מבנים אלגבריים 2, 80446 — סיכום

2 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־$a \in R^x$ או $b \in R^x$ (משמע $r \sim a$ או $r \sim b$).

הגדרה 1.3 (K־הומומורפיזם): 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

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

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 $\underbrace{f_0 \cdot g_0}_{\text{פרימיטיביים}}$ $f \cdot g = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$ 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 מפרושות:

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

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 בסיכום של מיכאל).

הוכחה: נשים לב ש־$\mathbb{Z}[t]^x = \mathbb{Z}^x$ ולכן $p \notin \mathbb{Z}^x$ 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 $0 \neq c \in \mathbb{Q}^x$ 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־$\mathbb{Z}[t]$
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 $m, n \in \mathbb{Z}$ $0 <$ 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 $\frac{1}{\ell} \cdot f = \frac{m \cdot n \cdot f}{m \cdot n \cdot \ell} = \underbrace{\frac{m}{\alpha} \cdot g \cdot \frac{n}{\beta} \cdot h}_{\in \mathbb{Z}[t]}$ 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 כך ש־$c \cdot g \cdot c^{-1} \cdot h \in \mathbb{Z}[t]$ כך 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 $\deg\left(\frac{f}{\mathrm{cont}(f)}\right) > 0$ 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 $\deg(g) > 0, \deg(h) = 0$ 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

10 משהו

11 תרגיל 2

11.1 טריקים

11.2 מסקנות

12 הרצאה 6 – 21/04

12.1 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 12.1: 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. $\square$

תרגיל 12.1: $\mathbb{F}_p[t] = \mathbb{Z}[t]/p\mathbb{Z}[t]$

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

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

$\square$

משפט 12.1 (קריטריון אייזנשטיין (Eisenstein's criterion)): 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 $0 \le i < n$
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 הגבת הכללית, 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־$p \mid b_i$ 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־$\mathbb{Q}[t]$. $\square$

דוגמה 12.1: 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 12.1: $x^2 - m^2, x^2 + 4$ תמיד פריקים: אם $p \mid m^2$ אז גם $p \mid m$.

הגדרה 12.1 (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 12.2:

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

עבור $p \in \mathbb{N}$ ראשוני, אז כל הפולינום הציקלוטומי מסדר p^n הוא $\frac{x^{p^n} - 1}{x^{p^{n-1}} - 1} \in \mathbb{Q}[x]$.

למה 12.2: 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

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

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 12.2 (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 12.3 (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. □

12.2 סגור אלגברי

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

הגדרה 12.2 (שדה סגור אלגברי): שדה K נקרא **שדה סגור אלגברית** אם לכל פולינום לא קבוע מעל K יש שורש ב־K.

הגדרה 12.3 (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 $c\in K^x$ ו־$a_i\in K$ לכל i.

למה 12.3: 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.

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

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

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

$(1)\Longrightarrow(4)$: 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 12.2 (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 12.1:

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 $\mathrm{dic}<0$ (דיסקרמיננטה)

הוכחה: נשים לב $2\iff 1$ ברור, ולכן מספיק שנוכיח רק את 1: נשים לב $f=\overline{f}=\mathbb{R}[t]\subseteq\mathbb{C}[t]$ 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 מבנינו 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־$\overline{f}=f$. בשל סגירות זו, גם בפירוק לגורמים לינאריים 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 $1 \leq i \leq n$ או ש־$a_i \in \mathbb{R}$ או ש־$a_i \in \mathbb{C}$ וכן $\overline{a_i} \in \{a_i \mid 0 \leq i \leq n\}$.
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 12.2: 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 12.3:

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. $\overline{\mathbb{Q}} = \overline{\mathbb{Q}\left(\sqrt[3]{2} + \sqrt[3]{5}\right)}$

13 הרצאה 7 – 22/04

13.1 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 13.1 (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 13.1: נניח כי K שדה ו־L/K הרחבה אלגברית, $\kappa = |K|$. אזי $|L| \le \max\{\kappa, \aleph_0\}$.
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

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

□

משפט 13.1 (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 $+_K |_K +_L, \cdot_K = \cdot_L |_K$.
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 $b \; a +_L b = a +_{L_i}$ 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 13.2 (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: $(F_1, \phi_1) \le (F_2, \phi_2)$ אם $F_1 \subseteq F_2$ ו־$\phi_2 |_{L_1} = \varphi_1$, 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 $\phi_i \; \phi |_{L_i}$ 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 $f_{\alpha/F} \mid f_{\alpha/K}$ (מההנחה שהפולינום המינימלי לכל $\alpha \in S$ מתפצל לחלוטין מעל E) ולכן בפרט $f_{\phi(\alpha)/F} \mid f_{\phi(\alpha)/K} \iff \phi\left(f_{\alpha/F}\right) \mid \phi\left(f_{\alpha/K}\right)$ 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.

14 תרגול 4 – 23/04

14.1 שדות פיצול

הגדרה 14.1 (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 14.1: 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 14.1: מה הם כל השדות K כך שמתקיים $\mathbb{Q} \subseteq K \subseteq L$?

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

15 הרצאה 8 – 28/04

15.1 קיום ויחידות סגור אלגברי – המשך

למה 15.1 (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: $\square$

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

16 הרצאה 9 – 29/04

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

16.2 הרחבות נורמליות ושדות פיצול

17 תרגיל 3

17.1 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 (ככל הנראה המקרים בהם $a_n=1$)

17.2 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

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