ברשומות של מיכאל

משפט 4.10: 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 4.4 (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 $\mu_n(K) = \mu_n$ (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 $t = 0 \ (n \neq 0)$, 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 $\alpha_1, \dots, \alpha_n$ עבור הערכים העצמיים $\xi_1, \dots, \xi_n \in \mu_n$ 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 $\langle \xi_i, \dots, \xi_n \rangle = \mu_m$ 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־$\xi_1, \dots, \xi_n$ 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 $\{\alpha, \xi\alpha, \xi^2\alpha, \dots, \xi^{n-1}\alpha\}$ 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. $\square$

4.10 טענה על הרחבות ציקלוטומיות תחת תנאי יפה

משפט 4.11: 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

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

$\square$