מבנים אלגבריים 2, 80446 — סיכום

12 במאי 2025

תוכן עניינים

1 הרצאה 1 – 24/03

1.1 מבוא להרחבת שדות

מוסכמה: אנחנו עובדים רק בחוג קומוטטיבי עם יחידה (0 הוא חוג עם יחידה) והומומורפיזם של חוגים לוקח 1 ל־1 (מכבד את מבנה החוג). כמו כן, אנחנו עובדים תמיד בתחום שלמות (תחום ללא מחלקי 0).

דוגמה 1.1 (הומומורפיזם של חוגים): $\varphi : \mathbb{Z} \to 0$ הוא הומומורפיזם של חוגים.

אלדוגמה 1.1 (לא הומומורפיזם של חוגים): $\varphi : 0 \to \mathbb{Z}$ הוא לא הומומורפיזם של חוגים.

דוגמה 1.2 (שדות): $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}, \mathbb{R}, \mathbb{C}$ עבור $p \in \mathbb{N}$ ראשוני בלבד.

אלדוגמה 1.2 (לא שדות): $0, \mathbb{F}[X], M_{n\times n}(\mathbb{F})$

הגדרה 1.1 (פולינום מתוקן): יהי f פולינום, ניזכר כי $f = \sum_{i=1}^{n} a_i x^i$. נגיד כי f הוא **מתוקן** אם המקדם המוביל שלו הוא 1.

הגדרה 1.2 (אי־פריק): R תחום שלמות ו־$0 \neq r \in R$. r נקרא **אי־פריק (irreducible)** אם איננו הפיך ואין לו פריק אמיתי. משמע, אם מתוך $r = ab$ נובע ש־$a \in R^\times$ או $b \in R^\times$ (משמע $a \sim r$ או $b \sim r$).

הגדרה 1.3 (K־הומומורפיזם): TODOOOOOOOOOOOOOOOOOO

מסקנה 1.1: K־הומומורפיזם של שדות הוא תמיד שיכון.

הוכחה: TODOOOOOOOOOOOOOOOOOO □

1.2 בניות

1.3 שדות ראשוניים

2 הרצאה 2 – 25/03

2.1 הרחבת שדות

2.2 יוצרים של הרחבות

3 תרגול 1 – 26/03

3.1 משהו

4 הרצאה 3 – 31/03

4.1 הרחבות אלגבריות

5 תרגיל 1

5.1 טריקים

5.2 מסקנות

6 תרגול 2 – 02/04

6.1 משהו

7 הרצאה 4 – 07/04

7.1 שימושים בסיסיים של תורת השדות – בניות עם סרגל ומחוגה

8 הרצאה 5 – 08/04

8.1 שימושים בסיסיים של תורת השדות – בניות עם סרגל ומחוגה – המשך

להשלים הקדמה

8.2 למות גאוס

הערה: אנחנו נעבוד עם $\mathbb{Z}[t]$ אבל ברשומות (פרק 1) מופיע שאפשר לחקור באותה צורה את $R[t]$ כאשר R תחום פריקות יחידה (למשל, תחום ראשי).

הגדרה 8.1 (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 8.2 (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.

משפט 8.1 (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 הפולינומים 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 מפורשות:

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

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

מסקנה 8.1: כל ראשוני $p \in \mathbb{Z}$ ראשוני ב־$\mathbb{Z}[t]$ (לא ראינו בהרצאה, מסקנה 1.2.5 ברשומות של מיכאל).

הוכחה: נשים לב ש־$\mathbb{Z}[t]^\times = \mathbb{Z}^\times \not\ni p$ ולכן p מחלק פולינום $h \in \mathbb{Z}[t]$ אם ורק אם $p \mid \mathrm{cont}(h)$.

אם $p \mid f \cdot g$ אז מלמת גאוס הראשונה נובע $p \mid \mathrm{cont}(f) \cdot \mathrm{cont}(g)$ ולכן $p \mid f$ או $p \mid g$. $\square$

משפט 8.2 (למת גאוס השנייה): יהי $f \in \mathbb{Z}[t]$ פולינום לא קבוע. נזכור כי $\mathbb{Q}[t]$ הוא $\mathrm{Frac}(\mathbb{Z})$, שדה השברים של $\mathbb{Z}[t]$. אז

1. אם $f = g \cdot h$ פירוק ב־$\mathbb{Q}[t]$ אזי קיים $c \in \mathbb{Q}^\times$ כך ש־$0 \neq c$ ש־$c \cdot g, c^{-1} \cdot h \in \mathbb{Z}[t]$ ולכן $f = (c \cdot g) \cdot (c^{-1} \cdot h)$ פירוק ב־$\mathbb{Z}[t]$
2. אם f פולינום מתוקן ו־$f = g \cdot h \in \mathbb{Q}[t]$ פירוק מתוקן (דהיינו f, g מתוקנים) אזי $g, h \in \mathbb{Z}[t]$
3. אם f פולינום אי־פריק ב־$\mathbb{Z}[t]$ אם ורק אם f פרימטיבי ואי־פריק ב־$\mathbb{Q}[t]$

הוכחה:

1. ניקח את הפירוק $f = g \cdot h$ עבור $g, h \in \mathbb{Q}[t]$ וניקח $m, n \in \mathbb{Z}$ כך ש־$0 < m, n$ 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־$\alpha\beta = m \cdot n \cdot \ell$ ונקבל $\frac{1}{\ell} \cdot f = \frac{m \cdot n \cdot f}{m \cdot n \cdot \ell} = \underbrace{\frac{m}{\alpha} \cdot g \cdot \frac{n}{\beta} \cdot h}_{\in \mathbb{Z}[t]}$ משמע $f = \ell \frac{m}{\alpha} \cdot g \cdot \frac{n}{\beta} \cdot h$.
2. נניח ש־f גם מתוקן, ולכן בפרט הוא פרימיטיבי, ולכן קיים פירוק $f = g \cdot h \in \mathbb{Q}[t]$ עם g, h מתוקנים.
   לפי (1) נובע שקיים $c, c^{-1} \in \mathbb{Z}$ כך ש־$c \cdot g \cdot c^{-1} \cdot h \in \mathbb{Z}[t]$ כך ש־$c \cdot g \cdot c^{-1} \cdot h$ ש־$f = c \cdot g \cdot c^{-1} \cdot h$.
   נסמן $g = \sum_{i=1}^{n} a_i t^i, h = \sum_{j=1}^{m} b_j t^j$. היות ו־$f$ מתוקן נובע כי $a_n b_m = 1$ ולכן בהכרח $a_n = b_m = 1$, ו־$c \cdot g, c^{-1} \cdot h$ עדיין פולינומים מתוקנים ולכן $c = \pm 1$ ולכן $g, h \in \mathbb{Z}[t]$.
3. (הוכח בהרצאה 6)

$\Longleftarrow$ נניח כי f אי־פריק ב־$\mathbb{Z}[t]$ ולכן $f = \mathrm{cont}(f) \cdot \frac{f}{\mathrm{cont}(f)}$ פירוק טריוויאלי ונשים לב כי $\deg\left(\frac{f}{\mathrm{cont}(f)}\right) > 0$ 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 מ־(1) 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.

$\Longrightarrow$ בכיוון השני, נניח ש־f פריק ב־$\mathbb{Z}[t]$ ולכן $f=g\cdot h$ עם g,h לא הפיכים. יש 2 מקרים אפשריים:

1. אם $\deg(f),\deg(g)>0$ ואז נובע כי f פריק ב־$\mathbb{Q}[t]$ על־ידי פירוק זה וזאת סתירה
2. בלי הגבלת הכלליות $\deg(h)=0,\deg(g)>0$ ולכן $1<h\in\mathbb{Z}_+$ אבל אז f לא פרימיטיבי וזאת שוב סתירה

$\square$

מסקנה 8.2: $\mathbb{Z}[t]$ הוא חוג פריקות יחידה והראשוניים שלו הם פולינומים פרימטיביים אי־פריקים והראשוניים של $\mathbb{Z}$.

הערה: באותה צורה מוכיחים שאם R תחום פריקות יחידה אזי גם $R[t_1,...,t_n]$ הוא גם תחום פריקות יחידה (באינדוקציה על n).

9 תרגול 3 – 09/04

9.1 משהו

10 תרגיל 2

10.1 טריקים

10.2 מסקנות

11 הרצאה 6 – 21/04

11.1 קריטריונים לאי־פריקות ב־$\mathbb{Q}[t]$

המוטיבציה שלנו היא חקר הרחבות של $\mathbb{Q}[t]$ אבל זה לא פשוט. אי־פריקות בדרך־כלל קשה להבחנה להבדיל מקיום שורש ב־$\mathbb{Q}$: דוגמה טובה לכך היא t^4+4.

סימון: R תחום שלמות, בהינתן אידיאל ראשוני $I \subseteq R$ נסמן את התחום $R/I = \overline{R}$ ועבור $a \in R$ נסמן $\overline{a}$ בתמונה של $\overline{R}$.
כמו כן, ההומומורפיזם $R \to \overline{R}$ מתרחב להומומורפיזם $R[t] \to \overline{R}[t]$ כאשר $f = \sum_{i=0}^n a_i t^i \mapsto \sum_{i=0}^n \overline{a_i} t^i = \overline{f}$.

למה 11.1: נניח כי $f \in \mathbb{Z}[t]$ פולינום מתוקן, $p \in \mathbb{N}$ ראשוני כך ש־$\overline{f} \in \mathbb{F}_p[t](t)$ (מודלו p זה הומומורפיזם של חוגים) אי־פריק.
אזי f אי־פריק ב־$\mathbb{Q}[t]$.

