מבנים אלגבריים 2, 80446 — סיכום

8 ביולי 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* $r \sim a$ או $r \sim b$, במבנים1 קראנו לזה יחס **חברות**).

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

הוכחה: אפשר לראות זאת מכלים של לינארית ישירות, או מהעובדה שהומומורפיזם של שדות הוא בפרט הומומורפיזם של חוגים, ולכן הגרעין שלו הוא אידיאל, אבל האידיאלים היחידים בשדה הם אידיאל האפס (הטריוויאלי) או כל השדה. □

1.2 בניות

הגדרה 1.3 (שדה מנות): R תחום שלמות, נגדיר **שדה מנות**

$$\mathrm{Frac}(R) = \left\{\frac{s}{r}\right\} \mid s, r \in R, r \neq 0\}/\sim$$

כאשר $\sim$ הוא יחס שקילות המקיים $\frac{s_1}{r_1} \sim \frac{s_2}{r_2} \iff s_1 r_2 = s_2 r_1$.

למה 1.1: לכל שיכון $R \hookrightarrow K$ כאשר K שדה, קיים ויחיד פיקטור $R \subset \mathrm{Frac}(R) \hookrightarrow K$.

הגדרה 1.4 (שדה פונקציות רציונליות): אם K שדה ו־S קבוצת משתנים (בדרך־כלל סופית אך אפשר גם אינסופית), נגדיר

$$K(S) \coloneqq \mathrm{Frac}(K[S])$$

זה **שדה פונקציות רציונליות מעל K במשתנים של S**.

הערה: $\mathrm{Frac}(K(S)) = \left\{\frac{P}{Q} \mid P, Q \in K[S], Q \neq 0\right\}$, כאשר Frac זהו השדה הקטן ביותר שמכיל את $K[S]$.

תרגיל 1.1: מתקיים $K(y)(x) = K(x)(y)$.

הוכחה: $K[x, y] = K[y, x]$ ולכן $\mathrm{Frac}(K[x, y]) = K(x, y) = K(y, x) = K(x)(y) = K(y)(x)$. □

טענה 1.1 (תזכורת: תנאים שקולים לבניית שדות ממנה):

1. אם R חוג ו־M אידיאל מקסימלי אז $K = R/M$ הוא שדה
2. אם K שדה ו־$f(t)$ פולינום אי־פריק מעליו אזי $K[t]/(f(t))$ הוא שדה

הערה: מהלמה של צורן נובע כי בכל חוג יש אידיאל מקסימלי.

דוגמה 1.3:

1. $\mathbb{C} = \mathbb{R}[t]/(t^2+1)$ (במילים אחרות, הוספנו t וחייבנו $t = i$ $t^2 + 1 = 0 \Rightarrow$)
2. $\mathbb{Q}\left(\sqrt{2}\right) = \mathbb{Q}(t)/(t^2 - 2)$
3. $\mathbb{Q}\left(\sqrt[3]{3}\right) = \mathbb{Q}(t)/(t^3 - 3)$

תרגיל 1.2:
1. $\mathbb{F}_3(t)/(t^2+1)=\mathbb{F}_9=\mathbb{F}_3\left[\sqrt{-1}\right]$
2. $\mathbb{F}_2(t)/(t^2+t+1)=\mathbb{F}_4(\mathbb{F}_4\neq\mathbb{Z}/4\mathbb{Z})$

הוכחה:
1. נשים לב שב־$\mathbb{F}_3$, אם נסתכל על הפולינום t^2+1 אז מתקיים $t^2=-1 \iff t^2+1=0$ אבל $-1\equiv 2(\bmod 3)$ ולכן $t^2=2$, ולפולינום t^2+1 אין שורשים ב־$\mathbb{F}_3$ (פשוט להציב $t\in\{1,2,3\}$).
כעת, $\mathbb{F}_3(t)/(t^2+1)$ מכיל את האיברים מהצורה $a+bt$ עבור $a,b\in\mathbb{F}_3$, קומבינטורית יש לנו $3\times 3=9$ אפשרויות לסכומים שונים, ואנחנו כבר יודעים מלינארית שזה גם הגודל של השדה $\mathbb{F}_9$ ועל־כן הם שקולים.
המקרה של $F_3(t)/(t^2+1)=\mathbb{F}_3\left[\sqrt{-1}\right]$ ברור מכך ש־$t^2=-1$.
2. על אותו רעיון כמו המקרה הקודם.

□

1.3 שדות ראשוניים

הגדרה 1.5 (שדה ראשוני): נגיד ששדה הוא **שדה ראשוני** אם הוא מהרשימה $\mathbb{Q},\mathbb{F}_2,\mathbb{F}_3,\cdots,\mathbb{F}_p$ כאשר p ראשוני בלבד.

למה 1.2: לכל שדה K קיים ויחיד תת־שדה ראשוני $K_0\subseteq K$ ובפרט שדות ראשוניים הם מנימליים ביחס להכלה.

הוכחה: נשים לב כי לכל חוג R קיים ויחיד הומומורפיזם $\mathbb{Z}\to R$ (כי $1_{\mathbb{Z}}\mapsto 1_R$ מהגדרת הומומורפיזם של חוגים).
בפרט, יש הומומורפיזם יחיד $\varphi:\mathbb{Z}\to K$ ו־$\mathbb{Z}\to\mathbb{Z}/\ker(\varphi)\subset R$, שכן $\mathbb{Z}$ תחום אוקלידי וולכן תחום ראשי ואז $\ker(\varphi)=(n)$ ונחלק למקרים:
1. $n=0$ אזי $\mathbb{Z}\hookrightarrow R$ ולכן גם $\mathrm{Frac}(\mathbb{Z})=\mathbb{Q}\hookrightarrow R$
2. אם $n\neq 0$ אז $n=p$ ראשוני כי $\mathbb{Z}/p\mathbb{Z}\subset R$ תחום וזה אומר ש־$\mathbb{F}_p=\mathbb{Z}/p\hookrightarrow K$

כמובן, אף $\mathbb{F}_p$ או $\mathbb{Q}$ לא מכיל שדה אחר מהרשימה ואי־אפשר לשכן אחד בשני. □

הגדרה 1.6 (המציין): **המציין** של שדה K הוא
1. $\mathrm{char}(K)=0$ אם $\mathbb{Q}\subseteq K$
2. $\mathrm{char}(K)=p$ אם $\mathbb{F}_p\subseteq K$

הגדרה 1.7 (הגדרה אלטרנטיבית למציין): $\mathrm{char}(K)$ הוא המספר החיובי p הקטן ביותר כך ש־$p\in K=0$ ו־$\mathrm{char}(K)=0$ אם לא קיים כזה.

הערה: מהלמה שראינו $\ker(\mathbb{Z}\to K)=(\mathrm{char}(K))$.

הערה (אזהרה): בשדה ממציין p הדבר **הכי** חשוב לעשות זה **לא** לחלק ב־p.

למה 1.3: אם $\varphi:K\to R$ הומומורפיזם של חוגים, K שדה ו־$R\neq 0$ אזי φ חד־חד ערכית.

הוכחה: $I=\ker(\varphi)\subseteq K$ אידיאל.
אם $I=0$ אז φ חד־חד ערכית וסיימנו, או שמתקיים $I=R$ ואז $1=0$ ולכן $R=0$ וזו סתירה. □

הגדרה 1.8 (אנדומורפיזם, אוטומורפיזם): הומומורפיזם $\varphi:K\to K$ נקרא **אנדומורפיזם** ומסומן $\mathbf{End}(K)$.
אם φ הפיך אז φ נקרא **אוטומורפיזם** ומסומן ב־ $\mathbf{Aut}(K)$ (שזו כמובן חבורה)

דוגמה 1.4: נניח ש־$\mathrm{char}(K)=p\neq 0$, אזי $\mathrm{Fr}(x)=x^p$ מגדיר אנדומורפיזם שנקרא לו **פרובניוס** מ־K לעצמו (עוד נתעסק בו בהמשך).

הוכחה: אכן $0\mapsto 0, 1\mapsto 1$ ו־$(xy)^p=x^py^p$ ובחיבור נשתמש בנוסחת הבינום $(x+y)^p=\sum_{i=0}^{p}\binom{p}{i}x^iy^{p-i}$ ונשים לב ש־$\binom{p}{i}$ מתחלק ב־p כמספר שלם כאשר $i\notin\{0,p\}$ ואז $(x+y)^p=x^p+y^p$ בכל שדה שבנו $p=0$. □

דוגמה 1.5: ב־$\mathbb{F}_3$ מתקיים $(x+y)^3=x^3+3x^2y+3xy^2+y^3$

תרגיל 1.3: אם $\mathbb{F}$ שדה סופי עם $\mathrm{char}(\mathbb{F})=p$ אז $\mathrm{Fr}_{\mathbb{F}}\in\mathrm{Aut}(\mathbb{F})$.

הוכחה: היות ו־$\mathbb{F}_r$ הוא חד־חד־ערכי (העתקה מתוך שדה), והשדה הוא סופי אז בהכרח הוא על, ולכן אוטומורפיזם. □

דוגמה 1.6: $\mathbb{F}_p(t)\xrightarrow{\mathrm{Fr}}\mathbb{F}_p(t)$ לא הפיכה כי אין $t=p$.

2 הרצאה 2 – 25/03

2.1 הרחבת שדות

פרק 3 ברשומות של מיכאל.

הגדרה 2.1 (הרחבת שדות): אם L שדה ו־$K \subseteq L$ הוא תת־שדה (קבוצה סגורה לפעולות) אז אומרים ש־L/K היא **הרחבת שדות**.

הערה: בדרך־כלל, נרצה להתחיל מ־K ולבנות הרחבות אבל כמעט תמיד אנחנו בונים שיכון שדות $L \hookrightarrow K$ במקום, אבל בפועל מהשיכון $\varphi : K \to L$ אפשר לבנות הרחבה על־ידי החלפה של $\varphi(K)$ ב־K.

הגדרה 2.2 (K־הומומורפיזם בין שדות): אם $L/K, F/K$ שתי הרחבות של K אזי **K־הומומורפיזם** מ־F ל־L זה הומומורפיזם $\varphi : F \to L$ כך שמתקיים $\varphi|_K = \mathrm{Id}$.

סימון: L/K הרחבת שדות, נסמן את חבורת כל K־אוטומורפיזמים של L ב־$\mathrm{Aut}_K(L)$ או ב־$\mathrm{Aut}(L/K)$

דוגמה 2.1:

1. $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \mathbb{Z}/2\mathbb{Z}$ (כי שורשים של פולינום הולכים בינם לבין עצמם)
2. $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$ הוא ענק ולא נחמד
3. $\mathrm{Aut}_{\mathbb{C}}(\mathbb{C}) = 1$
4. $\mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}\left(\sqrt{2}\right)\right) = \mathbb{Z}/2\mathbb{Z}$ עם ההצמדה $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ והזהות

2.2 יוצרים של הרחבות

הגדרה 2.3 (K[S], K(S)): נניח ש־L/K הרחבת שדות $(K \subseteq L)$ ו־$S \subseteq L$ תת־קבוצה, אז

1. $K[S]$ **תת־חוג** של L שמכיל את K ו־S והוא הקטן ביותר
2. $K(S)$ **תת־השדה** הקטן ביותר המכיל את K ואת S

הערה: הם קיימים ושווים לחיתוך של כל תתי־חוגים / שדות המכילים את שניהם (כמו ש־Span של מרחב וקטורי קיים).

למה 2.1: בהינתן הרחבת שדות L/K, יהיו $S \subseteq L$ ו־L $\varphi : K[x_s]_{s\in S} \to L$ הומומורפיזם שהוא הזהות על K ו־$x_s \mapsto s \in S \subseteq L$, אז מתקיים

1. $K[S] = \left\{f(s) \mid f \in K[x_s]_{s\in S}\right\}$
2. $K(S) = \mathrm{Frac}(K[S]) = \left\{\frac{f(S)}{g(S)} \mid f(x), g(x) \in K[x_s]_{s\in S}, g(S) \neq 0\right\}$

הוכחה: להשלים, למה 3.1.23 אצל מיכאל. $\square$

הערה: בדרך־כלל אין הומומורפיזם $K(X_s)_{s\in S} \to L$ כי עלולים לקבל "∞" (לחלק ב־0).

הגדרה 2.4 (הרחבה נוצרת סופית): הרחבה L/K נקראת **נוצרת סופית** אם קיים $S = \{\alpha_1, \cdots, \alpha_n\} \subseteq L$ סופית כך שמתקיים $K[S] = L$.

דוגמה 2.2: $\mathbb{C} = \mathbb{R} + i\mathbb{R}$ ו־$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$ ואפילו $\mathbb{C}/\mathbb{R}$ מרחב וקטורי נוצר סופית.
$\mathbb{C}(t)/\mathbb{C}$ נוצר סופית כשדה אבל לא נוצר סופית כחוג (דורש הוכחה) ואפילו $\mathbb{C}[t]/\mathbb{C}$ לא נוצר סופית כפולינומים.

הגדרה 2.5 (דרגת הרחבה): אם L/K הרחבת שדות, אז **הדרגה של ההרחבה** שנסמנה $[\boldsymbol{L} : \boldsymbol{K}]$ שווה למימד של L כמרחב וקטורי מעל K ולכן $\dim_K L = [L : K]$.

דוגמה 2.3:

1. $\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 2$ (כמו ש־$[\mathbb{C} : \mathbb{R}] = 2$)
2. נראה בהמשך שמתקיים $\left[\mathbb{Q}\left(\sqrt[3]{2} : \mathbb{Q}\right)\right] = 3$
3. $[K(t) : K] = \infty$

הגדרה 2.6 (הרחבת שדות סופית): הרחבה L/K נקראת **הרחבה סופית** אם $[L : K] < \infty$.

מוסכמה: $\infty \cdot n = \infty, \infty \cdot \infty = \infty$

למה 2.2 (כפליות הדרגה): אם $F/L/K$ הוא מגדל של הרחבות שדות אזי מתקיים

$$[F:K]=[F:L]\cdot[L:K]$$

ובפרט, F/K הרחבה סופית אם ורק אם $L/K, F/K$ הרחבות סופיות.

הוכחה: אם $F/L, L/K$ לא הרחבות סופיות בבירור גם F/K לא הרחבה סופית.

אם F/K סופי, אז הבסיס של F/K הוא גם בסיס מעל L ולכן F/L סופי ו־L תת־מרחב וקטורי ב־F ולכן גם הוא נוצר סופית מעל K.