הוכחה: נניח בשלילה כי f מתפרק ב־$\mathbb{Q}[t]$ ולכן קיים פירוק מתוקן $f = gh \in \mathbb{Q}[t]$ $(\deg g, \deg h > 0)$.
לפי (2) בלמת גאוס השנייה נובע כי $f = g \cdot h \in \mathbb{Z}[t]$ ואז $\overline{f} = \overline{g} \cdot \overline{h} \in \mathbb{F}_p[t]$ עם $\deg(\overline{g}), \deg\left(\overline{h}\right) > 0$ כי הפולינומים מתוקנים וזאת סתירה. □

תרגיל 11.1: $\mathbb{F}_p[t] = \mathbb{Z}[t]/p\mathbb{Z}[t]$

הוכחה: נגדיר $\varphi : \mathbb{Z}[t] \to \mathbb{F}_p[t]$ על־ידי $f(t) \mapsto \tilde{f}(t)$, כאשר $\tilde{f}(t)$ זה הפולינום המתקבל על־ידי הפחת כל מקדם ב־$f(t)$ למודלו p.
בדיקה קלה מראה כי זה אכן הומומורפיזם ונשים לב כי $\ker(\varphi) = \left\{ f(t) \in \mathbb{Z}[t] \mid \varphi(f) = 0 \in \mathbb{F}_p[t] \right\}$ אלו כל הפולינומים שבמודלו p הם מתאפסים משמע מתחלקים ב־p ולכן $\ker(\varphi) = p\mathbb{Z}[t]$. ממשפט האיזומורפיזם הראשון לחוגים נקבל

$$\mathbb{Z}[t]/\ker(\varphi) \cong \operatorname{Im}(\varphi) = \mathbb{F}_p[t] \Longrightarrow \mathbb{Z}[t]/p\mathbb{Z}[t] \cong \mathbb{F}_p[t]$$

□

משפט 11.1 (קריטריון אייזנשטיין (Eisenstein's criterion)): נניח ש־$f = \sum_{i=0}^n a_i t^i \in \mathbb{Z}[t]$ ו־$p \in \mathbb{N}$ ראשוני כך שמתקיימים הבאים

1. $p \nmid a_n$
2. $p \mid a_i$ לכל $0 \le i < n$
3. $p^2 \nmid a_0$

אז f אי־פריק.

הוכחה: נניח בשלילה שלא כך, ולכן מהלמות של גאוס נובע שמתקיים $f = g \cdot h = \sum_{j=1}^m b_j t^j \sum_{k=1}^l c_k^{t^k}$.
היות ו־$a_0 = b_0 c_0$ ו־$p \mid a_0$ נובע כי $p \mid b_0$ או $p \mid c_0$. בלי הגבלת הכלליות, נניח כי $p \mid b_0$ ו־$p \nmid c_0$ (שכן $p \mid a_0$ אבל $p \nmid a_0$ ולכן לא ניתן שגם $p \mid b_0$ וגם $p \mid c_0$).
ניקח את ה־$i \le m$ הקטן ביותר כך ש־$p \nmid b_i$ שקיים מהיות $b_m c_l = a_n$ ולכן $p \nmid b_m$.
כעת, בביטוי $a_i = b_i c_0 + \underbrace{b_{i-1} c_1 + \ldots + b_0 c_i}_{\text{מתחלקים ב־p}}$ אבל אז $p \nmid a_i$ וזאת סתירה.
אז f לא מתפרק לגורמים מדרגה גדולה מ־0 ואז f אי־פריק ב־$\mathbb{Z}[t]$ ומהלמה של גאוס נובע כי הוא גם אי־פריק ב־$\mathbb{Q}[t]$. □

דוגמה 11.1: יהי $x^n - m$ וקיים $p \in \mathbb{N}$ כך ש־$p \mid m$ ו־$p^2 \nmid m$ אז $x^n - m$ אי־פריק (ולא רק חסר שורשים).

אלדוגמה 11.1: $x^2 - m^2, x^2 + 4$ תמיד פריקים: אם $p \mid m^2$ אז גם $p \mid m$.

הגדרה 11.1 (פולינום ציקלוטומי): לפולינום מינימלי של שורש יחידה מעל $\mathbb{Q}$ נקרא **פולינום ציקלוטומי**.
לכל $n \in \mathbb{Z}$ מתאים פולינומים ציקלוטומי יחיד Φ_n שהוא פולינום מתוקן בעל מקדמים שלמים והוא הפולינום המינימלי של כל השורשים הפרמיטיביים מסדר n. משמע $\Phi_n(X) = \prod_\omega (X - \omega)$ כאשר ω עובר על כל השורשים הפרימיטיביים מסדר n.

דוגמה 11.2:

$$\Phi_1(x) = x - 1, \Phi_2(x) = x + 1, \Phi_3(x) = x^2 + x + 1, \Phi_4(x) = x^2 + 1, \Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

עבור $p \in \mathbb{N}$ ראשוני, אז כל פולינום הציקלוטומי מסדר p^n הוא $\frac{x^{p^n}-1}{x^{p^{n-1}}-1} \in \mathbb{Q}[x]$.
השלמה מויקיפדיה עבור n ראשוני, אז $\Phi_n(x) = \sum_{k=0}^{n-1} x^k$.
עבור $n = 2p$ עבור $p \neq 2$ ראשוני מתקיים $\Phi_n = \Phi_{2p} = \sum_{k=0}^{p-1} (-x)^k$.

למה 11.2: לכל $p \in \mathbb{N}$, הפולינום הציקלוטומי $\Phi_p(t) = \frac{t^p - 1}{t-1}$ אי־פריק מעל $\mathbb{Q}$.

הוכחה: זה טריק, נשנה משתנה ל־$x = t - 1$ ואז $t = x + 1$ ואז נקבל

$$\Phi_p(t) = \frac{(x+1)^p - 1}{x} = \left(x^p + px^{p-1} + \frac{p(p-1)}{2}\right)x^{p-2} + \ldots + px + 1 - \frac{1}{x} = x^{p-1} + \sum_{i=2}^{p-1} \binom{p}{i} x^{i-1} + p := f(x)$$

אז $f(x)$ אי־פריק לפי קריטריון אייזנשטיין שכן p מקדם חופשי מתוקן ו־$p \mid \binom{p}{i}$ לכל $0 < i < p$.

אם $\Phi_p(t)$ לא אי־פריק, אז קיימים $\Phi_p(t) = g(t) \cdot h(t) = g(x+1) \cdot h(x+1)$ וזאת סתירה. □

הערה: באותה צורה מוכיחים $\Phi_{p^n}(t) = \frac{t^{p^n} - 1}{t^{p^{n-1}} - 1}$ אי־פריק.

תרגיל 11.2 (תרגיל 10.104 בספר): הסיקו מקריטריון אייזנשטיין ששורש כלשהו של מספר ראשוני אינו שייך ל־$\mathbb{Q}$.

כלומר, הראו ש־$\sqrt[n]{p} \notin \mathbb{Q}$ לכל p ראשוני ו־$\mathbb{N} \ni n \geq 2$.

הוכחה: TODOOOOOOOOOOOOOOOOOO. □

תרגיל 11.3 (תרגיל 10.108 בספר): יהי $p \in \mathbb{N}$ ראשוני ויהי $f \in \mathbb{Z}[x]$ פולינום מתוקן. נסמן ב־$\overline{f} \in \mathbb{F}_p[x]$ את הפולינום המתקבל על־ידי פעולת מודלו p על כל מקדם בנפרד.

1. הוכיחו כי אם f פריק, אז גם $\overline{f}$ פריק.
2. הוכיחו כי ההפך הוא לא נכון – אם $\overline{f}$ פריק, לאו דווקא f פריק.

הוכחה: TODOOOOOOOOOOOOOOOOOO. □

11.2 סגור אלגברי

פרק 5 ברשומות של מיכאל, מוטיבציה: משוואות מסדר 5 לא ניתן לפתור.

הגדרה 11.2 (שדה סגור אלגברי): שדה K נקרא **שדה סגור אלגברית** אם לכל פולינום לא קבוע מעל K יש שורש ב־K.

הגדרה 11.3 (פולינום מתפצל לחלוטין): נגיד K שדה, נגיד כי $f \in K[t]$ **פולינום מתפצל לחלוטין** אם הוא מתפרק לגורמים לינאריים.

משמע, $f = c \prod_{i=1}^{\deg(f)} (t - a_i)$ כאשר $c \in K^\times$ ו־$a_i \in K$ לכל i.

למה 11.3: עבור שדה K הבאים שקולים

1. סגור אלגברית
2. כל פולינום $0 \neq f \in K[t]$ מתפצל לחלוטין
3. כל $f \in K[t]$ אי־פריק הוא מדרגה 1
4. ל־K אין הרחבות אלגבריות לא טריוויאליות

הוכחה: $(3) \iff (2)$ שכן תמיד יש פירוק לפולינומים אי־פריקים.

$(2) \implies (1)$: אם יש פירוק מלא, נובע מהגדרה שיש לי שורש.

$(1) \implies (2)$: נובע שלכל $f = g(t-a)$ יש פירוק כאשר $\deg g < \deg f$ ומסיימים את הטיעון עם אינדוקציה על $\deg(f)$.

$(4) \implies (1)$: אם קיימת הרחבה אלגברית לא טריוויאלית L/K ניקבל $\alpha \in L \setminus K$ ואז הפולינום $f_{\alpha/K}$ אי־פריק מדרגה $[K(\alpha):K] > 1$.

$(1) \implies (4)$: אם f אי־פריק ו־$\deg(f) > 1$ נגדיר $L = K[t]/(f)$ ו־$[L:K] = \deg(f) > 1$. □

הערה: השם סגור אלגברית נובע כי אין עוד הרחבות מעליהם.

משפט 11.2 (המשפט היסודי של האלגברה): $\mathbb{C}$ סגור אלגברית.

לא נוכיח כעת את המשפט אלא בהמשך, עד אז נשתמש בו על תנאי או בדוגמאות אך לא נסתמך עליו בהוכחות. יש לו כמה הוכחות (אלגברית, אנליטיות, טופולוגיות) אבל אנחנו נשתמש בכך שלכל פולינום $\mathbb{R}[t]$ מדרגה אי־זוגית יש שורש.

מסקנה 11.1:

1. כל פולינום לא קבוע ב־$\mathbb{R}[t]$ מתפרק למכפלה של גורמים לינאריים וריבועיים.
2. האי־פריקים ב־$\mathbb{R}[t]$ הם לינאריים וריבועיים עם $\text{dic} < 0$ (דיסקרמיננטה)

הוכחה: נשים לב $2 \iff 1$ ברור, ולכן מספיק שנוכיח רק את 1: נשים לב $\mathbb{R}[t] \subseteq \mathbb{C}[t]$ ו־$f = \overline{f}$ ולכן ההצמדה רק מחליפה את השורשים של $f = c\prod_{i=1}^{n}(t - a_i)$ (נשים לב שההצמדה היא בעצם תמורה, כי ההצמדה רק יכולה לשנות מיקום לשורשים אך לא את השורשים עצמם).