נשאר להראות שאם $F/L, L/K$ הרחבות סופיות אז השיוויון ממתקיים. נראה זאת באמצעות בניית בסיס:

נניח שמתקיים $[L:K]=n, [F:L]=m$ ונבחר בסיסים $\alpha_1, \cdots, \alpha_n$ בסיס של L/K ו־$\beta_1, \cdots, \beta_m$ בסיס של F/L, נוכיח ש־$\gamma_{ij}=\alpha_i\beta_j$ מהווה בסיס של F/K, עלינו להראות שפורש ובלתי־תלוי לינארית:

כל $c\in F$ ניתן לייצוג על־ידי $c=\sum_{j=1}^m b_j\beta_j$ עם $b_j\in L$, אז $b_j=\sum_{i=1}^n a_{ij}\alpha_i$ עם $a_{ij}\in K$, אז

$$c=\sum_{j=1}^m\left(\sum_{i=1}^n a_{ij}\alpha_i\right)\beta_j=\sum_{i,j}a_{ij}\gamma_{ij}$$

ולכן γ_{ij} פורש את F/K.

אם נניח ש־$a_{ij}\in K$ כך שמתקיים $\sum_{i,j}a_{ij}\gamma_{ij}=0$, אז

$$0=\sum_{i,j}a_{ij}\alpha_i\beta_j=\sum_{j=1}^m\left(\sum_{i=1}^n a_{ij}\alpha_i\right)\beta_j$$

אבל β_j בלתי־תלויים לינארית מעל L אז $\sum_i a_{ij}\alpha_i\in L$ הם כולם אפסים, אבל α_i בלתי־תלויים לינארית מעל K, אז a_{ij} הוא הביטוי שנעלם ולכן γ_{ij} הם בלתי־תלויים לינארית מעל K ולכן זה מהווה בסיס מעל F. $\square$

3 תרגול 1 – 26/03

3.1 חוג הפולינומים – תזכורת

3.2 בניית שדות בעזרת מנות של חוגי פולינומים

3.3 חישוב בשדה $E = F[x]/(f)$

להשלים

4 תרגיל 1

4.1 טריקים

להשלים

4.2 מסקנות

להשלים

5 הרצאה 3 – 31/03

5.1 הרחבות אלגבריות

פרק 3.2 ברשומות של מיכאל.

הגדרה 5.1 (איבר אלגברי, איבר טרנסצנדנטי): בהינתן הרחבה L/K ו־$\alpha \in L$, נגיד ש־α **אלגברי** מעל K אם קיים $f(t) \in K[t]$ כך שמתקיים $f(\alpha) = 0$, אחרת נגיד ש־α נקרא **טרנסצנדנטי** מעל K.
אם $\mathrm{char}(L) = 0$ אז $\alpha \in L$ אלגברי או טרנסנצנדטי אם הוא אלגברי או טרנסצנדנטי מעל $\mathbb{Q}$.

דוגמה 5.1: אלגבריים ב־$\mathbb{C}$: $\frac{1}{778}, \sqrt[3]{5}, \sqrt[5]{3} + \sqrt[3]{5}$ ובהמשך נוכיח שגם i.
טרנסצנדנטי ב־$\mathbb{C}$: e, π (עובדה מעניינת: לא ידוע אפילו אם $\pi + e$ הוא טרנסצנדנטי או אלגברי, כי- זה מספר אי־רציונלי).
נשים לב ש־e אלגברי מעל $\mathbb{C}$ ו־$\mathbb{R}$ ואפילו מעל $\mathbb{Q}(e), \mathbb{Q}(e^5 + e)$ (ברור שלהיות איבר אלגברי או טרנסצנדנטי תלוי בשדה שאני עליו).
הרעיון הכללי הוא שאם יש ל־α קירובים רציונליים "טובים מדי" אז α טרנסצנדנטי – כמו לדוגמה מספר ליוביל.

הגדרה 5.2 ($\overline{\mathbb{Q}}$): $\overline{\mathbb{Q}}$ ב־$\mathbb{C}$ קבוצת כל האיברים האלגבריים מעל $\mathbb{Q}$ ונראה היום שהוא שדה ואף בן־מנייה (הבן־מנייה הגיוני: יש מספר בן־מנייה של פולינום מעל $\mathbb{Q}$ ולכן יכולים להיות רק מספר בן־מנייה של שורשים ולכן יש מספר בן־מנייה של מספרים אלגבריים מעל $\mathbb{Q}$).

הגדרה 5.3 (פולינום מינימלי): תהיי L/K הרחבה ו־$\alpha \in L$, והוכחנו ש־$K[\alpha] = K[t]/I$ כאשר $I = \{f \in K[t] \mid f(\alpha) = 0\}$ ב־L.
I הוא אידיאל ראשי (נוצר על־ידי איבר אחד) כך ש־$K[t]$ חוג ראשי ו־I ראשוני, כי $K[\alpha] \subseteq L$ תחום שלמות (אם $0 = h(\alpha)g(\alpha)$ ב־L אז $g(\alpha) = 0$ או $h(\alpha) = 0$ אז אם $hg \in I$ אז $h \in I$ או $g \in I$ וראינו ש־I אידיאל ראשוני אם ורק אם R/I תחום שלמות).
מכאן, או $I = (f_\alpha(t))$ כאשר f_α הוא אי־פריק או $I = 0$ (בכלל זה אידיאל מקסימלי).
אם $I = 0$ אז α טרנסצנדנטי ואם f_α הוא אי־פריק אז α אלגברי.
אם קיימים פולינומים שונים מאפס שמתאפסים ב־α אז יש פולינום מתוקן מינימלי כזה, קוראים ליוצר זה **הפולינומים המינימלי של α מעל K** ונסמנו f_α או $f_{\alpha/K}$ כדי להדגיש מעל איזה שדה אנחנו מדברים (כאשר האחרון זו הצורה המועדפת), ברשומות מדי פעם זה מופיע גם בתור $f_{\alpha,K}$.

טענה 5.1 (תנאים לפולינום מינימלי): על־מנת להגיד ש־$f_{\alpha/K}$ הוא פולינום מינימלי, צריך להתקיים:
1. $f_{\alpha/K}(\alpha) = 0$
2. f פולינום מתוקן
3. f אי־פריק

דוגמה 5.2: $f_{\sqrt{2}/\mathbb{Q}} = t^2 - 2$ עם $\deg(f) = 2$, $f_{\sqrt{2}/\mathbb{Q}(\sqrt{2})} = t - \sqrt{2}$ עם $\deg(f) = 1$ (שדה יותר גדול => פולינום יותר קטן).

למה 5.1: אם $F/L/K$ מגדל הרחבות ו־$\alpha \in F$ איבר אלגברי מעל K הוא הוא גם אלגברי מעל L והפולינום המינימלי של α מעל L מחלק את הפולינום המינימלי של α מעל K, ובסימונים $f_{\alpha/L} \mid f_{\alpha/K}$.

הוכחה: $f_{\alpha/K} \in L[t]$ וגם $f_{\alpha/K}(\alpha) = 0$ ולכן הוא מתחלק ב־$f_{\alpha/L}$. □

סימון: $f_{\alpha/K} \cdot K[t] = m_{\alpha/K}$ האידיאל של כל הפולינומים מעל K שמתאפסים ב־α (או $m_{\alpha/K} = 0$ אם α הוא טרנסצנדנטי).

למה 5.2: תהיי L/K הרחבה ו־$\alpha \in L$
1. אם α אלגברי עם פולינום מינימלי $f_\alpha = f_{\alpha/K}$ ו־$d = \deg f_\alpha$ אזי $K(\alpha) = K[\alpha] = K[t]/(f_\alpha)$ ו־$1, \alpha, \cdots, \alpha^{d-1}$ מהווים בסיס של $K(\alpha)/K$ ובפרט מתקיים $d = [K(\alpha) : K]$
2. אם α טרנסצנדנטי אז $K(\alpha) \underset{t \mapsto \alpha}{\simeq} K(t)$ ו־$[K(\alpha) : K] = \infty$

הוכחה:
1. כבר הוכחנו ש־$K[\alpha] = K[t]/(f_\alpha)$ והיות ו־f_α הוא אי־פריק אז m_α הוא מקסימלי ולכן $K[\alpha]$ שדה ו־$K(\alpha) = K[\alpha]$.
   עכשיו נחשב את המימד של $K(\alpha) = K[t]/(f_\alpha)$ ונראה שמתקיים $\dim_K K[t]/(f) = \deg(f)$ לכל $f \neq 0$:
   לכל $h \in K[t]$ פולינום קיימים ויחידים q_h, r_h כך ש־$h = q_h \cdot f_\alpha + r_h$ וגם $\deg(r_h) < d = \deg(f)$ כאשר r_h היא החלוקה עם שארית.
   זה נותן לנו העתקה $r : K[t] \to K[t]_{<d}$, נראה שזו העתקה לינארית:
   לכל $g, h \in K[t]$ מתקיים $r_{g+h} = r(r_g + r_h)$ ולכן $r_{g+h} = r_g + r_h$, אותו הדבר לכפל בסקלר וקיבלנו העתקה לינארית ועל.
   מתקיים שהגרעין הוא $f_\alpha \cdot K[t] = m_\alpha$ ולכן (כמרחבים וקטורים) $K[\alpha] \simeq K[t]/m_\alpha \simeq K[t]_{<d}$ והבסיס כאן הוא $1, t, \cdots, t^{d-1}$ ואז $1, \alpha, \cdots, \alpha^{d-1}$ הוא בסיס.

2. מתקיים $K[t] \simeq K[\alpha]$ (כי $K[t] \simeq K[t]/m_\alpha \simeq K[\alpha]$) ולכן $K[t] = \mathrm{Frac}(K[t]) \simeq \mathrm{Frac}(K[\alpha]) = K(\alpha) \subset L$ ו־$K[\alpha] \subset K(\alpha)$ והמימד שלנו הוא ∞.

□

הערה: $K[t] \to K[t]_{<d}$ הוא **לא** הומומורפיזם של חוגים כי $K[t]_{<d}$ הוא לא חוג, הוא אפילו לא סגור לכפל.

הגדרה 5.4 (הרחבה פרימיטיבית): L/K נקראת **הרחבה פרימטיבית** אם היא נוצרת על־ידי איבר אחד, כלומר קיים $\alpha \in L$ כך שמתקיים $L = K(\alpha)$.

למה 5.3: אם K שדה ו־$f \in K[t]$ אי־פריק אז קיימת הרחבה פרימיטיבית L/K כך של־f יש שורש ב־L.

הוכחה: $L' = K[t]/(f(t))$ זה שדה, ולכן יש $\varphi : K \to L'$ שהוא שיכון כך ש־$L'/\varphi(K)$ הוא הרחבה פרמיטיבית הנוצר על־ידי שורשי f, מלמה שלא ראינו בהרצאות (3.1.17 ברשומות של מיכאל), יש הרחבה L/K שאיזומורפית ל־$L'/\varphi(K)$ ולכן L/K היא הרחבה פרימיטיבית הנוצרת על־ידי שורש של f ואז $f_\alpha \mid f \Rightarrow f_\alpha = f$. □

הגדרה 5.5 (דרגה של איבר): עבור α/K אלגברי, **הדרגה של α/K** היא $\deg_K(\alpha) = \deg\left(f_{\alpha/K}\right)$ (מהלמה שראינו זה אומר $K[\alpha] : K$).

הגדרה 5.6 (הרחבה אלגברית): תהיי L/K הרחבות שדות. נגיד שההרחבה היא **אלגברית** אם כל $\alpha \in L$ הוא אלגברי מעל K.

למה 5.4: תהיי L/K הרחבות שדות, אז

1. אם $[L : K] = d$ אז לכל $\alpha \in L$ אלגברי, $\deg_K(\alpha) \mid d$ (ומתקיים במקרה זה ש־L/K אלגברי)
2. אם $L = K(\alpha_1, \cdots, \alpha_n)$ אזי $[L : K] =\leq \prod_{i=1}^n \deg_K(\alpha_i)$ כאשר $\alpha_1, \cdots, \alpha_n$ אלגבריים

הוכחה:

1. בין $1, \alpha, \cdots, \alpha^d$ (יש כאן $d+1$ איברים) יש תלות לינארית וזה נותן פולינום מדרגה קטנה/שווה ל־d שמתאפס ב־α.
   בדרך אחרת אפשר לראות את זה $\deg_K(\alpha) = [K(\alpha) : K] \mid [L : K]$ מכפליות הדרגה
2. מתקיים

$$[L : K] = [K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdot \cdots \cdot [L : K(\alpha_1, \cdots, \alpha_n)]$$

אז כל אחד מהם נוצר על־ידי איבר בודד ולכן פרימיטיבי, אז

$$[L : K] = \prod_{i=1}^n [K(\alpha_1, \cdots \alpha_i) : K(\alpha_1, \cdots, \alpha_{i-1})] = \prod_{i=1}^n \deg_{K(\alpha_1, \cdots, \alpha_{i-1})}(\alpha_i) \leq \prod_{i=1}^n \deg_K(\alpha_i)$$

□

מסקנה 5.1: אם L/K הרחבה ו־$\alpha, \beta \in L$ אלגבריים מעל K, אזי גם $\alpha+\beta, \alpha-\beta, \alpha\cdot\beta, \frac{\alpha}{\beta}$ (אם האחרון מוגדר) אלגבריים מעל K מדרגה שקטנה שווה ל־$\deg_K(\alpha)\cdot\deg_K(\beta)$, ובפרט קבוצת כל המספרים האלגבריים ב־L מעל K היא שדה.

הוכחה: ניקח $L \supseteq K(\alpha, \beta)$ ולכן לפי הלמה לעיל $[K(\alpha, \beta) : K] \leq \deg_K(\alpha)\cdot\deg_K(\beta)$ ולכן כל $\gamma \in K(\alpha, \beta)$ אלגברי ואפילו יש חסם על הדרגה שלו, $\deg_K(\gamma) \leq \deg_K(\alpha)\cdot\deg_K(\beta)$. □

תרגיל 5.1: $\deg_{\mathbb{Q}}\left(\sqrt[3]{3}+\sqrt{2}\right) = 6$.

הוכחה: זה נובע מכך ש־$\sqrt[3]{3}, \sqrt{2}$ הם שניהם אלגבריים בהרחבה (השורשים של הפולינומים x^3-3, x^2-2) ולכן מהמסקנה $\deg_{\mathbb{Q}}\left(\sqrt[3]{3}+\sqrt{2}\right) \leq 6$.
השוויון נובע מכך שהם בלתי־תלויים לינארית (או אלגברית?) כי הם פתרונות של שורשים ממעלות שונות ולכן כל קשר ביניהם הוא רק הקשר הטריוויאלי (עם הנחה בשלילה וקצת עבודה נוכל לקבל שיש איבר אלגברי אחר שמאפס את הפולינומים הללו ואז זו סתירה להיות הפולינומים שמצאנו כפולינומים המינימליים). □

סימון: $\overline{\mathbb{Q}} = \{x \in \mathbb{C} \mid \mathbb{C}$ אלגברי ב־ $x\}$

הערה: הוכחנו שזה שדה לפי הגדרה ולכן $\overline{\mathbb{Q}}/\mathbb{Q}$ היא **הרחבה אלגברית** אך כמובן לא נוצרת סופית.

מסקנה 5.2: עבור הרחבת שדות L/K, הבאים שקולים

1. L/K סופית
2. L/K אלגברית נוצרת סופית
3. L נוצרת על־ידי איברים אלגבריים $\alpha_1, \cdots, \alpha_n$

הוכחה: $2 \Rightarrow 1$: נניח ש־L/K סופית אז היא אלגברית (מהלמה על הדרגות שראינו לעיל) ונוצרת סופית (אפילו כמרחב וקטורי).

$3 \Rightarrow 2$: מיידי מהגדרה.

$1 \Rightarrow 3$: נניח ש־$L = K(\alpha_1, \cdots, \alpha_n)$ כאשר $\alpha_1, \cdots, \alpha_n$ אלגבריים. אזי מהלמה שראינו $[L : K] \le \prod_{i=1}^{n} \deg_K(\alpha_i) < \infty$ ולכן סופית. □

מסקנה 5.3 (תנאי לטרנזטיביות הרחבות אלגבריות): יהיה $F/L/K$ מגדל הרחבות. אזי F/K אלגברי אם ורק אם F/L ו־L/K אלגבריים

הוכחה: $\Longleftarrow$ נניח ש־F/K אלגברית אז ברור ש־$L/K, F/L$ הרחבות אלגבריות ישירות מהגדרה.

$\Longrightarrow$ נניח ש־F/L ו־L/K אלגבריות ונוכיח כי כל $\alpha \in F$ אלגברי מעל K: α אלגברי מעל L ולכן קיים $0 \neq f = f_{\alpha/L}$ כך שמתקיים $f(\alpha) = 0 = \alpha^d + \beta_1\alpha^{d-1} + \cdots + \beta_d$ עם $\beta_1, \cdots, \beta_d \in L$.

היות ו־$\beta_1, \cdots, \beta_d$ אלגבריים מעל K, השדה $E = K(\beta_1, \cdots, \beta_d)$ הוא סופי מעל K עם הלמה לעיל.

היות ו־α הוא אלגברי מעל E, ההרחבה $E' = E(\alpha)/E = K(\alpha, \beta_1, \cdots, \beta_d)/K(\beta_1, \cdots, \beta_d)$ היא הרחבה סופית גם־כן.

נשים לב שקיבלנו מגדל הרחבות סופיות (E' סופית כי פרימטיבית מהיות α אלגברי)

$$K(\alpha, \beta_1, \cdots, \beta_d)/K(\beta_1, \cdots, \beta_d)/K$$

אז מהלמה שראינו על כפליות הדרגה

$$\deg_K(d) \le [K(\alpha, \beta_1, \cdots, \beta_d) : K] < \infty$$

□

הגדרה 5.7 ($\mathcal{C}$ מחלקה יציבה): נסמן ב־$\mathcal{C}$ את המחלקה של הרחבות שדות. $\mathcal{C}$ נקראת **יציבה** (ברשומות לפעמים שלמה) אם לכל מגדל $F/L/K$ של הרחבות, $F/K \in \mathcal{C}$ אם ורק אם $F/L, L/K \in \mathcal{C}$.

נשים לב שהוכחנו שמחלקות של הרחבות סופיות ואלגבריות היינן שלמות.

6 תרגול 2 – 02/04

6.1 משהו

להשלים

7 הרצאה 4 – 07/04

7.1 שימושים בסיסיים של תורת השדות – בניות עם סרגל ומחוגה

אני לא אוהבת לצייר, אז אני אוותר.

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

$$\operatorname{cont}(f) = \gcd(a_0, a_1, \dots, a_n)$$

הגדרה 8.2 (פולינום פרימיטיבי): פולינום $f(t) \in \mathbb{Z}[t]$ יקרא **פרימיטיבי** אם $\operatorname{cont}(f) = 1$.

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

משפט 8.1 (למת גאוס הראשונה): אם $f, g \in \mathbb{Z}[t]$ אזי $\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$. בפרט, fg פרימיטיבי אם ורק אם f ו־g פרימיטיביים.

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

נניח שלא ולכן קיים $p \in \mathbb{N}$ ראשוני כך שמתקיים $p \mid \operatorname{cont}(f_0 \cdot g_0)$, 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:

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

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־$\mathbb{Z}[t]^\times = \mathbb{Z}^\times$ ולכן $p \notin \mathbb{Z}^\times$ ולכן p מחלק פולינום $h \in \mathbb{Z}[t]$ אם ורק אם $p \mid \operatorname{cont}(h)$.

אם $p \mid f \cdot g$ אז מלמת גאוס הראשונה נובע $p \mid \operatorname{cont}(f) \cdot \operatorname{cont}(g)$ 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 $\operatorname{Frac}(\mathbb{Z})$, 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־$0 \neq c$ ב־$\mathbb{Z}[t]$ ולכן $c \cdot g, c^{-1} \cdot h \in \mathbb{Z}[t]$ 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־$0 < m, n$ ו־$m \cdot g, n \cdot h \in \mathbb{Z}[t]$ ואז נקבל פירוק $m \cdot n \cdot f = m \cdot g \cdot n \cdot h$.
נסמן $\ell = \operatorname{cont}(f), \alpha = \operatorname{cont}(m \cdot g), \beta = \operatorname{cont}(n \cdot h)$. מלמת גאוס הראשונה נקבל עם כפליות התכולה
$$\operatorname{cont}(m \cdot n \cdot f) = m \cdot n \cdot \ell = \alpha \cdot \beta = \operatorname{cont}(m \cdot g \cdot n \cdot h)$$
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 $f = \ell \frac{m}{\alpha} \cdot g \cdot \frac{n}{\beta} \cdot h$.
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. (הוכחה בהרצאה 6)

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

$\Longleftarrow$ 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

להשלים

10 תרגיל 2

10.1 טריקים

להשלים

10.2 מסקנות

להשלים

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. $\square$

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

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

$\square$

משפט 11.1 (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 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־$p \mid b_i$ 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 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 $p \in \mathbb{N}$ ראשוני, 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. $\square$

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: להשלים. $\square$

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: להשלים. $\square$

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: $(2) \iff (3)$ שכן תמיד יש פירוק לפולינומים אי־פריקים.
$(1) \impliedby (2)$: 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 $\deg(f)$.
$(1) \impliedby (4)$: 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־$[L : K] = \deg(f) > 1$. $\square$

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 $\mathrm{dic} < 0$ (דיסקרמיננטה)

הוכחה: נשים לב $2 \iff 1$ ברור, ולכן מספיק שנוכיח רק את 1: נשים לב $\mathbb{R}[t] \subseteq \mathbb{C}[t]$ $f = \overline{f} =$ 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 $F = \{\alpha \in L \mid K$ 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 $K \hookrightarrow E$ 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־$\phi_2 \mid_{L_1} = \varphi_1$, 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 $\phi_i \mid_{L_i} \phi$ לכל i.
מהלמה של צורן קיים איבר מקסימלי $(F, \phi) \in \mathcal{V}$ ונטען כי $F = L$ ולכן ϕ הוא השיכון $L \hookrightarrow E$ 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.

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

להשלים

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־$\widetilde{\overline{K}}'/K$ 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 $\overline{K}' = \phi\left(\overline{K}\right)$ 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 $\mathrm{Aut}\left(\overline{K}/K\right) \ni \sigma : \overline{K} \to K$ 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

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

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 $\deg_s(\alpha) = \deg_{K,s}(\alpha)$ 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 $\deg_i(\alpha) = \deg_{K,i}(\alpha)$ היא הריבוי של α ב־f_α: להשלים

הערה: להשלים

דוגמה 14.1 : להשלים

דוגמה 14.2 : להשלים

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 $p = \mathrm{char}(K) > 0$, 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: להשלים? $\square$

משפט 15.1: נניח כי $f \in K[t]$ פולינום אי־פריק ומתוקן ו־$\alpha \in \overline{K}$ שורש של f. אזי
1. אם $\mathrm{char}(K)=0$ אז f ו־α הם פרידים ואז $\deg_i(\alpha) = \deg(f) = \deg_K(\alpha)$
2. אם $\mathrm{char}(K)=p$ 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 $f=\sum_{i=0}^{d}a_it^i$ אז אם $f'=\sum_{i=1}^{d}ia_it^i=0$, אז לכל $i>0$ בהכרח מתקיים $ia_i=0\in K$ ולכן רק המקדמים $a_{pj}\neq 0$.

במילים אחרות מתקיים

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

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 $\frac{d}{p^l}=n=\deg(h)$, $p^l=p^{m+1}$. 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 להשלים), קיים $\sigma\in\mathrm{Aut}\left(\overline{L}/K\right)$ כך ש־$\sigma(\alpha)=\alpha'$ וזה בידיוק 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 $\phi:L\xrightarrow{\sim}\overline{L}$ כך שמתקיים $\phi(L)\neq L$.

מלמת ההרמה, ϕ מורחב ל־K־שיכון של שדות $\sigma:\overline{L}\xrightarrow{\sim}\overline{L}$ 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: להשלים $\square$

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 – להשלים
3. נניח כי L/K נורמלית ונטען כי L/F כ נורמלית להשלים

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

הוכחה: להשלים $\square$

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־$\overline{K} \supseteq S = \{\text{כל השורשים של } f \in P\}$ 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 $L \xrightarrow{\sim} L'$. $\square$

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 $S = \{\text{שורשי } f \in P\}$. נסתכל על $\mathrm{Aut}\left(\overline{K}/K\right) \ni \sigma \circlearrowleft \overline{K}$, 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 $L = K(\alpha_1, ..., \alpha_n)$ 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 $L = K(\alpha_1, ..., \alpha_n)$ כאשר $\alpha_1, ..., \alpha_n$ הם השורשים של f והלכן L/K אלגברית וגם נוצרת סופית ולכן סופית.

$\square$

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 $F = L^{nor}$. $\square$

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

להשלים ציור?

דוגמה 17.4: $L = \mathbb{Q}\left(\sqrt[4]{2}\right)$ ואז $L^{nor} = \mathbb{Q}\left(\sqrt[4]{2},i\right)$ ואז להשלים 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 $\sigma \in \mathrm{Aut}_K(L) = \mathrm{Aut}(L/K)$ משרה תמורה על C_f והומומורפיזם הצמצום מ־$\mathrm{Aut}_K(L) \to \mathrm{Perm}\, C_f = \mathrm{Aut}(C_f) = S_n$ הוא שיכון.

הוכחה: להשלים $\square$

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 $\xi \in \overline{K}$ שמקיים $\xi^n = 1$.

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

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

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

נשים לב ש־$\mu_n(K)$ היא תת־חבורה של $K^\times$ מסדר המחלק את n (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־$x \mapsto e^{((2\pi i x))}$ משרה איזומורפיזם $\mathbb{Q}/\mathbb{Z} \xrightarrow{\sim} \mu_\infty(\mathbb{C})$

הוכחה:

1. נשים לב שמתקיים

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

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 $\mu_\infty(\mathbb{Q}(i)) \subseteq \mu_4$.

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 $\frac{\pm 1 \pm \sqrt{-3}}{2} \notin \mathbb{Q}(i)$, אבל ה־4 האחרים כן ב־$\mathbb{Q}(i)$

כי בידיוק $\{\pm 1, \pm i\}$ 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־$\left[\mathbb{Q}\left(\sqrt{d}\right) : \mathbb{Q}\right] \leq 2$, 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 $\xi = -1 \in \mathbb{Q} \subset \mathbb{Q}\left(\sqrt{d}\right)$ 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

$$\varphi(x + \mathbb{Z}) = 1 \iff e^{2\pi i x} = 1 \iff x \in \mathbb{Z} \Rightarrow x + \mathbb{Z} = 0 + \mathbb{Z}$$

והוא גם אכן על, כי כל $\xi \in \mu_\infty(\mathbb{C})$ הוא שורש יחידה, ולכן הוא מהצורה $\xi = e^{2\pi i \frac{k}{n}}$ עבור n כלשהו, ולכן מספיק שנבחר $k \in \mathbb{Z}$ כך שמתקיים $\varphi\left(\frac{k}{n} + \mathbb{Z}\right) = \xi$.

$\square$

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 $G[p]$). $\square$

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

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

□

18 הרצאה 11 – 06/05

18.1 שורשי יחידה – המשך

הגדרה 18.1 (שורש יחידה פרימיטיבי מסדר n): יהי $2 \leq n \in \mathbb{N}$. **שורש יחידה פרימיטיבי מסדר n** הוא שורש יחידה שלכל $1 \leq m < n$ מתקיים $\xi^m \neq 1$.

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

$$m_\xi = x^{p-1} + x^{p-2} + ... + x + 1$$

מסקנה 18.1: אם K שדה סגור אלגברית ו־$n \geq 1$ 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 ξ_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 $n \geq 1$, 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 $\xi \in K$ שורש יחידה מסדר p^n, משמע $\xi^{p^n} = 1$ ולכן ξ 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

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

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 $\xi_n \notin K$, ולכן נשאר רק עם n־ים שעבורם $\gcd(n,p) = 1$, משמע

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

□

הערה: מיכאל אמר שהאיזומורפיזמים הללו הם לא יחידים ולא קנונים, כי הם "לא טבעיים" – הם תלויים בבחירה של K ו־$\xi_n \in K$ 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 $\mu_q=\mathbb{F}_q\setminus\{0\}$.
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 $\{x\mid x^q=x\}=\mathbb{F}_q\subset K$ 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 $\alpha^2+\alpha+1=0$ (זה שוב האוטומורפיזם $\alpha\mapsto\alpha+1$).