לטובת מי מבינינו שמתעב מרוכבים, ניזכר במספר עובדות קצרות. הצמוד המרוכב של מספר ממשי הוא ממשי. כמו־כן, הצמוד המרוכב סגור לחיבור

וכפל, כלומר הצמוד של מכפלה שווה למכפלה של צמודים, ואותו הדבר לחיבור. המשמעות היא שאם $f \in \mathbb{R}[x]$ פולינום ממשי, אז כפולינום מעל המרוכבים נקבל ש־$f = \overline{f}$. בשל סגירות זו, גם בפירוק לגורמים ליניאריים מעל המרוכבים מתקיים

$$\prod_{i=1}^{n}(x-a_i) = f(x) = \overline{f(x)} = \prod_{i=1}^{n}(x-\overline{a_i})$$

נוכל להסיק אם כך שהפירוק הלינארי אינווריאנטי לצמוד, כלומר לכל $1 \le i \le n$ או ש־$a_i \in \mathbb{R}$ או ש־$a_i \in \mathbb{C}$ וכן $\overline{a_i} \in \{a_i \mid 0 \le i \le n\}$.
נסמן את הממשיים כ־a_i ואת המרוכבים כ־α_j (תוך מחיקת הצמודים), ונקבל,

$$f(x) = \prod_{i=1}^{k}(x-a_i) \cdot \prod_{j=1}^{m}(x-\alpha_j)(x-\overline{\alpha_i})$$

כלומר f הוא מכפלה של גורמים לינאריים ממשיים ושל

$$(x-\alpha_i)(x-\overline{\alpha_i}) = x^2 - 2(\alpha_i + \overline{\alpha_i}) + \overline{\alpha_i}\alpha_i$$

אבל כפל של מספר בצמוד שלו הוא ממשי, וכן חיבור מספר מרוכב לצמוד שלו (עוד שתי זהויות חשובות), ולכן זהו גורם ריבועי ממשי. $\square$

מסקנה 11.2: נניח כי L/K הרחבה, L סגור אלגברית ונגדיר $F = \{\alpha \in L \mid K \text{ אלגברי מעל } \alpha\}$.
אז F סגור אלגברית וזה נקרא **הסגור האלגברי** (Algebraic closure) של K ב־L.

הוכחה: נניח F לא סגור אלגברית, כלומר $f(t) \in F[t]$ אי־פריק עם דרגה גדולה מ־1. אז יש ל־f שורש ב־L (כי L סגור אלגברית) עם שורש, אבל α אלגברי מעל F ולכן α/K אלגברי ואז $\alpha \in F$ וזאת סתירה. $\square$

דוגמה 11.3:

1. $\overline{\mathbb{Q}}$ הוא הסגור האלגברי של $\mathbb{Q}$ ולכן גם סגור אלגברית מעל $\mathbb{Q}$
2. $\mathbb{C} = \overline{\mathbb{R}} = \overline{\mathbb{C}}$
3. $\overline{\mathbb{Q}} = \overline{\mathbb{Q}\left(\sqrt[3]{2} + \sqrt[3]{5}\right)}$

12 הרצאה 7 – 22/04

12.1 קיום ויחידות סגור אלגברי

פרקים 5.3, 5.4 ברשומות של מיכאל. המטרה שלנו בזמן הקרוב זה להראות שלכל שדה K **קיים ויחיד עד־כדי איזומורפיזם** $\overline{K}$, סגור אלגברי.

הערה: סגור אלגברי $\overline{K}/K$ הוא הרחבה אלגברית ולפי הגדרה מקסימלית ביחס להכלה. לכן, טבעי לבנות אותו על־ידי הלמה של צורן (אינדוקציה בעייתית לנו כי לא בהכרח זה בן־מנייה) ונעבוד עם חסימה של העוצמה.

הגדרה 12.1 (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.

למה 12.1: 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 סופיים (שכן המקור של כל פולינום $f \in K[t]$ מכיל את כל השורשים שלו ב־L), ולכן

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

□

משפט 12.1 (קיום סגור אלגברי): לכל שדה K קיים סגור אלגברי $\overline{K}/K$.

הוכחה: 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 $+_L \mid_K +_K$, $\cdot_L \mid_K = \cdot_K$.
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 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. □

הערה: השתמשנו בהוכחה לעיל ש־$L/\overline{K}$ הרחבה אלגברית שכן $L/\overline{K}/K$ מגדל הרחבות.

למה 12.2 (למת ההרמה): נניח כי K שדה ו־L/K הרחבה אלגברית הנוצרת על־ידי $S \subseteq L$ ו־E/K הרחבת שדות כך שהפולינום המינימלי לכל $\alpha \in S$ מתפצל לחלוטין מעל E. אזי קיים K־שיכון של שדות $\phi : L \hookrightarrow E$.

הוכחה: נטען כי קיימת הרמה מקסימלית $E \hookrightarrow K$ לתת־שדה L: נסתכל על הקבוצה $\mathcal{V}$ המכילה את כל ה־K תתי־שדות $F_i \subseteq L$ ושיכון של K־שדות $\phi_i : F_i \hookrightarrow E$, זוהי קבוצה עם סדר חלקי: $(F_1, \phi_1) \leq (F_2, \phi_2)$ אם $F_1 \subseteq F_2$ ו־$\varphi_1 = \phi_2 \mid_{L_1}$, ויותר מזה לכל שרשרת $\{(F_i, \phi_i)\}_{i \in I}$ יש חסם עליון הנתון על־ידי $F = \cup_i \in IF_i$ ו־$\phi : L \hookrightarrow E$ כך שמתקיים ϕ_i $\phi \mid_{L_i}$ לכל i.
מהלמה של צורן קיים איבר מקסימלי $(F, \phi) \in \mathcal{V}$ ונטען כי $F = L$ ולכן ϕ הוא השיכון $E \hookrightarrow L$ המבוקש:
נניח בשלילה שלא, ולכן קיים $\alpha \in S$ כך ש־$\alpha \notin F$, אבל $f_{\alpha/K} \mid f_{\alpha/F}$ (מההנחה שהפולינום המינימלי לכל $\alpha \in S$ מתפצל לחלוטין מעל E) ולכן בפרט $f_{\phi(\alpha)/K} \mid f_{\phi(\alpha)/F} \iff \phi\left(f_{\alpha/K}\right) \mid \phi\left(f_{\alpha/F}\right)$ ולכן ל־$\phi(f)$ יש שורש $\beta \in E$ ואז $\phi(F) = F' \subseteq E$ המקיים

$$F(\alpha) = F[t]/(f_\alpha) \xrightarrow{\sim} F'[t]/(\phi(f_\alpha)) = F'(\beta)$$

משמע אנחנו יכולים להרים את ϕ אל $F(\alpha)$ על־ידי שליחה של α ל־β, משמע $\psi : F(\alpha) \hookrightarrow F'(\beta) \subseteq E$, אבל זאת סתירה למקסימליות של (F, ϕ) $\square$

הערה: ההוכחה לעיל התחילה בהרצאה של ה־22/04 הסתיימה ב־28/04.

13 תרגול 4 – 23/04

13.1 שדות פיצול

הגדרה 13.1 (מקרה פרטי של שדה פיצול): יהי $f \in \mathbb{Q}[x]$. ***שדה הפיצול של f*** הוא תת־השדה המינימלי של $\mathbb{C}$ שמכיל את שורשי f.

דוגמה 13.1: השורשים של $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ הם $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ כאשר $\omega = \frac{1}{2} + \sqrt{\frac{3}{4}}i$.
אז שדה הפיצול של f הוא $L = \mathbb{Q}\left(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right)$

תרגיל 13.1: מה הם כל השדות K כך שמתקיים $\mathbb{Q} \subseteq K \subseteq L$?

פתרון: מתקיים $[L:\mathbb{Q}] = \left[L:\mathbb{Q}\left(\sqrt[3]{2}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]$ $\square$

14 הרצאה 8 – 28/04

14.1 קיום ויחידות סגור אלגברי – המשך

למה 14.1 (bootstrap ללמת ההרמה): בנוסף להנחות של למת ההרמה, נניח כי גם מתקיים $\alpha \in L$ ו־$\beta \in E$ הוא השורש של הפולינום המינימלי $f_\alpha \in K[t]$ ב־E. אזי ניתן לבחור את ה־K שיכון $\varphi : L \hookrightarrow E$ כך שמתקיים $\varphi(\alpha) = \beta$.

הוכחה: היות ו־β הוא שורש של פולינום אי־הפיך f_α, יש לנו $f_\beta = f_\alpha$ ולכן יש הומומורפיזם $\phi_0 : K(\alpha) \xrightarrow{\sim} K(\beta) \subseteq E$.
S יוצרת את L מעל $K(\alpha)$ והפולינום המינימלי של כל $\gamma \in S$ מעל $K(\beta)$ מחלק את הפולינום המינימלי של γ מעל K ולכן מתפצל לחלוטין מעל E.

לכן, מלמת ההרמה ההומומורפיזם $\phi_0 : K(\alpha) \hookrightarrow E$ מורם להומומורפיזם $\phi L \hookrightarrow E$ ומבנייה קיבלנו את ϕ הנדרש. $\square$

משפט 14.1 (אי־יחידות של סגור אלגברי): *יהי K שדה ו־$\overline{K}/K$ ו־$\widetilde{K}'/K$ סגורים אלגבריים של K. אז קיים K־איזומורפיזם $\phi : \overline{K} \xrightarrow{\sim} \overline{K}'$.*
יתרה מכך, אם $f \in K[t]$ הוא פולינום אי־פריק עם שורשים $\alpha \in \overline{K}$ ו־$\alpha' \in \overline{K}'$, אז ניתן לבחור ϕ כך שיתקיים $\varphi(\alpha) = \alpha'$.

הוכחה: מהיות $\overline{L}/L$ הרחבה אלגברית וכל פולינום $f \in K[t]$ מתפצל לחלוטין מעל $\overline{K}'$, מלמת ההרמה נתקבל K־שיכון $\phi : \overline{K} \hookrightarrow \overline{K}'$.
אבל $\phi\left(\overline{K}\right)$ הוא סגור אלגברית ו־$\overline{K}'/\phi\left(\overline{K}\right)$ הוא אלגברי, נקבל כי $\phi\left(\overline{K}\right) = \overline{K}'$ ואז ϕ הוא איזומורפיזם, ומלמת ההרמה (bootstrap) נקבל $\phi(\alpha) = \alpha'$.
למה ϕ הוא על? אם לא, יש $x \in \overline{K}' \setminus \overline{K}$ לא אלגברי מעל $\overline{K}$ כי $\overline{K}$ סגור אלגברית ואז הוא לא אלגברי מעל K, אבל הנחנו שההרחבה $\overline{K}'/K$ היא אלגברית וזו סתירה. $\square$

הערה: סגור אלגברי $\overline{K}$ היינו יחיד עד־כדי איזומורפיזם σ, אבל σ לא יחיד:
ניתן לקחת את $\mathbb{Q}$ ולבנות ממנו את $\mathbb{R}$, אבל אין לו אוטומורפיזמים.
אם נבנה ממנו את $\mathbb{C}$, נקבל כמה אוטומורפיזמים – לדוגמה אוטומורפיזם ההצמדה $\alpha \mapsto \overline{\alpha}$ ואז אין $\mathbb{C}$ "נכון".

14.2 אוטומורפיזמים של $\overline{K}/K$

פרק 5.5 ברשומות של מיכאל.

סימון: עבור הרחבת שדות L/K נסמן את $\mathrm{Aut}(L/K)$ לפעמים גם בתור $\mathrm{Aut}_K(L)$.

הגדרה 14.1 (איברים צמודים): עבור הרחבת שדות L/K, נגיד כי $\alpha, \beta \in L$ הם **צמודים** אם $f_{\alpha/K} = f_{\beta/K}$.

הגדרה 14.2 (מחלקת צמידות): עבור הרחבת שדות L/K ו־$\alpha \in L$. אם f_α מתפצל לחלוטין ב־L אז קבוצת כל השורשים שלו (קבוצת כל הצמודים של α) מסומנת ב־C_α, **מחלקת צמידות** של α.

משפט 14.2: אם K שדה ו־$\overline{K}/K$ סגור אלגברי שלו, אז לכל $\alpha \in \overline{K}$ המסלול שלו תחת הפעולה של $\mathrm{Aut}\left(\overline{K}/K\right)$ היינה מחלקת צמידות של C_α.
הוכחה: בכיוון הראשון, אם $\sigma : \overline{K} \to K \ni \mathrm{Aut}\left(\overline{K}/K\right)$ אז $\sigma\left(f_{\alpha/K}\right) = f_{\sigma(\alpha)/K}$ שכן $\sigma \mid_K = \mathrm{Id}_K$ (כי אם $\sum a_i \alpha^i = 0$ אז $\sum \sigma(a_i)\sigma(\alpha)^i$), ולכן $\sigma(\alpha) \in C_\alpha$ ולכן המסלול של α שייך ל־C_α.
בכיוון השני, עבור כל $\alpha' \in C_\alpha$ (שורש אחר של f_α), קיים $\sigma : \overline{K} \to \overline{K}$ (bootstrap) כך ש־$\sigma(\alpha) = \overline{\alpha}$. מהיות $\overline{K}$ סגור אלגברית ואלגברי מעל K, ההרחבה $\overline{K}/\sigma\left(\overline{K}\right)$ היא טריוויאלית ולכן σ הוא אוטומורפיזם. $\square$

למה 14.2: נניח כי $L = K(\alpha)/K$ הרחבה אלגברית פשוטה (נוצרת על־ידי איבר אחד) מדרגה d ונניח כי F/K הרחבה.
אזי כל K־שיכון $\phi : L \hookrightarrow F$ לוקח את α לשורש $\phi(\alpha)$ של $f_{\alpha/K}$, וזה משרה העתקה חד־חד ערכית

$$\mathrm{Hom}_K(L, F) \simeq \{\beta \in F \mid f_\alpha(\beta) = 0\}$$

ובפרט מתקיים $|\mathrm{Hom}_K(L, F)| \leq d$ (חסם על כמות ההרמות).
הוכחה: אכן $\phi(\alpha)$ הוא שורש של $\varphi\left(f_{\alpha/K}\right) = f_{\alpha/K}$ ולכל $\beta \in F$ שורש של $f_{\alpha/K}$ מתקיים

$$L = K(\alpha) \underset{\beta}{\overset{\phi}{\simeq}} K(t)/f_\alpha \simeq K(\beta) \subseteq F$$

ϕ_β נקבע ביחידות על־ידי β כי $\left\{1, \alpha, ..., \alpha^{d-1}\right\}$ זה בסיס של L מעל K ולכן לכל $a \in L$ יש יצוג יחיד $\sum_{i=0}^{n-1} a_i \alpha^i$ ואז כל הומומורפיזם $\phi' : L \to F$ כך ש־$\phi'(\alpha) = \beta$ מקיים $\phi'(\alpha) = \sum_{i=0}^{d-1} a_i \beta^i$. $\square$

הגדרה 14.3 (דרגה ספרבילית, דרגה אי־ספרבילית): יהי $\alpha \in L$ אלגברי מעל K עם דרגה d.

הדרגה הספרבילית של α מעל K שתסומן $\deg_{K,s}(\alpha)$ $= \deg_s(\alpha)$ היא העוצמה של מחלקות הצמידות של $\alpha \in \overline{K}$ (בסימוני ההרצאות של מיכאל $\deg_s(\alpha) = \deg_{K,s}(\alpha) = |C_\alpha|$).

הדרגה האי־ספרבילית של α מעל K שתסומן $\deg_{K,i}(\alpha)$ $= \deg_i(\alpha)$ היא הריבוי של α ב־f_α: TODOOOOOOOOOOOOOOOOOOO

הערה: TODOOOOOOOOOOOOOOOOOOO

דוגמה 14.1: TODOOOOOOOOOOOOOOOOOOO

דוגמה 14.2: TODOOOOOOOOOOOOOOOOOOO

15 הרצאה 9 – 29/04

15.1 אוטומורפיזמים של $\overline{K}/K$ – המשך

יהיו K שדה, $f \in K[t]$ פולינום ממעלה n ו־L/K הרחבת שדות שבה f מתפצל, כלומר

$$f = c(x-\alpha_1)\cdot(t-\alpha_2)\cdot\ldots\cdot(t-\alpha_n) \in L[t]$$

הגדרה 15.1 (שורש פשוט): נאמר ש־$\alpha = \alpha_i \in L$ הוא **שורש פשוט (simple root)** של f אם הוא מופיע בידיוק פעם אחת בפיצול. כלומר, $f \mid (t-\alpha)$ אבל $f \nmid (t-\alpha)^2$.

הגדרה 15.2 (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 $f \mid (t-\alpha)^2$.

הגדרה 15.3 (פולינום פריד (ספרבילי)): הפולינום $f \in K[t]$ נקרא **פריד (ספרבילי, Separable)** אם אין לו שורשים מרובים בשדה ההרחבה L שבו הוא מתפצל.

הערה (מסקנה 14.7 בספר): תכונת הספרביליות של פולינום אינה תלויה בשדה ההרחבה L שבו הוא מתפצל.

למה 15.1: יהי K שדה, אזי $f \in K[t]$ הוא פריד אם ורק אם $\gcd(f,f') = 1$ (כאשר f' הוא הנגזרת של f).

הוכחה: $\Longrightarrow$ נניח כי $\gcd(f,f') = 1$.
מההנחה נובע $1 = uf + vf' \in K[t]$ ולכן גם ב־$\overline{K}$.
נניח f אי־פריד נובע כי $t-\alpha)^2 \mid f \in \overline{K}[t]$ ולכן $(t-\alpha) \mid f'$ ולכן $t-a \mid 1 = uf+vg$, סתירה.
$\Longleftarrow$ נניח כי $f \in K[t]$ הוא פריד.
נסמן $f' = ((t-a_i)g)' = g'(())$. מתקיים

$$f' = ((t-\alpha_i)g)' = g'(t-a_i) + g(t-\alpha_i) + g$$

אבל

$$(t-a_i) \mid f' = g'(t-a_i) + g \Longleftrightarrow (t-\alpha_i) \mid g$$

אבל זה קורה אם ורק אם $(t-\alpha_i)$ שורש מרובה. $\square$

הערה: ברשומות של מיכאל, ההוכחה המפורטת בכיוון $\Longleftarrow$ היא:
$\Longleftarrow$ נניח כי $f \in K[t]$ הוא פריד.
מתקיים $f' = ((t-\alpha_i)g)' = g'(t-a_i)+g$ נניח בשלילה כי $\gcd(f,f') \neq 1$ ונסמן ב־$g \in K[t]$ מחלק אי־פריק. אז $f = gh$ ו־$g \mid f' = h'g + hg'$.
נובע מכך ש־$g \mid hg'$ ולכן או ש־$g \mid h$ או ש־$g \mid g'$.
במקרה הראשון, $g^2 \mid f$ ולכן נקבל כי f אי־פריד וזו סתירה.
במקרה השני, g מחלק פולינום ממעלה נמוכה יותר ולכן $g' = 0$ (כי אחרת נקבל ש־g הוא פולינום פריק מטעמי דרגות וזו סתירה), אבל אז כל המונומים (שלא אפסים) של $g = \sum_{i=0}^{d} c_i t^i$ הם מהצורה $c_{pj}t^{pj}$ כאשר $p = \operatorname{char}(K) > 0$, אבל אז $g = \left(\sum_{j=0}^{\frac{d}{p}} c_{pj}^{\frac{1}{p}} t^j\right)^p$ הוא אי־פריד וזו סתירה.

תרגיל 15.1: f ו־f' הוא אותו פולינום הן ב־$K[t]$ והן ב־$\overline{K}[t]$.