הוכחה:

1. ראשית מהמשפט לעיל נובע כי $\mathbb{F}_9$ הוא ההרחבת שדות היחידה (עד־כדי איזומורפיזם) של $\mathbb{F}_3$ מדרגה 2 ($[\mathbb{F}_9:\mathbb{F}_3]=2$).
נבחן את הפולינום x^2+1, נשים לב שהוא לא מתאפס לאף $a\in\mathbb{F}_3$ והוא אי־פריק מעל $\mathbb{F}_3$.
נשים לב שכל איבר ב־$\mathbb{F}_3(i)$ הוא מהצורה $a+bi\in\mathbb{F}_3$ וגם $i^2=2$, ויש לנו 9 צירופים אפשריים מקומבינטוריקה.
מהמשפט לעיל נקבל כי $\mathbb{F}_9=\mathbb{F}_3(i)$.
2. נבחר את הפולינום x^2+x+1 ואנחנו כבר יודעים שהוא אי־פריק מעל $\mathbb{F}_2[x]$ כי אין לו פיתרונות ב־$\mathbb{F}_2$ (ולכן הוא גם ראשוני) ונבחר α המקיימת $\alpha^2+\alpha+1=0$.
עכשיו, $\mathbb{F}_2[\alpha]=\mathbb{F}_2[x]/(x^2+x+1)$ ונשים לב שהוא מכיל 4 איברים $\{0,1,\alpha,\alpha+1\}$ כצירופים לינאריים של 1 ו־α ונטען שהאיברים $\{1,\alpha,\alpha+1\}$ מהווים חבורה כפלית מסדר 3:
מההנחה על α שבחרנו נובע $\alpha^2=\alpha+1$ ולכן

$$\alpha^3=\alpha^2+\alpha=(\alpha+1)+\alpha=2\alpha+1=1(\bmod 2)$$

אז זה סגור לחיבור, כפל ויחידה וקיבלנו שזה אכן שדה.
מצאנו שדה עם 4 איברים ומהטענה לעיל מתקיים $\mathbb{F}_2[x]/(x^2+x+1)=\mathbb{F}_4$.

$\square$

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־$n=\deg\left(f_{\alpha/\mathbb{F}_q}\right)$. $\square$

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.
$2\Longleftarrow 1$ 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 $r=q^d$.
$1\Longleftarrow 2$ 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: $\left\{1, \mathrm{Fr}_q, ..., \mathrm{Fr}_{q^{d-1}}\right\} = \mathbb{Z}/d\mathbb{Z} \simeq \mathrm{Aut}_{\mathbb{F}_q}\left(\mathbb{F}_{q^d}\right)$

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־$1 = \left|\hom_{\mathbb{F}_q}\left(\mathbb{F}_q(\alpha), \mathbb{F}_q(\alpha)\right)\right|$, 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 $\left\{x \mid \mathrm{Fr}_q^i(x) = x\right\} \to \mathrm{Aut}_{\mathbb{F}_q}\left(\mathbb{F}_{q^d}\right) = \left\{1, \mathrm{Fr}_q, ..., \mathrm{Fr}_{q^{d-1}}\right\}$ 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 (לקשר למסקנה).
כל $a \in \mathbb{F}_q$ מקיים $\mathrm{Fr}_q(a) = a^q = a$ ולכן Fr הוא איבר של G.
מאותה סיבה, $\mathrm{Fr}_q)^d = 1 \in G$ 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: $\bigcup_{n\geq 1} \mathbb{F}_{p^n} = \overline{\mathbb{F}_p}$ 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

להשלים

20 תרגיל 4

20.1 טריקים

להשלים

20.2 מסקנות

להשלים

21 הרצאה 12 – 12/05

21.1 הרחבות ציקלוטומיות

פרק 6.3 ברשומות של מיכאל.

המטרה שלנו היא לחשב את הדרגה של $[\mathbb{Q}(\xi_n):\mathbb{Q}]=\varphi(n)$ כאשר $\varphi(n)$ היא פונקציית אויילר, נרצה לפרק את $t^n-1(=\phi_n(t))$, לדבר על מכפלות ציקליות ולחשב את $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi_n))$.

הגדרה 21.1 (הרחבה ציקלוטומית): הרחבה L/K נקראת **הרחבה ציקלוטומית** אם $L=K(\xi)$ (נוצר על־ידי ξ שורש יחידה).

יהי n הסדר של ξ ($\xi^n=1$, דהיינו ξ שורש פרימיטיבי), אז כל הצמודים של ξ מעל K הם גם־כן שורשי יחידה פרימיטיביים מסדר n (שכן, $\xi^n=1$ וגם $\nexists 0<m<n\ (m\in\mathbb{N})\ s.t.\ \xi^m=1$).

ממסקנה שראינו (לקשר), כל K־אוטומורפיזם $\sigma\in\mathrm{Aut}_K(L)$ נקבע ביחידות על־ידי $\sigma(\xi)=\xi'$, ולכן יש הומומורפיזם צמצום $\sigma\mid_{\mu_n}$ כחבורה (למה? כי $\mu_\in\subset L^\times=\langle\xi\rangle$), ולכן $\mathrm{Aut}_K(L)\hookrightarrow\mathrm{Aut}(\mu_n)$.

תרגיל 21.1 (6.3.2 ברשומות של מיכאל):

1. $a\in\mathbb{Z}/n\mathbb{Z}$ הוא הפיך אם ורק אם $\gcd(a,n)=1$
2. תהיי $(H,+)$ חבורה ציקלית מסדר n עם יוצר g. להראות כי ag הוא יוצר של H אם ורק אם $(a,n)=1$
3. להראות שיש הומומורפיזם קאנוני $\mathrm{Aut}(H)\xrightarrow{\sim}(\mathbb{Z}/n\mathbb{Z})^\times$ כך ש־$\sigma_a\mapsto a$ הנתון על־ידי $\sigma_a(h)=ah$ עבור $h\in H$

הוכחה:

1. בכיוון הראשון נניח ש־$\gcd(a,n)=1$, מזהות בז'ו נובע שקיימים x,y כך שמתקיים $ax+ny=1$ ולכן $ax\equiv 1\bmod n$, ולכן x הוא ההופכי הכפלין של a ב־$\mathbb{Z}/n\mathbb{Z}$ ולכן a הפיך.

   בכיוון השני, נניח ש־a הפיך ולכן קיים b כך ש־$ab\equiv 1\bmod n$, ולכן קיים k כך שמתקיים $ab=1+kn$ משמע $ab-kn=1$. אבל צד שמאל הוא צירוף לינארי של a,n ולכן עבור $d=\gcd(a,n)$ נובע כי d מחלק גם כל צירוף לינארי של a,n ובפרט $d\mid ab-kn$, אבל אז $d\mid 1$ ולכן $d=1$.

2. בכיוון הראשון נניח ש־$\gcd(a,n)=1$ ונסתכל על תת־החבורה הנוצרת על־ידי ag שכל איבריה הם מהצורה $k(ag)$ עבור $k\in\mathbb{Z}$.

   הסדר של ag הוא ה־$m\in\mathbb{N}$ המינימלי כך ש־$m(ag)=0$, אבל g הוא יוצר של H ולכן g הוא 0 אם ורק אם ma הוא כפולה של n ולכן אנחנו מחפשים $ma\equiv 0\bmod n$, וזה נתון על־ידי $m=\frac{n}{\gcd(a,n)}=\frac{n}{1}=n$ ולכן הסדר של ag הוא n ו־ag הוא יוצר של H.

   בכיוון השני, נניח ש־ag הוא יוצר של H, ולכן $o(ag)=n$, אבל זה גם ה־$m\in\mathbb{N}$ המינימלי כך ש־$m(ag)=0$ והוא כפולה של n, אבל ה־m המינימלי שמקיים את זה נתון על־ידי $m=\frac{n}{\gcd(a,n)}$, ולכן $\gcd(a,n)=1\iff\frac{n}{\gcd(a,n)}=n$.

1. להשלים?

$\square$

למה 21.1: יהי $L=K(\xi)$ הרחבה ציקלוטומית מסדר n ו־n הסדר של ξ (כאשר L/K הרחבה נורמלית). אזי

1. ξ^a הוא שורש פרימיטיבי מסדר n אם ורק אם $\gcd(n,a)=1$
2. הומומורפיזם הצמצום מקיים $(\mathbb{Z}/n\mathbb{Z})^\times\xleftarrow{\sim}\mathrm{Aut}(\mu_n)\hookleftarrow\mathrm{Aut}_K(L)$ (הוא שיכון) ו־$a\mapsto\sigma$ אם ורק אם $\sigma(\eta)=\eta^a$ עבור $\eta\in\mu_n$

להשלים כמה טענות לא ברורות בהקשר להוכחה לעיל :(

הערה (תזכורת – משפט השאריות הסיני): עבור $m,n\in\mathbb{N}$ מתקיים

$$\mathbb{Z}_{mn}\cong\mathbb{Z}_m\times\mathbb{Z}n\iff\gcd(m,n)=1$$

באינדוקציה אפשר להוכיח שהטענה נכונה לכל $n_1,...,n_r$ זרים בזוגות.

עוד מסקנה שנובעת ממשפט השאריות הסיני עם תוספת קטנה זה שעבור $n=\prod_{i=1}^r n_i$ זרים בזוגות מתקיים

$$(\mathbb{Z}_n)^\times\cong\left(\mathbb{Z}_{n_i}\right)^\times\times...\times\left(\mathbb{Z}_{n_r}\right)^\times$$

זה נובע ממשפט השאריות הסיני ויחד עם ההוכחה שעבור R,S חוגים מתקיים $(R\times S)^\times\cong R^\times\times S^\times$ (פשוט לפתוח מההגדרות ויישר יש איזומורפיזם).

למה 21.2: יהי $1<n\in\mathbb{N}$.

1. אם $p\in\mathbb{N}$ ראשוני כך ש־$p\neq 2$ אז $(\mathbb{Z}/p^n\mathbb{Z})^\times$ היא ציקלית מסדר $p^{n(p-1)}$
2. החבורה $(\mathbb{Z}/2^n\mathbb{Z})^\times\cong\mathbb{Z}/2^{n-2}\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$

הוכחה: בתור התחלה להוכחה, ניקח את שני המקרים בחשבון. נסתכל על הומומורפיזם הצמצום עם מודלו p ואז $\lambda : G_{p^n} \to G_P = \mathbb{F}_p^\times$ $\square$

יש פה הרבה מה להשלים...

22 הרצאה 13 – 13/05

22.1 הרחבות ציקלוטומיות – המשך

תשלימי

22.2 הרחבות רדיקליות

פרק 6.4 ברשומות של מיכאל.

הגדרה 22.1 (הרחבה רדיקלית): הרחבת שדות L/K נקראת **הרחבה רדיקלית** אם $L = K\left(a^{\frac{1}{n}}\right)$.
לפעמים נראה אותה בתור $K(\alpha)/K$ עבור α המקיים $\alpha^n - a = 0$.

הערה (פתולוגיה): כבר ראינו שתי בעיות שיכולות לקרות בהרחבות מהסוג הזה:

1. הפולינום $f(t) = t^n - a$ נגזרתו היא $f'(t) = nt^{n-1}$ ולכן הפולינום הוא פריד אם ורק אם $n \in K^\times$ ו־$a \neq 0$ או $n = 1$ ו־$a = 0$
2. ההרחבה $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ לא מעניינת, שכן אין לה אוטומורפיזמים (זה כי $\mu_3 \notin \mathbb{Q}$)

בלי שתי החריגות הללו, התורה שנתעסק בה היא מאוד יפה.

למה 22.1: נניח ש־K הוא שדה, $n \in K^\times$ (אם $\mathrm{char}(K) = 0$ או $\gcd(n, \mathrm{char}(K)) = 1$) כך ש־$\mu_n \subset K$ ו־$a \in K$. אז הבאים שקולים

1. נגדיר $L = K(\alpha)$ כאשר $\alpha = a^{\frac{1}{n}}$ (ההרחבה הנוצרת על־ידי שורש בודד) אז L הוא שדה פיצול של $t^n - a$ (מההכלה $\mu_n \subset K$ נובע שאם הוספתי שורש 1, פיצלתי הכל) ו־$\mu_n \alpha = \left\{\alpha, \xi_n \alpha, \ldots, \xi_n^{n-1}\alpha\right\}$ קבוצת כל השורשים ב־K
2. כל $\sigma \in \mathrm{Aut}_K(L)$ משמר את $\mu_n \alpha$, זאת־אומרת פועל על קבוצה זו על־ידי כפל באיבר $\xi_\sigma \in \mu_n$ ונקבע לחלוטין על־ידי ξ_σ. בפרט, יש לנו שיכון טבעי $\mathrm{Aut}_K(L) \to \mu_n$
3. $|\mathrm{Aut}_K(L)| = [L : K]$ ובפרט $\mathrm{Aut}_K(L) = \mu_n$ אם ורק אם $t^n - a$ הוא אי־פריק (זה קורה אם ורק אם $C_{\alpha/K = \mu_n \alpha}$)

הוכחה:

1. מכך ש־$n \in K^\times$, μ_n מכילה n איברים.
   כל $\xi\alpha \in \mu_n \alpha$ הוא השורש ה־n־י של a.
   לפולינום $t^n - a$ יש לכל היותר n שורשים, ולכן שורשי הפולינום הם בידיוק $\mu_n \alpha$.
   כעת, $\mu_n \in K$ ולכן $\mu_n \alpha \in L = K(\alpha)$ דהיינו הפולינום מתפצל לחלוטין ב־L (כל השורשים שם) ולכן L הוא שדה פיצול של הפולינום הזה (בפרט, הוא נוצר על־ידי שורש אחד)
2. אוטומורפיזם σ לוקח את α לצמוד שלו, שגם הוא שורש של $t^n - a$ ולכן $\sigma(\alpha) = \xi_\sigma \alpha$ עבור $\xi_\sigma \in \mu_n$.
   יתרה מכך, לכל שורש אחר $\xi\alpha \in \mu_n \alpha$ מתקיים
   $$\sigma(\xi\alpha) = \sigma(\xi)\sigma(\alpha) = \xi\xi_\sigma\alpha = \xi_\sigma \cdot (\xi\sigma)$$
   משמע σ מכפילה כל שורש ב־$\xi\sigma$ ונקבל העתקה $\lambda : \mathrm{Aut}_K(L) \to \mu_n$ שלא תלויה בבחירה של השורש $a^{\frac{1}{n}}$.
   יתרה מכך, σ פועלת לפי ξ_σ ו־τ פועלת לפי ξ_τ אז $\sigma\tau$ פועלת לפי $\xi_\sigma\xi_\tau$ כי
   $$(\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\xi_\tau\alpha) = \xi_\sigma\xi_\tau\alpha$$
   ולכן λ זה הומומורפיזם.
   לבסוף, כל $\sigma \in \mathrm{Aut}_K(L)$ נקבעת ביחידות לפי $\sigma(\alpha)$ שכן α יוצר את L מעל K ולכן σ נקבעת לפי ξ_σ ולכן λ חד־חד ערכית וקיבלנו שיכון
3. יהי $f(t)$ גורם אי־פריק של $t^n - a$ כך ש־α שורש שלו.
   אז $[L : K] = \deg(f)$ הוא מספר השורשים של הפולינום הפריד f, ולכן ל־α יש בידיוק $[L : K]$ הצמדות ב־L והעוצמה לפי למה שראינו (לקשר) היא בידיוק $|\mathrm{Aut}_K(L)|$

□

הערה: את הלמה וההוכחה לעיל התחלנו לראות בהרצאה של ה־13/05 וסיימנו ב־19/05.