הוכחה: TODOOOOOOOOOOOOOOOOOO? $\square$

משפט 15.1: נניח כי $f \in K[t]$ פולינום אי־פריק ומתוקן ו־$\alpha \in \overline{K}$ שורש של f. אזי

1. אם $\operatorname{char}(K) = 0$ אז f ו־α הם פרידים ואז $\deg_i(\alpha) = \deg(f) = \deg_K(\alpha)$
2. אם $\operatorname{char}(K) = p$ אז קיים פולינום אי־פריק ופריד $g \in K[t]$ ו־$l \geq 0$ כך ש־$f(t) = g\left(t^{p^l}\right)$.

יתרה מכך, אם $\beta_1, \ldots, \beta_n$ הם השורשים של g כאשר $n = \deg(g)$ אז ל־f יש n שורשים שונים זה מזה $\alpha_j = \beta_j^{\frac{1}{p^l}}$ וכל אחד מהם הוא מריבוי של p^l (משמע $f = \prod_{i=1}^{n}(t-\alpha_i)^{p^l}$).
בפרט, מתקיים $\deg_s(\alpha) = n, \deg_i(\alpha) = p^l, \deg(\alpha) = np^l$.

הוכחה: נסמן $d = \deg(f)$ ונניח כי $d > 1$ שכן אחרת הכל טריוויאלי.
ראינו ש־f אי־פריד אם ורק אם $\gcd(f,f')$ f פריד אם ורק אם $\gcd(f,f') = 1$. אם זה קורה ו־$f' \neq 0$ אז $0 < \deg\gcd(f,f') \leq \deg f' <$

$\deg f$ ולכן ל־f יש גורם לא טריוויאלי וזו סתירה (כי f אי־פריד) ולכן $\gcd(f, f') \neq 1$ אם ורק אם $f' = 0$.

מכאן, אם $\mathrm{char}(K) = 0$ אז $f' \neq 0$ ולכן $\deg f' = \deg f - 1$ ולכן f פריד.

אם $\mathrm{char}(K) = p$, אז f פריד וסיימנו או ש־$f' = 0$.

נניח כי $f = \sum_{i=0}^{d} a_i t^i$ אז אם $f' = \sum_{i=1}^{d} i a_i t^i = 0$, אז לכל $i > 0$ בהכרח מתקיים $i a_i = 0 \in K$ ולכן רק המקדמים $a_{pj} \neq 0$.

במילים אחרות מתקיים

$$f' = 0 \iff f = \sum_{j=-}^{\frac{d}{p}} a_{pj} t^{pj}$$

ואז $g(x) = \sum a_{pj} x^j$ ו־$f = g(t^p)$. אבל g הוא אי־פריק: אחרת $g(x) = g_1(x) g_2(x)$ ואז $f(t) = g(t^p) = g_1(t^p) g_2(t^p)$ וזו כמובן סתירה.

אז g אי־פריק ובאינדוקציה על $\deg(g) < \deg(f)$ נקבל $g = h\left(t^{p^m}\right)$ ו־h פריד ולכן $f = h\left(t^{p^{m+1}}\right)$.

נסמן $n = \deg(h) = \frac{d}{p^l}$, $p^l = p^{m+1}$. h פריד ולכן $h(x) = \prod_{i=1}^{n} (x - \beta_i)$ ויש לו n שורשים שונים, ואם נבחר $x = t^{p^l}$ נקבל $f = \prod_{i=1}^{n} \left(t^{p^l} - \beta_i\right)$, וניקח $\alpha_i = \beta_i^{\frac{1}{p^l}} \in \overline{K}$ ואז המכפלה שלנו (פרובניוס) היא $f = \prod_{i=1}^{n} (t - \alpha_i)^{p^l}$ וסיימנו. $\square$

15.2 הרחבות נורמליות

פרק 5.6 ברשומות של מיכאל.

הגדרה 15.4 (הרחבה אלגברית נורמלית): הרחבה אלגברית L/K נקראת **נורמלית** אם לכל K־שיכון $\sigma : L \hookrightarrow \overline{K}$ אותה התמונה $\sigma(L) \subseteq \overline{K}$ (לא תלוי בבחירת $\overline{K}/K$).

משפט 15.2: עבור הרחבה אלגברית L/K הבאים שקולים

1. L/K נורמלית
2. אם $\overline{L}/L$ סגור אלגברי של L, אזי $\mathrm{Aut}\left(\overline{L}/L\right)$ לוקחת את L לעצמו (לא מזיזה אותו)
3. לכל $\alpha \in L$, $f_{\alpha/K}$ מתפצל לחלוטין ב־L

הוכחה: $1 \Rightarrow 2$: בעצם, $\overline{L}$ זה גם סגור אלגברי של K (מיחידות עד־כדי איזומורפיזם), ואז כל $\sigma \in \mathrm{Aut}\left(\overline{L}/K\right)$ נותן שיכון אחר $\sigma(L) \subseteq \overline{L}$ ולכן $\sigma(L) = L$.

$2 \Rightarrow 3$: ניקח $\alpha' \in \overline{L}$ שהוא שורש אחר של $f_{\alpha/K}$ ולכן לפי משפט שראינו על חבורות $\mathrm{Aut}\left(\overline{L}/K\right)$ (להשלים) **TODOOOOOOOOOOOOOOOOOO**, קיים $\sigma \in \mathrm{Aut}\left(\overline{L}/K\right)$ כך ש־$\sigma(\alpha) = \alpha'$ וזה בדיוק אומר ש־$f_{\alpha/K}$ מתפצל לחלוטין ב־L.

$3 \Rightarrow 1$: ניקח K־שיכון $\sigma : L \to \overline{K}$ ולכן לכל $\alpha \in L$ מתקיים $f_{\alpha/K} = f_{\sigma(\alpha)/K}$ וכל שורשיו $C_{\sigma(\alpha)} = C_\alpha \subseteq L$ לפי ההנחה, ולכן $\sigma(L) = \cup_{\alpha \in L} C_{f_{\alpha/K}}$ לא תלוי בשיכון. $\square$

הערה: את הכיוון $2 \Rightarrow 1$ מיכאל הוכיח ברשומות שלו בשלילה: נניח ש־L/K היא לא נורמלית ולכן קיים K־שיכון $\phi : L \hookrightarrow \overline{L}$ כך שמתקיים $\phi(L) \neq L$.

מלמת ההרמה, ϕ מורחב ל־K־שיכון של שדות $\sigma : \overline{L} \hookrightarrow \overline{L}$ שחייב להיות איזומורפיזם שכן $\overline{L}/\sigma\left(\overline{L}\right)$ זו הרחבה אלגברית של סגור אלגברי של שדות, ולכן הרחבה טריוויאלית.

לכן $\sigma \in \mathrm{Aut}_K\left(\overline{L}\right)$ לא משמר את L, אבל זו סתירה להנחה של (2).

16 תרגיל 3

16.1 טריקים

1. הבינום של ניוטון ככלי לחלוקת פולינומים (אפשר גם סכום סדרה הנדסית)
2. היה גם בהרצאה, אבל בשביל קריטריון אייזנשטיין כדאי להשתמש בטריק $x \mapsto x+1$
3. לפשט ביטויים בתוך שורש, לדוגמה

$$\sqrt{11+6\sqrt{2}} = \sqrt{9+6\sqrt{2}+2} = \sqrt{9+6\sqrt{2}+\sqrt{2}^2} = \sqrt{\left(3+\sqrt{2}\right)^2} = 3+\sqrt{2}$$

4. פולינום יכול להיות אי־פריק אבל לא לקיים את קריטריון אייזנשטיין (אני מניחה שזה ככל הנראה המקרים בהם $a_n = 1$)

16.2 מסקנות

1. עבור $p_1, ..., p_n$ ראשוניים שונים זה מזה מתקיים $\left[\mathbb{Q}\left(\sqrt{p_1}, ..., \sqrt{p_n}\right) : \mathbb{Q}\right] = 2^n$ ובסיס ל־$\mathbb{Q}\left(\sqrt{p_1}, ..., \sqrt{p_n}\right)$ הוא

$$\mathcal{B} = \left\{ \sqrt{\prod_{i\in S} p_i} \mid S \subseteq \{1, ..., n\} \right\}$$

17 הרצאה 10 – 05/05

17.1 הרחבות נורמליות – המשך

מסקנה 17.1: אם $L \ni \alpha$ ו־L/K נורמלית, אזי $f_{\alpha/K}$ מתפצל לחלוטין ($C_\alpha \subset L$) ו־$\mathrm{Aut}(L/K)$ פועלת טרנזטיבית על C_α.

הוכחה: TODOOOOOOOOOOOOOOOOOO □

דוגמה 17.1: עבור $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$, חבורת האוטומורפיזמים היא רק הזהות.

דוגמה 17.2 (טרנזטיביות/אי־טרנזטיביות של הרחבות נורמליות): בדומה לכך שנורמליות היא לא תכונה טרנזטיביות בין חבורות, גם מחלקת ההרחבות הנורמליות היא לא שלמה, בכמה דרכים: נניח כי $L/F/K$ מגדל הרחבות.

1. נניח L/F ו־F/K הרחבות נורמליות, נטען כי L/K לא הרחבה נורמלית: $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$
2. נניח L/K נורמלי ונטען שלא בהכרח F/K נורמלית – TODOOOOOOOOOOOOOOOOOO
3. נניח כי L/K נורמלית ונטען כי L/F כ נורמלית TODOOOOOOOOOOOOOOOOOO

תרגיל 17.1: L/K הרחבה ריבועית גורר כי L/K נורמלית (אנלוגי לחבורה מאינדקס 2 היא נורמלית).

הוכחה: TODOOOOOOOOOOOOOOOOOO □

17.2 שדות פיצול

פרק מספר 5.6 ברשומות של מיכאל.

הגדרה 17.1 (שדה פיצול): נניח K שדה ו־L/K הרחבה ו־$P \subseteq K[t]$ קבוצת פולינומים שונה מ־0.
L נקרא **שדה פיצול של P** אם כל $f \in P$ מתפצל לחלוטין ב־L ו־$L = K(S)$ כאשר $S = \{\text{כל השורשים של } f \in P\}$.
בפרט, L/K אלגברית שכן היא נוצרת על־ידי השורשים.

למה 17.1: אם K שדה ו־$P \subseteq K[t]$ קבוצת פולינומים שונה מ־0 אזי שדה פיצול של P מעל K קיים ויחיד עד־כדי איזומורפיזם (שבדרך־כלל אינו יחיד).

הוכחה: ניקח $\overline{K}$ ו־$S \subseteq \overline{K}$ $= \{\text{כל השורשים של } f \in P\}$ ואז $K(S) = L \subseteq \overline{K}$ שדה פיצול.
אם L' שדה פיצול אחר, קיים הומומורפיזם $\phi : L \hookrightarrow L'$ מלמת ההרמה (L נוצר על־ידי S ו־L' מפצל כל $f \in P$) ולבסוף $K(\phi(S)) = L'$ כאשר $\phi(S)$ הם השורשים ולכן $L \xrightarrow{\sim} L'$. □

הערה: סגור אלגברי הוא שדה פיצול של כל הפולינומים.

משפט 17.1:

1. הרחבה אלגברית L/K היינה נורמלית אם ורק אם L הוא שדה פיצול של $P \subseteq K[t]$ שאינם 0
2. ההרחבה אלגברית L/K היינה נורמלית וסופית אם ורק אם L הוא שדה פיצול של $f \in K[t]$ פולינום בודד (ואולי אף פריק)

הוכחה:

1. $\Leftarrow$ L/K נורמלית אזי L הוא שדה פיצול של $\left\{f_{\alpha/K} \mid \alpha \in L\right\}$ כי כל $f_{\alpha/K}$ מתפצל לחלוטין.
$\Longrightarrow$ נניח L שדה פיצול של P ולכן $L = K(S)$ כאשר $S = \{f \in P \text{ שורשי}\}$. נסתכל על $\overline{K} \circlearrowleft \in \mathrm{Aut}\left(\overline{K}/K\right)$, מתקיים $\sigma(S) = S$ ולכן $K(S) = K(\sigma(S))$ משמע $\sigma(L) = L$, ולכן לפי התנאים השקולים לנורמליות נקבל ש־L/K נורמלית.
2. $\Leftarrow$ L/K נורמלית סופית וניקח יוצרים $L = K(\alpha_1, \ldots, \alpha_n)$ וניקח $f = \prod_{i=1}^n f_{\alpha_i/K}$, אז כל α_i שורשים של f ו־f מתפצל לחלוטין.
$\Longrightarrow$ אם L/K שדה פיצול של $f \in K[t]$ אז $L = K(\alpha_1, \ldots, \alpha_n)$ כאשר $\alpha_1, \ldots, \alpha_n$ הם השורשים של f והלכן L/K אלגברית וגם נוצרת סופית ולכן סופית.

□

הגדרה 17.2 (L^{nor}): נניח L/K הרחבה אלגברית, ניקח (תלוי גם ב־K), $\boldsymbol{L^{nor}}$ שדה פיצול של $P = \left\{f_{\alpha/K} \mid \alpha \in L\right\}$ (P יחידה עד־כדי איזומורפיזם).
L^{nor} זה הסגור הנורמלי של L מעל K.

למה 17.2: L^{nor}/K זו הרחבה נורמלית מינימלית (ביחס להכלה) המכילה את L.

הוכחה: L^{nor}/K שדה פיצול (של P) ולכן נורמלית.
כמובן, $L^{nor} = K(S)$ כאשר S זה שורשי $P \subset L$ ולכן $L \subseteq L^{nor}$.
לבסוף, אם $L^{nor} \supseteq F \supseteq L \supseteq K$ כאשר F/K נורמלית, נובע כי כל $f_{\alpha/K} \in P$ מתפצל לחלוטין ב־F ולכן $F = L^{nor}$. □

דוגמה 17.3: $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)=L^{nor}/L=\mathbb{Q}\left(\sqrt[3]{2}\right)/K=\mathbb{Q}$.
TODOOOOOOOOOOOOOOOOOOO ציור?

דוגמה 17.4: $L=\mathbb{Q}\left(\sqrt[4]{2}\right)$ ואז $L^{nor}=\mathbb{Q}\left(\sqrt[4]{2},i\right)$ ואז TODOOOOOOOOOOOOOOOOOOO ציור?

למה 17.3: יהי K שדה, $f\in K[t]$ פולינום מדרגה $d>0$ (פולינום לא קבוע) ו־L שדה פיצול של f. נסמן $C_f=\{f \text{ כל שורשי}\}$ אזי
1. $[L:K]\le d!$
2. כל $\sigma\in \operatorname{Aut}_K(L)=\operatorname{Aut}(L/K)$ משרה תמורה על C_f וההומומורפיזם הצמצום מ־$\operatorname{Aut}_K(L)\to \operatorname{Perm} C_f=\operatorname{Aut}(C_f)=S_n$ הוא שיכון.

הוכחה: TODOOOOOOOOOOOOOOOOOOO $\square$

17.3 שורשי יחידה

פרק 6.1 ברשומות של מיכאל.

הגדרה 17.3 (שורש יחידה מסדר n): יהי $n\in\mathbb{N}$. **שורש יחידה מסדר n** בתוך $\overline{K}$ הוא $\zeta\in\overline{K}$ שמקיים $\zeta^n=1$.

הגדרה 17.4 (חבורת μ_n, חבורת שורשי היחידה מסדר n): עבור K שדה ו־$1\le n\in\mathbb{N}$ נגדיר

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

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

נשים לב ש־$\mu_n(K)$ היא תת־חבורה של $K^\times$ מסדר המחלק את n (זוהי כמובן חבורה אבלית עם כפל).

סימון: 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.

דוגמה 17.5:

$$\mu_\infty(\mathbb{R})=\mu_\infty(\mathbb{Q})=\{\pm 1\}=\mu_2$$

$$\mu_\infty=\mu_\infty(\mathbb{C})=\left\{e^{\frac{2\pi i m}{n}}\mid 1\le m\le n,(m,n)=1\right\}$$

תרגיל 17.2: (בהרצאה מיכאל נתן את זה כדוגמה ופירט קצת, ברשומות שלו זה מופיע כתרגיל אז נוכיח במסודר)
1. נראה שמתקיים $\mu_\infty\left(\mathbb{Q}\left(\sqrt{-3}\right)\right)=\mu_6$
2. נראה שמתקיים $\mu_\infty\left(\mathbb{Q}\left(\sqrt{-3}\right)\right)=\mu_4$ אם $d=-1$
3. נראה שמתקיים $\mu_\infty\left(\mathbb{Q}\left(\sqrt{d}\right)\right)=\mu_2$ לכל $d\notin\{-1,-3\}$
4. נראה ש־$e^{((2\pi i x)}$ $x\mapsto$ משרה איזומורפיזם $\mathbb{Q}/\mathbb{Z}\xrightarrow{\sim}\mu_\infty(\mathbb{C})$

הוכחה:
1. נשים לב שמתקיים

$$\mu_6=\{\zeta\mid \zeta^6=1\}=\left\{e^{\frac{2\pi i k}{6}}\mid 0\le k\le 5\right\}\underset{\omega=\frac{e^{2\pi i}}{3}}{=}\{1,\omega,\omega^2,-1,-\omega,-\omega^2\}$$

נשים לב שמתקיים $\mathbb{Q}(\omega)=\mathbb{Q}\left(\sqrt{-3}\right)$ שכן $\omega^2+\omega+1=0$, משמע כל השורשים שראינו ב־μ_6 נמצאים ב־$\mathbb{Q}\left(\sqrt{-3}\right)$.
2. מתקיים $i=\frac{e^{\pi i}}{2}$ ולכן $i^4=1$, ובגלל ש־$\mu_4=\{1,-1,i,-i\}$ נובע ישירות ש־$\mu_4\subset\mathbb{Q}(i)$ ולכן $\mu_4\subseteq\mu_\infty(\mathbb{Q}(i))$.
עבור ההכלה בכיוון השני, ניזכר ש־$[\mathbb{Q}(i):\mathbb{Q}]=2$ ולכן נבחן את כל הפולינומים הציקלוטומיים שדרגתם קטנה או שווה ל־2.
נשים לב שהחל מ־$n=7$ כל הפולינומים הציקלוטומיים הם מדרגה גדולה מ־6, ולכן מספיק שנסתכל על $n\in\{1,2,3,4,5,6\}$:

1. $\Phi_1(x)=x-1\Rightarrow \deg(\Phi_1(x))=1$
2. $\Phi_2(x)=x+1\Rightarrow \deg(\Phi_2(x))=1$
3. $\Phi_3(x)=x^2+x+1\Rightarrow \deg(\Phi_3(x))=2$
4. $\Phi_4(x)=x^2+1\Rightarrow \deg(\Phi_4(x))=2$
5. $\Phi_5(x)=x^4+x^3+x^2+x+1\Rightarrow \deg(\Phi_5(x))=4$
6. $\Phi_6(x)=x^2-x+1\Rightarrow \deg(\Phi_6(x))=2$

ולכן המועמדים היחידים שלנו הם $n\in\{1,2,3,4,6\}$.
אנחנו יודעים כבר ש־$\Phi_3(x),\Phi_6(x)$ לא אפשריים, כי כפי שראינו בתרגול במקרה זה מתקיים $\frac{\pm1\pm\sqrt{-3}}{2}\notin\mathbb{Q}(i)$, אבל ה־4 האחרים כן ב־$\mathbb{Q}(i)$

כי בדיוק $\{\pm 1, \pm i\}$ ולכן נקבל גם את ההכלה השנייה.
בסה"כ מצאנו כי $\mu_\infty(\mathbb{Q}(i)) = \mu_4$.

3. בהמשך לבדיקה מהסעיף הקודם, אנחנו כבר יודעים להגיד שלא ייתכן תחת ההנחה ש־$d \notin \{-1, -3\}$ ש־
$$\mu_\infty\left(\mathbb{Q}\left(\sqrt{d}\right)\right) = \mu_6 \vee \mu_\infty\left(\mathbb{Q}\left(\sqrt{d}\right)\right) = \mu_3 \vee \mu_\infty\left(\mathbb{Q}\left(\sqrt{d}\right)\right) = \mu_4$$
ובגלל ש־$2 \leq \left[\mathbb{Q}\left(\sqrt{d}\right) : \mathbb{Q}\right]$, נישאר רק עם $\mu_\infty\left(\mathbb{Q}\left(\sqrt{d}\right)\right) = \mu_2$ או $\mu_\infty\left(\mathbb{Q}\left(\sqrt{d}\right)\right) = \mu_1$.
אבל בבירור לא ייתכן ש־$\mu_\infty\left(\mathbb{Q}\left(\sqrt{d}\right)\right) = \mu_1$ שכן $\zeta = -1 \in \mathbb{Q} \subset \mathbb{Q}\left(\sqrt{d}\right)$ ולכן בסך־הכל נקבל $\mu_\infty\left(\mathbb{Q}\left(\sqrt{d}\right)\right) = \mu_2$.