הערה: במקרה כללי כאשר $n \in K^\times$ אבל לא בהכרח ש־$\mu_n \subseteq K$ אז L שדה הפיצול של $t^n - a$ הוא $K\left(\xi_n, \alpha = a^{\frac{1}{n}}\right)$ ו־$\mathrm{Aut} \subseteq \mu_n$

23 תרגול 6 – 14/05

23.1 שדות קומפוזיטום

תשלימי

24 תרגיל 5

24.1 טריקים

תשלימי

24.2 מסקנות

תשלימי

25 הרצאה 14 – 19/05

25.1 הרחבות רדיקליות – הרחבות ארטין־שרייר

פרק 6.4 ברשומות של מיכאל.

הגדרה 25.1 (הרחבות ארטין־שרייר): נניח ש־$\mathrm{char}(K)=p>0$ אז $\mu_p=\{1\}$ ופולינומים t^p-a לא ספרבילים לחלוטין (יש שורש 1, אין אוטומורפיזמים, הרחבות אי־פרידות), אז במקרה זה יש לנו תחליף: פולינום מהצורה $t^p-t-a\in K[t]$ נקרא **ארטין־שרייר** ועבור כל שורש α של פולינום זה, ההרחבה $L=K(\alpha)/K$ נקראת **הרחבת ארטין־שרייר**

תרגיל 25.1: $f(t)=t^p-t-a$ הוא אדטיבי, משמע $f(\alpha+\beta)-f(\alpha)+f(\beta)$ (זה לא אמור לקרות לפולינומים מדרגה יותר מ־1 במציין 0).

פתרון: נשים לב שמתקיים בגלל שאנחנו במציין p

$$(\alpha+\beta)^p=\alpha^p+\beta^p$$

אז (נתעלם ממהקבוע a כי הוא בכל־מקרה יעלם כשנחסר בין אגפים)

$$f(\alpha+\beta)=\alpha^p+\beta^p-\alpha-\beta=(\alpha^p-\alpha)+(\beta^p-\beta)-f(\alpha)+f(\beta)$$

□

למה 25.1: יהי K שדה ממציין $0<p,a\in K$ ו־$\alpha\in\overline{K}$ המקיים $\alpha^p-\alpha=a$ (במילים אחרות, α הוא שורש של פולינום ארטין־שרייר).
אזי $\alpha+\mathbb{F}_p=\{\alpha,\alpha+1,\cdots,\alpha+p-1\}$ (זו חבורה אדטיבית ולא כפלית), היא קבוצת השורשים של הפולינום $f(t)=t^p-t-a$ ו־$L=$ $K(\alpha)/K$ שדה פיצול של $f(t)$.
$\alpha\in K$ לא מעניין כי הוא מתפצל לחלוטין, ולכן אם $\alpha\notin K$ אזי $p=[L:K]$ ויש איזומורפיזם של חבורות $\mathrm{Aut}_K(L)\simeq\mathbb{F}_p(=\mathbb{Z}/p)$ המקיים $\sigma\mapsto\sigma(\alpha)-\alpha$

הוכחה: עבור כל $i\in\mathbb{F}_p$, מהתרגיל, $(\alpha+i)^p-(\alpha+i)-a=\underbrace{\alpha^p-\alpha-a}_{=0}+\underbrace{i^p-i}_{=0}=0$ כאשר $i^p-i=0$ נובע מכך שהפרובניוס קבוע על $\mathbb{F}_p$ וכן כי כל $\alpha+\mathbb{F}_p$ היא קבוצת שורשים של $f(t)$ ו־$a+\mathbb{F}_p\subseteq K(\alpha)=L$ ולכן זה שדה פיצול של $f(t)$.
נניח $\alpha\notin K$ אז ניקח $f_{\alpha/K}$ שדרגתו גדולה מ־1 ולכן יש לו עוד שורש α', ולכן יש $\sigma\in\mathrm{Aut}_K(L)$ כך שמתקיים $\sigma(\alpha)=\alpha'$ ולכן $\sigma(\alpha)=\alpha+$ $i(i\in\mathbb{F}_p^\times)$ ו־$\sigma^m=\alpha+mi$ ואז $\mathbb{F}_p\subset\mathbb{Z}i$ ולכן כל $\alpha+i$ צמוד של α/K, כלומר $C_\alpha=\alpha+\mathbb{F}_p$.
$$\sigma\overset{\lambda}{\mapsto}i$$
נקבל אם כך ש־$p=[L:K]=\deg f_{\alpha/K}$ והאוטומורפיזמים $\sigma'\mapsto i'$ כך שמתקיים $\sigma(\alpha)=\alpha+i$ אז

$$\sigma(\sigma'(\alpha))=\sigma(\alpha+i)=\sigma(\alpha)+\sigma(i)=\alpha+(i+i')\Rightarrow\lambda(\sigma\sigma')=\lambda(\sigma)+\lambda(\sigma')$$

□

25.2 הרחבות פרידות (ספרביליות)

פרק 7.1 ברשומות של מיכאל.

הגדרה 25.2 (דרגה פרידה, דרגה אי־פרידה): עבור הרחבה סופית L/K נגדיר **דרגה פרידה (ספרבילית)** של L/K על־ידי

$$[L:K]_s=|\mathrm{Hom}_K(L,K)|$$

זה בעצם מספר ה־K־שיכונים. נגדיר **דרגה אי־פרידה** כ־$[L:K]_i=\frac{[L:K]}{[L:K]_s}$ (בתור התחלה זה ב־$\mathbb{Q}$ אבל בהמשך נראה שזה שלם).

למה 25.2: נניח ש־$L=K(\alpha)/K$ הרחבה פרמיטיבית, אזי $[L:K]_s=\deg_{K,s}(\alpha)$ ו־$[L:K]_i=\deg_{K,i}(\alpha)$.
בפרט, $[L:K]_i=1$ אם $\mathrm{char}(K)=0$ ו־$p^n=[L:K]_i$ אם $\mathrm{char}(K)=p$.

הוכחה: $[L:K]_S=\left|\mathrm{Hom}_K\left(K(\alpha),\overline{K}\right)\right|=|C_\alpha|$ שכן לכל צמוד יש K־שיכון יחיד שלוקח את $\alpha\mapsto\alpha'$ ו־$\deg_{K,s}(\alpha)=|C_\alpha|$.
השיוויון השני נובע מכך שמתקיים $[L:K]=\deg_K(\alpha)$ ולכן $[L:K]_i=\frac{[L:K]}{[L:K]_s}=\frac{\deg_K(\alpha)}{\deg_{K,s}(\alpha)}=\deg_{K,i}(\alpha)$, ישירות מההגדרה, כאשר

$$\deg_{K,i}(\alpha)=1\iff\mathrm{char}(K)=0,\deg_{K,i}(\alpha)=p^n\iff\mathrm{char}(K)=p$$

□

למה 25.3 (כפליות הדרגות הפרידות והאי־פרידות במגדל הרחבות): לכל מגדל הרחבות סופיות $L/F/K$ מתקיים

1. $[L:K]_s = [L:F]_s \cdot [F:K]_s$
2. $[L:K]_i = [L:F]_i \cdot [F:K]_i$

הוכחה: נשים לב שמספיק להוכיח את הראשון כי מכפליות הדרגה אוטומטית נקבל את השני.
היות ו־$\left|\mathrm{Hom}_K\left(L,\overline{K}\right)\right| = [L:K]_s$, לכל $\sigma : L \hookrightarrow \overline{K}$ נגדיר צמצום $\sigma|_F : F \hookrightarrow \overline{K}$ וזה נותן לנו העתקה

$$\lambda : \mathrm{Hom}_K\left(L,\overline{K}\right) \to \mathrm{Hom}_K\left(F,\overline{K}\right)$$

ניקח $\tau \in \mathrm{Hom}_K\left(F,\overline{K}\right)$ ונחשב את גודל הסיב $\lambda^{-1}(\tau)$ כקבוצות: נזהה את F עם $\sigma(F)$ ואז $\overline{K} = \overline{K}$ (כי זה סגור אלגברי גם של כל הרחבה) ואז הסיב נהיה איזומורפי ל־$\mathrm{Hom}_F\left(L,\overline{K}\right)$.
מכאן, בכל סיב של λ יש בדיוק $\left|\mathrm{Hom}_F\left(L,\overline{K}\right)\right| = [L:F]_s$ איברים ולכן

$$[L:K]_s = \left|\mathrm{Hom}_K\left(L,\overline{K}\right)\right| = \underbrace{\left|\mathrm{Hom}_F\left(L,\overline{K}\right)\right|}_{=[L:F]_s} \cdot [L:F]_s$$

□

מסקנה 25.1: לכל הרחבה סופית L/K, $[L:K]_i = 1$ אם $\mathrm{char}(K) = 0$ ו־$[L:K]_i \in p^{\mathbb{N}}$ אם $\mathrm{char}(K) = p > 0$.

הוכחה: זה נובע ישירות מכך שכל הרחבה סופית היא מגדל של הרחבות פרימיטיביות: כי אם $L = K(\alpha_1, \cdots, \alpha_n)$ אז

$$K = K_0 \subset K_1 = K_0(\alpha_1) \subset \cdots$$

ואז מהלמה לעיל

$$[L:K]_i = [L:K_{n-1}] \cdot [K_{n-1}:K_{n-2}]_i \cdot \cdots \cdot [K_1:K_0]_i$$

כל אחד מהם או 1 או p^n ולכן גם המכפלה שלהם. □

הגדרה 25.3 (הרחבה פרידה): הרחבה אלגברית L/K נקראת **הרחבה פרידה (ספרבילית)** אם לכל $\alpha \in L$ היינו פריד מעל L.
נובע ישירות מהגדרה ש־L/K היא הרחבה פרידה אם ורק אם כל תת־הרחבה סופית היא הרחבה פרידה.

משפט 25.1: עבור הרחבה סופית L/K הבאים שקולים:

1. L/K הרחבה פרידה
2. $L = K(\alpha_1, \cdots \alpha_n)$ כך ש־$\alpha_1, \cdots, \alpha_n$ פרידים מעל K
3. $[L:K]_s = [L:K]$
4. $[L:K]_i = 1$

הוכחה: ראשית, בבירור $4 \Rightarrow 3 \Rightarrow 2 \Rightarrow 1$ ישירות מהגדרה וגם $4 \Longleftrightarrow 3$ מהגדרת הדרגה.
$4 \Rightarrow 2$: נגדיר $K_j = K\left(\alpha_1, \cdots \alpha_j\right)$ כך ש־$K = K_0$ ו־$L = K_n$ תמשיכי!

□

26 הרצאה 15 – 20/05

26.1 הרחבות פרידות (ספרביליות) – המשך

תשלימי

26.2 שדות פרפקטים (Perfect Fields)

הגדרה 26.1 (שדה פרפקט): שדה K נקרא **פרפקט** אם $\mathrm{char}(K)=0$ או $\mathrm{char}(K)=p$ ו־$K=K^p$ (זה שקול לכך ש־Fr_p הוא אוטומורפיזם ו־$K=K^p$).

הערה: במציין p יש סדרה $K^{p^2}\simeq K^p\overset{\mathrm{Fr}}{\simeq}K\simeq K^{\frac{1}{p}}$ ... ולכן $K^{p^2}\subseteq K\subseteq K^{\frac{1}{p}}\subseteq ....$

דוגמה 26.1: כל שדה סופי (כי Fr זה אנדומורפיזם ומשיקולי סדר נקבל שהוא גם על וגם מתקיים $\{x\mid x^{p^n}=x\}=\mathbb{F}_{p^n}\subseteq K$, נקודות השבת של פרובניוס).

אלדוגמה 26.1: K במציין p, נסתכל על $K[t]$ אבל הוא לא שדה פרפקטי כי $t\notin K^p$.

משפט 26.1: יהי K שדה אזי

1. K פרפקטי אם ורק אם כל הרחבה אלגברית L/K היא ספרבילית
2. אם K פרפקטי אזי לכל הרחבה אלגברית L/K, L פרפקטי

הוכחה:

1. אפשר להניח ש־$\mathrm{char}(K)=p\neq 0$ כי בשדה ממציין 0 כל הרחבה היא ספרבילית.
נניח כי K לא פרפקטי ולכן קיים $a\in K/K^p$ ולכן $a^{\frac{1}{p}}=\alpha\in\overline{K}\setminus K$, נסמן $L=K(\alpha)$ ו־$t^p-a=(t^p-a^p)\mid f_{\alpha/K}$ ולכן $f_{\alpha/K}=(t-\alpha)^m$ עבור $1<m\leq p$ (כי $\alpha\notin K$) ולכן α אי־פריד ונקבל ש־$[L:K]_i=m>1$ ואפילו $m=p$ אבל אז ההרחבה לא פרידה.
בכיוון השני, נניח שקיימת הרחבה L/K אי־פרידה וזה קורה אם ורק אם קיים $\alpha\in L$ שהוא אי־פריד מעל K וניקח $K[t]\ni f=f_{\alpha/K}$ הפולינום המינימלי. לפי משפט קודם, $f=g(t^{p^n})$ כאשר g פריד ולכן $n>0$ $f=h^p$ עבור $h=\sum_{i=0}^m a_i^{\frac{1}{p}}t^i$, אבל f אי־פריק ב־$K[t]$ ולכן $a_i^{\frac{1}{p}}\notin K$ אבל אז $K^p\neq K$
2. נניח כי K פרפקטי ו־L/K אלגברית. אז לכל F/L אלגברית, F/K פרידה (פרפקטי => פרידה לפי (1)) ולכן F/L פרידה. אבל זה אומר שכל הרחבה של L היא פרידה ולפי (1) נקבל ש־L פרפקטי.

$\square$

הגדרה 26.2 (פרפקטיזציה): לכל שדה K במציין $p>0$ נגדיר **פרפקטיזציה** $K^{\frac{1}{p^\infty}}=\bigcup_{n\in\mathbb{N}}K^{\frac{1}{p^n}}$.