4. נגדיר $\varphi : \mathbb{Q}/\mathbb{Z} \to \mu_{\infty(\mathbb{C})}$ על־ידי $\varphi(x + \mathbb{Z}) = e^{2\pi i x}$.
ראשית זה מוגדר היטב, כי אם $x \equiv y \bmod \mathbb{Z}$ אז
$$x - y \in \mathbb{Z} \Rightarrow e^{2\pi i x} = e^{2\pi i y} \cdot e^{2\pi i (x-y)} = e^{2\pi i y} \cdot 1 = e^{2\pi i y}$$
זה גם אכן הומומורפיזם
$$\varphi((x + \mathbb{Z}) + (y + \mathbb{Z})) = \varphi((x + y) + \mathbb{Z}) = e^{2\pi i (x+y)} = e^{2\pi i x} \cdot e^{2\pi i y} = \varphi(x + \mathbb{Z}) \cdot \varphi(y + \mathbb{Z})$$
הוא גם חד־חד ערכי כי הגרעין הוא טריוויאלי, שכן מתקיים
$$\varphi(x + \mathbb{Z}) = 1 \Longleftrightarrow e^{2\pi i x} = 1 \Longleftrightarrow x \in \mathbb{Z} \Rightarrow x + \mathbb{Z} = 0 + \mathbb{Z}$$
והוא גם אכן על, כי כל $\zeta \in \mu_\infty(\mathbb{C})$ הוא שורש יחידה, ולכן הוא מהצורה $\zeta = e^{2\pi i \frac{k}{n}}$ עבור n כלשהו, ולכן מספיק שנבחר $k \in \mathbb{Z}$ כך שמתקיים $\varphi\left(\frac{k}{n} + \mathbb{Z}\right) = \zeta$.

□

נתזכר כמה הגדרות ממבנים 1 בשביל הסדר, כי הנושאים הללו עלו בהרצאה ולא התעמקנו בהם:

הגדרה 17.5 (איבר פיתול): תהיי G חבורה. איבר $g \in G$ נקרא **איבר פיתול (torison)** אם הסדר של g סופי.

הגדרה 17.6 (חבורת־פיתול): **חבורת פיתול** היא חבורה שכל איבריה הם איברי פיתול.

הגדרה 17.7 (חסרת־פיתול): חבורה **חסרת־פיתול (torison free)** היא חבורה שכל איבריה, פרט ליחידה, אינם איברי פיתול.

דוגמה 17.6:
1. כל חבורה סופית היא חבורת פיתול
2. $\mathbb{Q}, \mathbb{Z}$ הן חבורות חסרות פיתול

למה 17.4: עבור A חבורת אבלית, קבוצת איברי הפיתול של A
$$A_{tor} = \{a \in A \mid \exists m \in \mathbb{N}_{\geq 1}\ s.t.\ ma = 0\}$$
היא תת־חבורה והמנה A/A_{tor} היא חסרת־פיתול.

הערה: לא רק שחבורת שורשי היחידה היא חבורה אבלית תחת הכפל, זו תת־חבורת פיתול של חבורת ספירת היחידה
$$\mathbb{S}^1 = \mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$$

הגדרה 17.8 ($H[p]$): עבור חבורה אבלית H נגדיר $H[p]$ כתת־החבורה של כל האיברים שסדרם הוא p
$$H[p] = \{h \in H \mid h^p = 1\}$$
אז H ציקלית אם ורק אם לכל $p \mid |H|$ יש p איברים ב־$H[p]$.
בעצם, $H[p]$ היא תת־חבורת פיתול.

למה 17.5: יהי K שדה ו־$G \leqslant K^\times$ עם n איברים. אזי G ציקלית ובעצם $G = \mu_n(K) = \mu_n$ ובפרט כל μ_n היא ציקלית.

הוכחה: אם p ראשוני כך ש־$p \mid n$ אזי $G[p] \subset \{x^p - 1 \in K$ שורשים של$\}$ ולכן יש לכל היותר p שורשים, ולכן G ציקלית (כי יש $\alpha \in G[p]$ שהסדר שלו לא מחלק את המעלה, ולכן הוא מסדר גדול יותר, משמע יוצר של $G[p]$). □

הערה: בכל שדה K ממציין $p > 0$, מתקיים $\mu_p(K) = 1$ כי לפולינום $x^{p^n} - 1 = (x-1)^{p^n}$ יש רק שורש אחד, $x = 1$.

למה 17.6: יהי K שדה ו־$n \geq 1$ כך ש־$\mu_n = \mu_n(K)$(דהיינו, $x^n - 1$ מתפצל לחלוטין ב־K) ויהי $m \in K^\times$ הגורם הגדול ביותר של n.
במילים אחרות:

1. אם $\mathrm{char}(K) = 0$ נבחר $n = m$
2. אם $\mathrm{char}(K) = p$ נבחר $n = p^l m$ כאשר $\gcd(m,p) = 1$

אז מתקיים $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mu_n$.

הוכחה: ל־$f = x^m - 1$ יש m שורשים ($m \in K^\times$) כי $f' = mx^{m-1}$ והשורשים הם רק 0 ול־$x^m - 1$ אנחנו יודעים ש־0 הוא לא שורש.
לכן $\gcd(f, f') = 1$ ולפי טענה שראינו נובע כי f פריד עם m שורשים, ולכן ל־μ_m יש m איברים.
אם $\mathrm{char}(K) = 0$ סיימנו ואם $\mathrm{char}(K) = p$ נבחר $\mu_n = \mu_m \oplus \mu_p^l = \mu_m$, שכן

$$\left(t^{p^l m} - 1\right) = \left(t^m - 1\right)^{p^l} \Rightarrow \mu_{p^l m} = \mu_m$$

□

18 הרצאה 11 – 06/05

18.1 שורשי יחידה – המשך

הגדרה 18.1 (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 $\zeta^m \neq 1$.

דוגמה 18.1: עבור $K = \mathbb{Q}$ ו־$2 \le n$ ראשוני, המספר $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ הוא שורש יחידה פרימיטיבי מסדר p ואז $L = \mathbb{Q}(\zeta)$ שדה הרחבה מעל $\mathbb{Q}$.
ראינו גם שהפולינום המינימלי של ζ מעל $\mathbb{Q}$ הוא

$$m_\zeta = x^{p-1} + x^{p-2} + \dots + x + 1$$

מסקנה 18.1: אם K שדה סגור אלגברית ו־$n \ge 1$ אז שורש פרימיטיבי של יחידה מסדר n קיים ב־K אם ורק אם n הוא הפיך ב־K משמע אם ורק אם $n \in K^\times$.

תרגיל 18.1: נניח כי K סגור אלגברית ונראה שמתקיימים
1. אם $\mathrm{char}(K) = 0$ אז $\mu_\infty(K) \backsimeq \mathbb{Q}/\mathbb{Z}$
2. אם $\mathrm{char}(K) = p > 0$ אז $\mu_\infty(K) \backsimeq \mathbb{Q}/\mathbb{Z}\left[\frac{1}{p}\right]$

הוכחה:
1. K סגור אלגברית ולכן מכיל את כל שורשי היחידה ζ_n לכל n. כל $\frac{a}{n} \in \mathbb{Q}/\mathbb{Z}$ הוא מסדר סופי ולכן $\mathbb{Q}/\mathbb{Z}$ היא חבורת פיתול עם "עותק" לכל $\mathbb{Z}/n\mathbb{Z}$ לכל $n \ge 1$, וזה בידיוק $\mu_\infty(K)$: אם נסתכל על האיזומורפיזם שהגדרנו בתרגיל הקודם, ונחדד אותו להיות $\varphi : \mathbb{Q}/\mathbb{Z} \to \mu_\infty(K)$ הנתון על־ידי $\varphi\left(\frac{a}{n} + \mathbb{Z}\right) = e^{\frac{2\pi i a}{n}} \in \mu_n(K)$, זה מגדיר באמת איזומורפיזם כמו שראינו.
2. יהי $\zeta \in K$ שורש יחידה מסדר p^n, משמע $\zeta^{p^n} = 1$ ולכן ζ הוא שורש של $x^{p^n} - 1$, אבל $\left(x^{p^n} - 1\right)' = 0$ כי $\mathrm{char}(K) = p$ ולכן $\gcd\left(x^{p^n} - 1, \left(x^{p^n} - 1\right)'\right) = 1$ ולכן זהו פולינום פריד.

מנגד, כל השורשי יחידה במציין p חייבים להיות מסדר זר ל־p, ולכן

$$\mu_\infty(K) = \bigcup_{\substack{n \ge 1, \\ \gcd(n,p)=1}} \mu_n(K)$$

אבל זה בידיוק אומר ש־$\mu_{\infty(K)} \backsimeq \mathbb{Q}/\mathbb{Z}\left[\frac{1}{p}\right]$, שכן כל $x \in \mathbb{Q}/\mathbb{Z}$ הוא מהצורה $x = \frac{a}{n} + \mathbb{Z}$, ואם $p \mid n$ אז $\zeta_n \notin K$, ולכן נשאר רק עם n־ים שעבורם $\gcd(n,p) = 1$, משמע

$$\mu_\infty(K) \backsimeq \biguplus_{\substack{n \ge 1, \\ \gcd(n,p)=1}} \mathbb{Z}/n\mathbb{Z} \backsimeq \mathbb{Q}/\mathbb{Z}\left[\frac{1}{p}\right]$$

□

הערה: מיכאל אמר שהאיזומורפיזמים הללו הם לא יחידים ולא קנונים, כי הם "לא טבעיים" – הם תלויים בבחירה של K ו־$\zeta_n \in K$ ומצריך לקבע שורשי יחידה פרימיטיביים בצורה ספציפית לכל n.

18.2 שדות סופיים

פרק 6.2 ברשומות של מיכאל.
אנחנו אוהבים שדות סופיים כי בשדה סופי כל האיברים הם שורשי יחידה.