הגדרה 26.3 (p-רנק): לכל שדה K במציין $p>0$ נגדיר **$[p]$־רנק** על־ידי $0[K:K^p]=p^n$ (אולי ∞)

תרגיל 26.1:

1. להראות ש־$K^{\frac{1}{p^\infty}}$ הוא השדה פרפקט המינימלי המכיל את K
2. להראות שמתקיים $\left[K^{p^l}:K^{p^{l+1}}\right]=\left[K^{\frac{1}{p}}:K\right]=[K:K^p]$ לכל $l\in\mathbb{Z}$ (רמז: פרובניוס)
3. להראות שאם K/K^p סופי אז $[K:K^p]_s=1$ ולכן p־רנק הוא מספר טבעי

27 תרגול 7 – 22/05

27.1 משהו

תשלימי

28 תרגיל 6

28.1 טריקים

תשלימי

28.2 מסקנות

תשלימי

29 הרצאה 16 – 26/05

29.1 הרחבות אי־פרידות בטהרה (purely inseparable)

29.2 תורת גלואה

29.3 התאמת גלואה

30 הרצאה 17 – 27/05

30.1 התאמת גלואה – המשך

31 תרגול 8 – 28/05

31.1 משהו

32 תרגיל 7

32.1 טריקים

32.2 מסקנות

33 הרצאה 18 – 03/06

33.1 המשפט היסודי של תורת גלואה

34 תרגול 9 – 04/06

34.1 פולינומים סימטריים

הגדרה 34.1 (פולינומים סימטריים אלמנטריים): יהי F שדה ו־$L = F(t_1, \cdots, t_n)$, יש פעולה $L \circlearrowleft S_n$ על־ידי $\sigma \cdot t_i = t_{\sigma(i)},\ \sigma \cdot$
.$P(t_1, \cdots, t_n) = P\left(t_{\sigma(1), \cdots \sigma(n)}\right)$
נסמן ב־$K = L^{S_n}$ את שדה נקודות השבת של הפעולה, ובהרצאה ראינו שמתקיים $\mathrm{Gal}(L/K) \simeq S_n$.
נגדיר $f(x) = \prod_{i=1}^{n}(x - t_i) \in L[x]$ ונכתוב $f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$, כאשר $-s_1, s_2, (-1)^n s_n$ הם מקדמי f, ומתקיים

$$-s_1 = -t_1 - t_2 - \cdots - t_n \Rightarrow s_1 = \sum_{i=1}^{n} t_i$$

$$s_2 = \sum_{1 \le i < j \le n} t_i t_j,\ s_k = \sum_{1 \le i_1 < i_2 < \cdots i_k \le n} t_i \cdots t_k$$

הביטויים $s_1, \cdots s_n$ נקראים **הפולינומים הסימטריים האלמנטריים (ל־n משתנים)** והם שייכים ל־L^{S_n} (הם רק משנים את סדר הגורמים אבל זה לא משנה את f).

טענה 34.1: K (שדה השבת של L תחת הפעולה של S_n מההגדרה לעיל) מקיים $L = F(s_1, \cdots, s_n)$.

הוכחה: את ההכלה $\supseteq$ כבר ראינו, עבור הכיוון השני: L הוא שדה פיצול של f מעל $F(s_1, \cdots, s_n)$ אז $[L : F(s_1, \cdots, s_n)] \le \deg(f)! = n!$ ומצד שני, $[L : F(s_1, \cdots, s_n)] = \underbrace{[L : K]}_{\substack{=n! \\ \text{ממשפט ארטין} \\ \text{וסדר החבורה } S_n}} \cdot [K : F(s_1, \cdots, s_n)]$ וביחד לאחר צמצום ב־$n!$ נקבל $[K : F(s_1, \cdots, s_n)] \le 1$ ולכן בהכרח מתקיים מהגדרת הדרגה $[K : F(s_1, \cdots, s_n)] = 1$. $\square$

נרצה להראות ש־$F(s_1, \cdots, s_n) \simeq F(x_1, \cdots, x_n)$ כאשר $x_i \mapsto s_i$ (הערה: חשוב איזומורפיזם ולא זהות, הדוגמה הכי טובה היא $F(x^2) \subseteq F(x)$ שהם איזומורפיים עם $y = x^2$ אבל הם לא זהים!), נראה זאת לא ישירות אלא באמצעות טענה על פולינומים.

משפט 34.1 (המשפט היסודי של הפולינומים הסימטריים): $F[t_1, \cdots t_n]^{S_n} = F[s_1, \cdots, s_n]$ ויש איזומורפיזם $F[x_1, \cdots x_n] \xrightarrow{\sim} F[s_1, \cdots, s_n]$ כך ש־$P(x_1, \cdots, x_n) \mapsto P(s_1, \cdots s_n)$.

הערה: זה יוביל אותנו להוכחה הרצוייה עם מעבר לשדה שברים.

את ההוכחה של המשפט נחלק לשניים: נראה את "יש איזומורפיזם" ואז נראה את המיפוי, לשם כך נצטרך כמה הגדרות וטענות נוספות:
איברי $F[t_1, \cdots t_n]^{S_n}$ נקראים פולינומים סימטריים. בפולינום סימטרי, אם אחד המונומים הוא $t_1^{a_1} \cdots t_n^{a_n}$ אז גם $t_{\sigma(1)}^{a_1} \cdots t_{\sigma(n)}^{a_n}$ הוא מונום של אותו פולינום (זאת אומרת, אם ניקח את $f(t_1, t_2) = t_1 + t_1t_2^2 + \cdots$ יהיה סימטרי אם גם t_2 וגם $t_2t_1^2$ נמצאים ב־$\cdots$).

הגדרה 34.2 (הסדר הלקסיגורפי על המונומים): נתון על־ידי $t_1^{a_1} \cdot t_2^{a_2} \cdot \cdots \cdot t_n^{a_n} > t_1^{b_1} \cdot t_2^{b_2} \cdot \cdots \cdot t_n^{b_n}$ אם:
1. $a_1 + \cdots + a_n > b_1 + \cdots b_n$
2. $a_1 + \cdots + a_n = b_1 + \cdots b_n$ וגם ה־i הראשון כך ש־$a_i \ne b_i$ מקיים $a_i > b_i$

טענה 34.2 (תכונות הסדר הלקסיגורפי על המונומים):
1. אם $m_{,1}, m_2$ מונומים וגם $m_{1'}, m_{2'}$ מונומים כך ש־$m_1 > m_2$ וגם $m_{1'} > m_{2'}$ אז $m_1m_{1'} > m_2m_{2'}$
2. לכל מונום יש מספר סופי של מונומים שקטנים ממנו

מסקנה 34.1 (מתכונה 1): אם יש לנו קבוצת פולינומים $f_1, \cdots, f_k$ אז המונום המוביל של $f_1 \cdot \cdots \cdot f_k$ הוא מכפלת המונומים המובילים. בפרט, המונום המוביל של $s_1^{a_1} \cdot \cdots \cdot s_n^{a_n}$ הוא $t_1^{a_1+a_2+\cdots+a_n} \cdot t_2^{a_2+\cdots a_n} \cdot \cdots \cdot t_n^{a_n} = t_1^{a_1} \cdot (t_1t_2)^{a_2} \cdot (t_1t_2t_3)^{a_3} \cdot \cdots$.
לכן למונומים שונים ב־s_i־ים, במונחי ה־t_i־ים, יש מונומים מובילים שונים.
כמסקנה ישירה נקבל שאם $0 \ne P \in F[x_1, \cdots, x_n]$ אז $P(s_1, \cdots, s_n) \ne 0$ למה? כי P הוא צירוף לינארי לא טריוויאלי של מונומים ב־x_i־ים, כשנציב את ה־s_i־ים נקבל צירוף לינארי לא טריוויאלי של מונומים ב־s_i־ים, מתוך אלו, כשנשכתב למונחי t_i־ים, רק לאחד יש דרגה מקסימלית במונחי t_i־ים והוא לא יכול להצטמצם עם שום דבר.
זה מביא לנו את "היש איזומורפיזם" מהמשפט היסודי.

דוגמה 34.1: ניקח $f_1 = t_1 + t_2^2,\ \ f_2 = t_1t_2 + t_2^2$. מהגדרת הסדר הלקסיגורפי, t_2^2 הוא מונום מוביל של f_1 ו־t_1t_2 הוא מונום מוביל של f_2.
אז $f_1f_2 = t_1^2t_2 + t_1t_2^2 + t_1t_2^3 + t_2^4$ והמונום המוביל יהיה $t_1t_2^3$.

כעת, בהינתן f פולינום סימטרי, אחנו רוצים להראות שקיים $p \in F[x_1, \cdots x_n]$ כך ש־$f = P(s_1, \cdots, s_n)$.
ניקח את המונום המוביל של f: $c \cdot t_1^{a_1} \cdot \cdots \cdot t_n^{a_n}$ ומכיוון ש־f סימטרי אז $a_1 \geq a_2 \geq \cdots \geq a_n$ (אם $a_i < a_{i+1}$ ל־i כלשהו, אז ניתן להחליף בין t_i לבין t_{i+1} ולקבל מונום גדול יותר, גם הוא ב־f). נשים לב שזה בידיוק המונום המוביל של $c \cdot s_1^{a_1-a_2} \cdot s_2^{a_2-a_3} \cdot \cdots \cdot s_n^{a_n}$ וזה פולינום סימטרי.
המונום המוביל של $f - c \cdot s_1^{a_1-a_2} \cdot s_2^{a_2-a_3} \cdot \cdots \cdot s_n^{a_n}$ קטן יותר.
אחרי מספר סופי של צעדים נגיע ל־0 (כי יש רק מספר סופי של מונומים שקטנים יותר מהמונום $c \cdot s_1^{a_1-a_2} \cdot s_2^{a_2-a_3} \cdot \cdots \cdot s_n^{a_n}$ וכל פעם אנחנו מקטינים ממש את המונום המוביל), ולכן כשנגיע ל־0 זה אומר שהבענו את f כצירוף לינארי של מונומים ב־$s_1, \cdots s_n$.

דוגמה 34.2: ניקח $f = t_1^2 + t_2^2$ ומהגדרת הסדר הלקסיגורפי נקבל ש־t_1^2 הוא מונום מוביל, ונכתוב את f כביטוי בפופלנומים סימטריים אלמנטריים.
בצעד הראשון, ניקח את $s_1^2 = (t_1 + t_2)^2 = t_1^2 + 2t_1t_2 + t_2^2$ ואז $f - s_1^2 = t_1^2 + t_2^2 - t_1^2 - 2t_1t_2 - t_2^2 = -2t_1t_2 = P_1$.
בצעד השני ניקח אז את $P_1 - 2s_2$ כאשר $2s_2 = 2\sum_{1 \leq i < j \leq 2} t_it_j = 2t_1t_2$ ואז $P_1 - 2s_2 = 2t_1t_2 - 2s_2 = 0$.
ולכן $f = s_1^2 - 2s_2$.

Norm, Trace 34.2

הגדרה 34.3 (עקבה ונורמה של הרחבה סופית): תהיי L/K הרכחבה סופית ו־$\alpha \in L$ ונגדיר העתקה $M_\alpha : L \to L$ אופרטור K־לינארי (ההרחבה סופית) על־ידי $M_\alpha(x) = \alpha \cdot x$.
נגדיר את **העקבה** על־ידי $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}(M_\alpha)$ ואת **הנורמה** נגדיר על־ידי $N_{L/K}(\alpha) = \det(M_\alpha)$.

דוגמה 34.3: $K = \mathbb{Q}, L = \mathbb{Q}\left(\sqrt{7}\right)$. בסיס ל־$L/K$ הוא למשל $\mathcal{B} = \left(b_1 = 1, b_2 = \sqrt{7}\right)$ ועבור $\alpha = x + y\sqrt{7}$ נקבל ש־M_α ביחס לבסיס $\mathcal{B}$ היא $\left[M_\alpha\right]_{\mathcal{B}} = \begin{bmatrix} x & 7y \\ y & x \end{bmatrix}$ כאשר $\alpha b_2 = 7y + x\sqrt{7}$ ואז

$$\mathrm{Tr}_{L/K}(\alpha) = 2x, N_{L/K}(\alpha) = \det\begin{bmatrix} x & 7y \\ y & x \end{bmatrix} = x^2 - 7y^2$$

טענה 34.3: אם $\alpha_1, \cdots \alpha_n$ הם הצמודים של α אזי

$$\mathrm{Tr}_{L/K}(\alpha) = \frac{[L:K]}{d}\sum_{i=1}^{d}\alpha_i,\ \ N_{L/K}(\alpha) = \left(\prod_{i=1}^{d}\alpha_i\right)^{\frac{[L:K]}{d}}$$

הוכחה: בתרגיל בית 9. $\square$

35 תרגיל 8

35.1 טריקים

35.2 מסקנות

36 שעת קבלה של גבע – 05/06

36.1 מסקנות

37 הרצאה 19 – 09/06

37.1 עוד עובדות על התאמת גלואה

37.2 שימושים של תורת גלואה

38 הרצאה 20 – 10/06

38.1 בניות של מצולעים משוכללים

39 תרגול 10 – 11/06

39.1 הדיסקרמיננטה

לאורך התרגול, F שדה, $\mathrm{char}(F) \neq 2, f \in F[x]$ ו־L שדה פיצול של f.
ב־L מתקיים $f(x) = \alpha \prod_{i=1}^{n}(x - \alpha_i)$ כאשר α הוא המקדם המוביל ו־α_i שורשים.
נניח לבנתיים ש־f אי־פריק ומתוקן, נסמן $G = \mathrm{Gal}(L/F)$ וראינו ש־G משתכנת ב־S_n על השורשים.
נסמן $\sigma \in G$ את $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ ונגדיר $R = \prod_{1 \le i < j \le n}\left(\alpha_i - \alpha_j\right) \in L$.

למה 39.1: $\sigma(R) = \pm R$ לכל $\sigma \in G$ ו־$\sigma(R) = R$ אם ורק אם $\sigma \in A_n$.