למה 18.1 (אנדומורפיזם פרובניוס): נניח ש־K שדה עם $\mathrm{char}(K) = p > 0$.
נגדיר $\mathrm{Fr}(x) = x^p$ וזהו אנדומורפיזם (הומומורפיזם $\mathrm{Fr} : K \to K$) הנקרא **אנדומורפיזם פרובניוס**.
עבור שדות סופיים עם $\mathrm{char}(K) = p$ ראשוני, זה Fr הוא אוטומורפיזם.
את התמונה של Fr^n נסמן ב־K^{p^n}.

הוכחה:
1. $$\mathrm{Fr}(ab) = (ab)^p = a^p b^p = \mathrm{Fr}(a)\,\mathrm{Fr}(b)$$
2. מנוסחת הבינום של ניוטון

$$\mathrm{Fr}(a+b)=(a+b)^p=\sum_{i=0}^{p}\binom{p}{i}a^ib^{p-i}=a^p+b^p=\mathrm{Fr}(a)+\mathrm{Fr}(b)$$

3. בגלל שאנחנו בתחום שלמות ואין מחלקי אפס, זה גם חד־חד ערכי שכן $\mathrm{Fr}(a)=a^p=0\iff a=0$

$\square$

הערה: את הלמה לעיל לא ראינו בהרצאה אבל מיכאל הזכיר אותה, 3.1.12 ברשומות של מיכאל.

משפט 18.1: לכל ראשוני $p\in\mathbb{N}$ ו־$q=p^n$ עבור $n\geq 1$, קיים שדה $\mathbb{F}_q$ עם q איברים והוא יחיד עד־כדי איזומורפיזם (שאינו יחיד).
בפרט, כל שדה סופי הוא איזומורפי ל־$\mathbb{F}_q$ כאשר q חזקה של ראשוני.

הוכחה: ניקח $\mathbb{F}_p$ ונגדיר הרחבה K כשדה פיצול של $t^{q-1}-1$ שכן השורשים שלו הם בדיוק $\mathbb{F}_q\setminus\{0\}=\mu_q$.
נראה שבתוך K יש q איברים – ניקח את כל ה־x־ים כך ש־$x^q=0$ וזה בעצם $\mathrm{Fr}^{q(x)}=x$.
נטען שכל האיברים שלקחנו הוא מהווים שדה: $\mathrm{Fr}^q(x)=x$ וגם $\mathrm{Fr}^q(y)=y$ ולכן $\mathrm{Fr}^q(x+y)=x+y$ ובאותו אופן נקבל גם כפל.
לכן נקבל $K\supset\mathbb{F}_q=\{x\mid x^q=x\}$ ובדיעבד $K=\mathbb{F}_q$.
הערה: כל הפתרונות שונים שכן $(x^q-x)'=1$ והפולינום שלנו פריד (פולינום הוא פריד אם ורק אם $\gcd(f,f')=1$).
מכאן, $\mathbb{F}_q$ יחיד עד־כדי איזומורפיזם כי הוא שדה פיצול של t^q-t מעל $\mathbb{F}_q$.
לבסוף אם $\mathbb{F}$ שדה סופי אזי F מכיל את $\mathbb{F}_p$ כאשר $\mathrm{char}\,F=p$ (ראינו בהרצאה 1) ולכן $F\approx\mathbb{F}_p^n$ כמרחב וקטורי מעל $\mathbb{F}_p$ ולכן $|F|=p^n$ ולכן $F\approx\mathbb{F}_{p^n}=\mathbb{F}_q$. $\square$

תרגיל 18.2:
1. $\mathbb{F}_9=\mathbb{F}_3(i)$
2. $\mathbb{F}_4=\mathbb{F}_2(\alpha)$ כאשר $\alpha\alpha^2+\alpha+1=0$ (זה שוב האוטומורפיזם $\alpha\mapsto\alpha+1$).

הוכחה: TODOOOOOOOOOOOOOOOOOOOO $\square$

מסקנה 18.2: אם $\mathbb{F}_q$ שדה סופי אז לכל $n\geq 1$ יש בדיוק הרחבה אחת $K/\mathbb{F}_q$ מדרגה n והיא יחידה עד־כדי איזומורפיזם ובנוסף הרחבה זו היא פרימיטיבית (קיים α כך ש־ $\mathbb{F}_q[\alpha]=\mathbb{F}_{q^n}$ כאשר α פריד).

הוכחה: מהמשפט לעיל קיימת ויחידה ההרחבה $\mathbb{F}_{q^n}/\mathbb{F}_q$, וההרחבה נוצרת על־ידי α שהוא יוצר של $\mathbb{F}_{q^n}^{\times}$.
מתקיים גם $f=t^{q^n}-t\mid f_{\alpha/\mathbb{F}_q}$, אבל f הוא פריד כי $f'=-1$ ולכן $f_{\alpha/\mathbb{F}_q}$ הוא פריד ו־$\deg\left(f_{\alpha/\mathbb{F}_q}\right)=n$. $\square$

מסקנה 18.3: נניח $\mathbb{F}_q,\mathbb{F}_r$ שדות סופיים. הבאים שקולים:
1. קיים שיכון $\mathbb{F}_q\hookrightarrow\mathbb{F}_r$
2. $r=q^d$ עבור $d\in\mathbb{N}$
3. $r=p^n$ ו־$q=p^m$ עבור $m\mid n$

הוכחה: $3\iff 2$ ברור.
$2\Longrightarrow 1$ אם $\phi:\mathbb{F}_q\hookrightarrow\mathbb{F}_r$ קיים, אז $\left(\mathbb{F}_q\right)^d\xrightarrow{\sim}\mathbb{F}_r$ כמרחב וקטור כאשר $d=\left[\mathbb{F}_r:\mathbb{F}_q\right]$ ולכן $r=q^d$.
$1\Longrightarrow 2$ נניח כי $r=q^d$ משמע שתי ההרחבות הן הרחבות שדה השדה הראשוני $\mathbb{F}_p$. אבל $q-1\mid r-1=q^d-1$ ולכן $x^{q-1}-1\mid x^{r-1}-1$ ואז שדה הפיצול של $\mathbb{F}_r$ של x^r-x מכיל את שדה הפיצול $\mathbb{F}_q$ של x^q-x ומהיחידות סיימנו. $\square$

משפט 18.2: נניח ש־$\mathbb{F}_{q^d}/\mathbb{F}_q$ הרחבת שדות סופית מדרגה d אז $\mathrm{Aut}_{\mathbb{F}_q}\left(\mathbb{F}_{q^d}\right)$ היא ציקלית עם d איברים ויוצר Fr_q.
(זאת אומרת $\mathrm{Fr}_q=\left(\mathrm{Fr}_q\right)^n=x^q=\mathrm{Fr}_q(x),q=p^n$)

הערה: $\mathrm{Aut}_{\mathbb{F}_q}\left(\mathbb{F}_{q^d}\right)\simeq\mathbb{Z}/d\mathbb{Z}=\left\{1,\mathrm{Fr}_q,...,\mathrm{Fr}_{q^{d-1}}\right\}$

הוכחה: $\mathbb{F}_{q^d}=\mathbb{F}_q(\alpha)$ עבור α פריד מדרגה d $\left(\deg\left(f_{\alpha/\mathbb{F}_q}\right)=d\right)$ ולכן $d=|C_\alpha|$ ו־$\left|\hom_{\mathbb{F}_q}\left(\mathbb{F}_q(\alpha),\mathbb{F}_q(\alpha)\right)\right|=1$, שכן σ נקבעת ביחידות על־ידי $\sigma(\alpha)\in C_\alpha$.
נותר להוכיח שהיא ציקלית ולתאר אותה: כל Fr_q^i עבור $0\leq i\leq d-1$ הוא הזהות על $\mathbb{F}_q$ ואינו הזהות על $\mathbb{F}_{q^d}$ שכן $\left\{x\mid\mathrm{Fr}_q^i(x)=x\right\}=$ $\left\{x\mid x^{q^i}=x\right\}$ ויש בדיוק $q^i<q^d$ איברים כאלו.
משמע $\left\{1,\mathrm{Fr}_q,...,\mathrm{Fr}_{q^{d-1}}\right\}=\mathrm{Aut}_{\mathbb{F}_q}\left(\mathbb{F}_{q^d}\right)\to\left\{x\mid\mathrm{Fr}_q^i(x)=x\right\}$ כאשר 1 הוא זהות ו־Fr_q הוא יוצר. $\square$

הוכחה טיפה שונה מהרשומות של מיכאל: מהמסקנה שראינו לעיל, ההרחבה היא פרימיטיבית ולכן $G=\mathrm{Aut}_{\mathbb{F}_q}\left(\mathbb{F}_{q^d}\right)$ וממסקנה שראינו נובע כי היא מדרגה של לכל היותר d (TODOOOOOOOOOOOOOOOOOOOO לקשר למסקנה).
כל $a\in\mathbb{F}_q$ מקיים $\mathrm{Fr}_q(a)=a^q=a$ ולכן Fr הוא איבר של G.
מאותה סיבה, $\left(\mathrm{Fr}_q\right)^d=1\in G$ וגם $\left(\mathrm{Fr}_q\right)^i\neq 1$ לכל $i<d$ שכן $\left(\mathrm{Fr}_q\right)^i$ מקבע לכל היותר q^i איברים.
לכן Fr_q יוצרת את תת־חבורה ציקלית H מסדר d ומכיוון ש־$|G|\leq d$ נובע כי $H=G$. $\square$

הערה: $\overline{\mathbb{F}_p} = \bigcup_{n\geq 1}\mathbb{F}_{p^n}$ הוא יחיד עד־כדי $\mathrm{Aut}_{\mathbb{F}_p}\left(\overline{\mathbb{F}_p}\right)$ כי אנחנו צריכים לבחור איך לשכן את התתי־שדות.
נראה ונוכיח בהמשך שבעצם מתקיים $\mathrm{Aut}_{\mathbb{F}_p}\left(\overline{\mathbb{F}_p}\right) = \mathrm{Fr}_q^{\hat{\mathbb{Z}}}$.

19 תרגול 5 – 07/05

19.1 משהו

20 תרגיל 4

20.1 טריקים

20.2 מסקנות