הוכחה: מתקיים

$$\sigma(R) = \prod_{1 \le i < j \le n}\left(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}\right)$$

שכן σ הוא אוטומורפיזם ולכן מכבד כפל.
יש כאן את אותם הגורמים כמו ב־R בפרט אולי לסימן ולכן $\sigma(R) = \pm R$, כאשר הסימן הוא $(-1)^{\ell}$ כאשר

$$\ell = |\{(i,j) \mid i < j \wedge \sigma(i) > \sigma(j)\}|$$

וידוע ש־$\mathrm{sgn}(\sigma) = (-1)^{\ell}$. □

הגדרה 39.1 (הדיסקרמיננטה): נסמן ב־$D_f = R^2$ את **הדיסקרמיננטה של f** ונשים לב ש־$\sigma\left(D_f\right) = D_f$ לכל $\sigma \in G$ ולכן $D_f \in L^G = F$.
במילים אחרות, D_f אינווריאנטי תחת כל אוטומורפיז

$$\sigma\left(D_f\right) = \sigma(R^2) = \sigma(R)^2 = (\pm R)^2 = R^2 = D_f \underset{\forall \sigma}{\Rightarrow} D_f \in L^G \underset{\text{מהתאמת גלואה}}{=} F$$

מסקנה 39.1: $G \subseteq A_n$ אם ורק אם D_f היא ריבוע ב־F (כלומר, יש לה שורש ב־F).

הוכחה: $\Leftarrow$ אם $G \subseteq A_n$ אז $\sigma(R) = R$ לכל $\sigma \in G$ ולכן $R \in L^G = F$ ולכן $R \in F$ הוא שורש ריבועי של D_f.
$\Longrightarrow$ אם ל־D_f יש שורש ב־F אז $R \in F = L^G$ אז $\sigma(R) = R$ לכל $\sigma \in G$ ולכן $\sigma \in A_n$ לכל $\sigma \in G$. □

הערה: זו תחת ההנחה ש־f פולינום מתוקן ו־$\mathrm{char}\, F \neq 2$. אם הוא לא היה מתוקן, היה אפשר לחלק בגורם המוביל ולקבל את אותה ההרחבה.

דוגמה 39.1:

$$f = (x - \alpha_1)(x - \alpha_2)$$

ולכן

$$R = \alpha_1 - \alpha_2, \; R^2 = \left(\alpha_1 - \alpha_2\right)^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2$$

אז נוכל לכתוב

$$f = x^2 - (\alpha_1 + \alpha_2)x - 2\alpha_1\alpha_2 \coloneqq x^2 + bx + c$$

כאשר

$$c = -2\alpha_1\alpha_2, b = -(\alpha_1 + \alpha_2)$$

ולכן

$$D_f = R^2 = (b^2 - 2c) - 2c = b^2 - 4c$$

אז אם D_f כן ריבוע ב־F אז $G \subseteq A_2$ אבל $A_2 = \{e\}$ ולכן f מתפצל כבר ב־F וקיבלנו קריטריון חדש לפריקות או אי־פריקות לפולינום מתוקן מדרגה 2.

מסקנה 39.2: $F\left(\sqrt{D_f}\right) \subseteq L$ אז $\mathrm{Gal}\left(L/F\left(\sqrt{D_f}\right)\right) = G \cap A_n$.

הוכחה: ישירות מ התאמת גלואה. □

כל זה היה תחת ההנחה ש־f מתוקן והוכחנו תכונות של D_f אבל אין לנו ביטוי יפה עבורו, אז המטרה שלנו זה להביע את D_f כפולינום במקדמי f.

הגדרה 39.2 (הרזולטנטה): יהיו $f,g\in F[x]$ הנתונים על־ידי $f=a_0x^n+a_1x^{n-1}+\cdots+a_n,\ \ g=b_0x^n+b_1x^{n-1}+\cdots+b_n$.
הרזולטנטה של f,g היא המטריצה הריבועית מסדר $m+n\times m+n$ (דרגות f,g בהתאמה) הנתונה על־ידי

$$\operatorname{Res}(f,g)=\det\begin{bmatrix}a_0&a_1&\cdots&a_n&0&\cdots&0\\0&a_0&a_1&\cdots&a_n&\cdots&0\\\vdots&\ddots&\ddots&\ddots&\ddots&\ddots&\vdots\\0&\cdots&0&a_0&a_1&\cdots&a_n\\b_0&b_1&\cdots&\cdots&b_m&\cdots&0\\\vdots&\ddots&\ddots&\ddots&\ddots&\ddots&\vdots\\0&\cdots&b_0&b_1&\cdots&\cdots&b_m\end{bmatrix}$$

למה 39.2: $\operatorname{Res}(f,g)=0$ אם ורק אם ל־f,g יש גורם משותף מדרגה חיובית.

הוכחה: נסמן $f=a_0x^n+\cdots+a_n,\ \ g=b_0x^m+\cdots+b_m$, אז

$$\operatorname{Res}(f,g)=\det\begin{bmatrix}a_0&a_1&\cdots&a_n&0&\cdots&0\\0&a_0&a_1&\cdots&a_n&\cdots&0\\\vdots&\ddots&\ddots&\ddots&\ddots&\ddots&\vdots\\0&\cdots&0&a_0&a_1&\cdots&a_n\\b_0&b_1&\cdots&\cdots&b_m&\cdots&0\\\vdots&\ddots&\ddots&\ddots&\ddots&\ddots&\vdots\\0&\cdots&b_0&b_1&\cdots&\cdots&b_m\end{bmatrix}$$

כמקודם זו מטריצה $m+n\times m+n$, כאשר $(a_0,a_1,\cdots,a_n,0\cdots,0)$ הוא וקטור המקדמים של $x^{n-1}f$.
וקטור המקדמים של $x^if=0\cdot x^{m+n}+\cdots+a_0x^{n+i}+\cdots+a_nx^i+0$ לכל $0<i\le m$ הוא $\left(0_{(m+n)},\cdots,0_{(n+i+1)},a_0,\cdots,a_n,0,\cdots,0\right)$
כאשר בסוגריים זה האינדקס ובאותו אופן גם עבור g בהצבה של b במקום a ו־$m+i+1$ במקום$n+i+1$.
$\operatorname{Res}(f,g)=0$ אם ורק אם יש תלות לינארית בין השורות וזה קורה אם ורק אם יש תלות בין הפולינומים

$$x^{m-1}\cdot f,x^{m-2}\cdot f,\cdots,f,x^{n-1}\cdot g,x^{n-2}\cdot g,\cdots,g$$

כלומר

$$0=\sum_{i=0}^{m-1}c_ix^if+\sum_{i=0}^{n-1}d_ix^ig=\left(\sum_{i=0}^{m-1}c_ix^i\right)f+\left(\sum_{i=0}^{n-1}d_ix^i\right)g\Rightarrow\left(\sum_{i=0}^{m-1}c_ix^i\right)f=\left(-\sum_{i=0}^{n-1}d_ix^i\right)g$$

זו כפולה משותפת של f,g מדרגה קטנה ממש מ־$m+n$ והיא שונה מ־0 אם ורק אם התלות לא טריוויאלית.
יש כפולה כזאת אם ורק אם ל־f,g יש גורם משותף מדרגה חיובית: אחרת, הם זרים, וכפולה משותפת חייבת להיות מכפלה של כל הגורמים האי־פריקים של שניהם ובפרט מדרגה של לפחות $m+n$. $\square$

דוגמה 39.2: $\operatorname{Res}(x+8,x^2+1)=0,\ \ \operatorname{Res}(x+1,2x+2)=\det\begin{bmatrix}1&1\\2&2\end{bmatrix}=0$

משפט 39.1: אם $f=a_0\prod_{i=1}^n(x-\alpha_i)$ ו־$g=b_0\prod_{i=1}^m(x-\beta_i)$ בשדה פיצול כלשהו, אז

$$\operatorname{Res}(f,g)=a_0^mb_0^n\prod_{i,j}\left(\alpha_i-\beta_j\right)=(-1)^{mn}b_0^n\prod_{i=1}^mf(\beta_i)=a_0^m\prod_{i=1}^ng(\alpha_i)$$

הוכחה: טכני מאוד. $\square$

הערה (תזכורת – נגזרת פורמלית וכלל לופיטל לנגזרת פורמלית):
עבור $f=a_0x^n+a_1x^{n-1}+\cdots+a_n$ מתקיים $f'=na_0x^{n(n-1)}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}$ כלל לופיטל לנגזרת פורמלית אומר שמתקיים $f'(\alpha_i)=\prod_{j\neq i}\left(\alpha_i-\alpha_j\right)$.

הגדרה 39.3: יהי $f=a_0x^n+\cdots+a_n$ ונסמן $n'=\deg(f')$, אז הדיסקרמיננטה של f היא

$$(-1)^{\frac{n(n-1)}{2}}\cdot a_0^{n-n'-2}\cdot\operatorname{Res}(f,f'):=D_f$$

למה 39.3: $D_f=a_0^{2n-2}\cdot\prod_{1\le i<j\le n}\left(\alpha_i-\alpha_j\right).$ ובפרט, גם ביחס להגדרה לעיל ו־D_f הוא ריבוע ב־F אם ורק אם $\operatorname{Gal}(L/F)\subseteq A_n$.

הוכחה: בתרגיל בית 10. $\square$

40 תרגיל 9

40.1 טריקים

40.2 מסקנות

41 הרצאה 21 – 16/06

41.1 סכומי גאוס

הערה: יש קצת מלחמה ולכן ההרצאות מכאן והלאה עוברות בזום ולא בצורה להיט. אז רוב התוכן מפה והלאה הוא תרגום של הרשומות של מיכאל והוספות מהספר/גוגל.

פרק 8.3 ברשומות של מיכאל.

יהי p ראשוני ונבחן את $L=\mathbb{Q}(\xi_p)$, ראינו שמתקיים $G=\mathrm{Gal}(L/\mathbb{Q})\simeq(\mathbb{Z}/p\mathbb{Z})^\times\simeq\mathbb{Z}/(p-1)\mathbb{Z}:=G^{ad}$.
ראינו שב־G יש תת־חבורה יחידה H מאינדקס 2, שסימנו אותה $H=G^2$ וזו ההרחבה של כל הריבועים ב־G.

מסקנה 41.1: לכל $d\mid p-1$ יש תת־חבורה יחידה מסדר d והיא $G^{\frac{p-1}{d}}$.

מסקנה 41.2: תת־חבורה מאינדקס 2 היא $G^2\leq G$ עבור $p\neq 2$.

דוגמה 41.1: עבור $p=5$ נקבל $G=\{1,2,3,4\},G^2=\{1,4\}$.

הגדרה 41.1 (סימן לז'נדר מודלו p): יהי p מספר ראשוני ($p\neq 2$) ו־$a\in\mathbb{Z}$, אז

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

ובסימונים של מיכאל

$$\left(\frac{a}{p}\right)=\begin{cases}1 & a\in G^2\\ -1 & a\in G\setminus G^2\\ 0 & \text{אחרת }(p\nmid a)\end{cases}$$

זה כמובן הומומורפיזם $G\mapsto G/H=\{\pm1\}$, בעצם $a\mapsto aH$ והגרעין הוא בידיוק G^2.

דוגמה 41.2: עבור $p=5$ מתקיים

a	$\left(\frac{a}{p}\right)$
0	0
1	1
2	-1
3	-1
4	1
5	0

תרגיל 41.1: ב־F_p להראות שמתקיים
1. $\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}$
2. $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

הוכחה:
1. זה מבחן אויילר.
2. נובע ישירות מסעיף א' וחוקי חזקות

$$\left(\frac{ab}{p}\right)=(ab)^{\frac{p-1}{2}}=a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

הגדרה 41.2 (סכום גאוס): $S_p=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\xi_p^a$.

משפט 41.1: יהי $p > 2$ ראשוני ו־$S = S_p$.
אם $p = 4n+1$ אז $S^2 = p$ ו־$\mathbb{Q}(\sqrt{p})$ היא תת־ההרחבה הריבועיות היחידה של $\mathbb{Q}(\xi_p)$.
אם $p = 4n+3$ אז $S^2 = -p$ ו־$\mathbb{Q}(\sqrt{-p})$ היא תת־ההרחבה הריבועית היחידה של $\mathbb{Q}(\xi_p)$.

הוכחה: מההגדרה של S_p, מספיק שנחשב את

$$(\star)\ S^2 = \left(\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\xi_p^a\right)^2 = \sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\xi^{a+b} = \sum_{a=0}^{p-1}c_a\xi_p^a = c_0 + \sum_{a=1}^{p-1}c_a\xi_p^a$$

הסדר סכימה עבר להיות מ־0 כי $\left(\frac{0}{p}\right) = 0$ לכל p שנבחר ונשים לב ש־$S^2 \in \mathbb{Q}$.
ננמק למה $S^2 \in \mathbb{Q}$: לכל $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ (בגלל התאמת גלואה) ונסתכל על האוטומורפיזם $\sigma_k : \xi \mapsto \xi^k$, נחשב

$$\sigma_k(S_p) = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\xi^{ak} \underset{b=ak \bmod p}{=} \sum_{b=1}^{p-1}\left(\frac{bk^{-1}}{p}\right)\xi^b = \left(\frac{k^{-1}}{p}\right)\sum_{b=1}^{p-1}\left(\frac{b}{p}\right)\xi^b \underset{\substack{k^{-1}\equiv k^{p-2} \bmod p \\ \text{ומהכפליות מהתרגיל}}}{=} \left(\frac{k}{p}\right)\sum_{b=1}^{p-1}\left(\frac{b}{p}\right)\xi^b = \left(\frac{k}{p}\right)S_p$$

ולכן

$$\sigma_k(S_p^2) = \left(\sigma_{k(S_p)}\right)^2 = \left(\left(\frac{k}{p}\right)S_k\right)^2 = \left(\frac{k}{p}\right)^2 S_p^2 \underset{\left(\frac{k}{p}\right)\in\{\pm1\}}{=} S_p^2$$

ולכן כל σ בחבורת גלואה משמרת את S_p^2 ולכן $S_p^2 \in \mathbb{Q}$.
נחזור להוכחה שלנו: ב־S יש לנו $\frac{p-1}{2}$ פעמים את 1 ו־$\frac{p-1}{2}$ פעמים את -1 ולכן כאשר נפתח סוגריים נקבל $\sum_{a=0}^{p-1} c_a = 0$.
נרצה לחשב את c_0, שהוא נתון על־ידי (פשוט מהגדרה/פתיחת סוגריים)

$$c_0 = \sum_{\substack{a+b=0 \bmod p \\ 1\le a,b\le p-1}}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

במילים אחרות,

$$a+b \equiv 0 (\bmod p) \iff b \equiv -a (\bmod p)$$

אז מכך ש־$b \in \{1, \cdots p-1\}$ נקבל ש־$-a \in \{1, \cdots p-1\}$ גם־כן, ואז

$$\begin{aligned} c_0 &= \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(-\frac{a}{p}\right) \underset{\text{מהכפליות מהתרגיל}}{=} \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{a}{p}\right)\left(-\frac{1}{p}\right) \\ &= \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)^2\left(-\frac{1}{p}\right) \underset{\left(\frac{a}{p}\right)^2=1\forall x\not\equiv0(\bmod p)}{=} \sum_{a=1}^{p-1}\left(-\frac{1}{p}\right) \\ &= (p-1)\left(\frac{-1}{p}\right) \underset{\text{מהתרגיל}}{=} (p-1)(-1)^{\frac{p-1}{2}} \end{aligned}$$

ולכן אם $p \equiv 1 \bmod 4$ אז $\left(-\frac{1}{p}\right) = 1$ ואם $p \equiv 3 \bmod 4$ אז $\left(-\frac{1}{p}\right) = -1$.
למה $p \bmod 4$? כי זו פשוט דרך מהירה לקבל האם החזקה תניב (-1) או 1, נחלק למקרים:
1. אם $p \equiv 1 \bmod 4$ אז $p = 4n+1$ ואז $\frac{p-1}{2} = 2n$ ואז יש לנו חזקה זוגית ונקבל $1 = (-1)^{2n}$
2. אם $p \equiv 3 \bmod 4$ אז $p = 4n+3$ ואז $\frac{p-1}{2} = 2n+1$ ואז יש לנו חזקה אי־זוגית ונקבל $(-1) = (-1)^{2n+1}$

עכשיו בחזרה ל־$(\star)$, ראינו כי $c_0 \in \mathbb{Q}$ וגם $S^2 \in \mathbb{Q}$ ולכן $c_0 + (p-1)c_1 = 0$ (כי $c_1 = \cdots c_{p-1}$) ולכן

$$-c_1 = \frac{c_0}{p-1} = (p-1)\frac{\left(\frac{-1}{p}\right)}{p-1} = \left(\frac{-1}{p}\right)$$

ובסך־הכל

$$S^2 = c_0 + \sum_{a=1}^{p-1} = (p-1)\left(\frac{-1}{p}\right) + \left(\frac{-1}{p}\right) = p\left(\frac{-1}{p}\right) = p(-1)^{\frac{p-1}{2}}$$

$\square$

הערה: ההוכחה לעיל אומרת גם ש־$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}(\xi_p), \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\xi_p)$ הן תתי־ההרחבות שראינו בהקדמה.

הערה: גאוס הוכיח שאם $\xi = e^{\frac{2\pi i}{p}}$ אזי $S_p = \sqrt{p}$ אם $p = 4n+1$ ו־$S_p = \sqrt{p}i = \sqrt{-p}$ כאשר $p = 4n+3$.

דוגמה 41.3: נוכיח כי $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
הטריק הוא לבטא את $\sqrt{2}$ באמצעות ξ_8: נחשב כמה תתי־הרחבות ריבועיות יש ב־$\mathbb{Q}(\xi_8/\mathbb{Q})$: מתקיים

$$G = \mathrm{Gal}(\xi_8/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^\times = \{1,3,5,7\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

ולכן יש לנו 3 תתי־הרחבות ריבועיות (כי יש 3 תתי־חבורות מאינדקס 2): נשים לב שמתקיים

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

$$\xi_8 + \xi_8^{-1} = \sqrt{2}$$

$$\xi_8 = e^{\frac{2\pi i}{8}} = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2}(1+i)$$

ולכן ההרחבות המדוברות הן $\mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}\left(\sqrt{-2}\right), \mathbb{Q}(i)$.
לכן אם $p \equiv \pm 1 \bmod 8$ אז $8 \mid p^2 - 1$ ולכן ב־$\mathbb{F}_{p^2}^\times$ (ציקלית!) קיים איבר ξ_8 מסדר 8 ולכן $\mathbb{F}_{p^2}(\xi_8) \subseteq \mathbb{F}_{p^2}$ וגם

$$\pm\sqrt{2} = \left(\sqrt{2}\right)^p = \xi_8^p + \xi_8^{-p}$$

41.2 הרחבות ציקליות ופתירות ברדיקלים

פרק 8.4 ברשומות של מיכאל.
נרצה לחקור הרחבות שניתן לבטא בעזרת $\sqrt[n]{a}$ (ושורשים של ארטין־שרייר במציין p).

הגדרה 41.3: במציין 0 נגדיר $\sqrt[\infty]{K}$ כשדה הקטן ביותר המכיל את K וסגור לשורש $\sqrt[n]{\cdot}$ כלשהו.

הערה: נראה כי $\sqrt[\infty]{\mathbb{Q}} \subsetneq \mathbb{Q}$.

הגדרה 41.4 (הרחבה ציקלית): הרחבת שדות L/K נקראת **ציקלית** אם זו הרחבת גלואה סופית ־$G = \mathrm{Gal}(L/K)$ היא ציקלית.

משפט 41.2: תהיי L/K הרחבת שדות מדרגה n ונניח כי $\mu_n \subset K$ ו־$n \in K^\times$.
אזי L/K היא הרחבה ציקלית מדרגה n אם ורק אם $L = K(\alpha)$ עבור $\alpha = a^{\frac{1}{n}}$ עבור $a \in K$.
הוכחה: $\Longrightarrow$ נניח כי $L = K\left(a^{\frac{1}{n}}\right)$, מלמה שראינו, L/K היא הרחבת גלואה ו־$G = \mathrm{Gal}(L/K)$ משוכן לתוך μ_n (שכן צמודים של $a^{\frac{1}{n}}$ הם מהצורה $a^{\frac{1}{n}}\xi^i$) ולכן $G = \mu_n$ היא ציקלית (כי $K(a^{\frac{1}{n}}/L$ פרידה ונורמלית ומשיוויון דרגות נקבל את השיוויון).
$\Longleftarrow$ נניח כי L/K הרחבת שדות ציקלית ולכן $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/n\mathbb{Z}$ ויהי σ יוצר של ההרחבה, עלינו למצוא יוצר $\alpha = a^{\frac{1}{n}}$ של L/K.
נסתכל על σ כאופרטור לינארי $\sigma : L \to L$: מכך ש־$\sigma^n = 1$, הפולינום המינימלי $f_\sigma(t) \mid t^n - 1$ ומההנחה $t^n - 1$ ספרבילי ומתפרק לחלוטין ב־K (מתקיים $t^n - 1 = \prod_{\xi_i \in \mu_n}(t - \xi_i)$).
מלינארית (כי הפולינום המינימלי מתפרק לגורמים לינאריים שונים) אנחנו יודעים ש־σ לכסין מעל K, ולכן קיים בסיס $\alpha_1, \cdots \alpha_n$ כך ש־$\sigma(\alpha_i) =$ $\xi_i\alpha_i$ עבור $\xi_i \in \mu_n$.
בטח שכל ξ_i מייצרים את μ_n: הם יוצרים תת־חבורה μ_m כך ש־$\sigma^m = 1$ ולכן $m = n$.
ולכן אם $\alpha = \alpha_1 \cdot \cdots \cdot \alpha_i$ אז $\sigma(\alpha) = \underbrace{(\xi_1 \cdot \cdots \cdot \xi_n)}_{\text{יוצר } \xi \in \mu_n}\alpha$.
מכאן נקבל $\sigma^j\alpha = \xi^j\alpha \neq \alpha$ עבור $0 < j < n$ ולכן ל־α יש n צמודים שונים ולכן $L = K(\alpha)$ מדרגה n ובנוסף $\sigma(\alpha^n) = \xi^n\alpha^n = \alpha^n$ ולכן $\alpha^n \in L^{\mathrm{Gal}(L/K)} \underset{\text{ארטין}}{=} K$. □

42 הרצאה 22 – 17/06

42.1 הרחבות ציקליות ופתירות ברדיקלים – המשך

הערה: אם $p=\mathrm{char}(K)$ אז ההרחבות המעניינות מדרגה p הן ארטין־שרייר שזה בעצם $L=K(\alpha)$ כאשר $\alpha^p-\alpha=a$, $\alpha=\wp$ (זה שורש ארטין־שרייר, שורש מסדר p שהוא פריד וברגע שמצאנו אחד מצאנו את כולם) ונוכיח שאלו כל ההרחבות הציקליות מדרגה p.
ב־$L=K\left(a^{\frac{1}{n}}\right)$, זה μ_n כפול שורש בודד $a^{\frac{1}{n}}=\mu_n\cdot\alpha$ וחבורת גלואה היא μ_n.
ב־$L=K(\alpha)$ זה $\alpha+\mathrm{Fr}_p$ עבור $\alpha=\wp$ וחבורת הגלואה היא $\mathbb{F}_p$.

משפט 42.1: אם $\mathrm{char}(K)=p$ ו־$[L:K]=p$ אז L/K ציקלית (גלואה) אם ורק אם $L=K(\alpha)$ כאשר $\alpha^p-\alpha-a=0$ לכל $a\in K$, זאת אומרת $L=K(\wp)$ (זאת־אומרת אם L/K היא הרחבת ארטין־שרייר).

הוכחה: $\Longleftarrow$ אם $L=K(\alpha)$ אז $\mathrm{Aut}(L/K)=\left(\mathbb{F}_p,+\right)$ גלואה כי יש שם p אוטומורפיזמים (ראינו כשדיברנו על הרחבות ארטין־שרייר). $\Longleftarrow$
נניח כי L/K ציקלית וניקח $0\neq\sigma\in\mathrm{Aut}(L/K)=\mathbb{Z}/p\mathbb{Z}$ שהוא כמובן יוצר.
נתבונן איך σ פועל $\sigma:L\to L$, מכך שהוא יוצר מתקיים $\sigma^p=\mathrm{Id}$ ולכן הפולינום האופייני של σ מחלק את t^p-1 $\underbrace{t^p-1}_{=(t-1)^p}\mid f_\sigma$.
לכן $\sigma-\mathrm{Id}$ נילפוטנטי ולא 0 וקיים $\beta\in L$ כך ש־$\sigma(\beta)\neq\beta$.
נסמן $b=\sigma(\beta)-\beta\neq0$ אבל $\sigma(b)-b=0$ ולכן $b\in L^\sigma=L^{\langle\sigma\rangle}=L^G=K$, כלומר $b\in K$ ($\beta\notin K$ כי $\sigma(\beta)\neq\beta$).
ניקח $\alpha=\frac{\beta}{b}$ ואז $\sigma(\alpha)-\alpha=\frac{\sigma(\beta)-\beta}{b}=1$.
לסיכום, הפעולה של G על $\left\{\alpha\overset{\sigma}{\mapsto}\alpha,1\overset{\sigma}{\mapsto}\alpha+2\cdots\right\}$, כלומר זו קבוצת הצמודים של α (הם הצמודים על המסלול $\sigma(\alpha)=\alpha+1$ כמו ארטין־שרייר).
ואז הפולינום המינימלי

$$f_\alpha=(t-\alpha)\cdot(t-\alpha-1)\cdot\dots\cdot(t-\alpha-p+1)$$

נסמן $a=\alpha^p-p$ ונטען ש־$f_\alpha=t^p-t-a$: נראה לשכל $i\in\mathbb{F}_p$ מתקיים $f(\alpha+i)=(\alpha+i)^p-(\alpha+i)-a=0$.
מתקיים

$$(\alpha+i)^p=\alpha^p+i^p\underset{i^p=i\left(i\in\mathbb{F}_p\text{ כי}\right)}{=}\alpha^p+i$$

ולכן נקבל

$$f(\alpha+i)=(\alpha+i)^p-(\alpha+i)=\alpha^p+i-\alpha-i-a=\alpha-\alpha-a\underset{a=\alpha^p-\alpha}{=}0$$

ולכן לכל $i\in\mathbb{F}_p$, $(\alpha+i)$ שורש של t^p-t-a.
השורשים של t^p-t-a זה כל α_i כך ש־$\alpha_i^p-\alpha=a$, זו בדיוק הקבוצה $\{\alpha,\alpha+1,\dots,\alpha+i-1\}$ ולכן יש p שורשים שונים ואז $f_\alpha=t^p-t-a$.
נסיק $a\in K$:

$$\sigma(a)=\sigma(\alpha^p-\alpha)=(\sigma(\alpha))^p-\sigma(\alpha)=(\alpha+1)^p-(\alpha+1)=\alpha^p-\alpha=a\in K$$

ובזאת סיימנו כי זו הרחבת ארטין־שרייר. $\square$

הערה: מספיק להגיד בהוכחה לעיל גלואה ולא ציקלית כי מהתאמת גלואה בכל־מקרה חבורת גלואה היא מסדר p ראשוני וזה יהיה ציקלית כך או כך.

הערה: יש משפט שמתאר הרחבות ציקליות מסדר p^n אבל הוא הרבה יותר כבד.

כעת, נרצה לחקור הרחבות פתירות (גלואה פתירות) והרחבות פתירות ברדיקלים ובעצם נוכיח שזה אותו הדבר.

הגדרה 42.1 (מגדל רדיקלי): הרחבה סופית L/K נקראת **מגדל רדיקלי** אם היא מתפצלת למגדל $L=K_n/K_{n-1}/\cdots/K_0=K$ כך ש־$K_{i+1}=K_i(\alpha)$ עבור α שורש יחידה $(\omega_n=\alpha)$ של $a^{\frac{1}{n}}$ עבור $n\in K^\times$ או $\alpha=\mathscr{P}(a)$ שורש ארטין־שרייר.

הגדרה 42.2 (סגור רדיקלי): $\sqrt[\infty]{K}=\bigcup_{L_i/K\text{ מגדל רדיקלי}}L_i$

תרגיל 42.1: $\sqrt[\infty]{K}$ הוא השדה הקטן ביותר שמכיל את K וסגור להוצאת שורש והוצאת שורש ארטין־שרייר ($\sqrt[n]{\cdot}$).

הגדרה 42.3 (הרחבה רדיקלית): הרחבה אלגברית L/K נקראת **רדיקלית** אם $L\subseteq\sqrt[\infty]{K}$.
כמובן, אם L/K סופית אז L/K רדיקלית אם רק אם $L\subseteq F$ כך ש־F/K מגדל רדיקלי (כי איחוד של כל המגדלים זה הסגור הרדיקלי)

הערה: יכול להיות ש־L/K לא מגדל בעצמה; למשל אם L/K הרחבה ריבועית ולא גלואה ו־$\mu_3 \subseteq K$ ו־$3 \neq \mathrm{char}(K)$.

תרגיל 42.2: אם $K \subseteq L \subseteq F$ מגדל ריבועי אז L/K מגדל ריבועי (גלואה וחבורת p).
רמז: צריך לקחת סגור גלואה שזה עדיין מגדל ריבועי ובסגור גלואה להשתמש (בתרגום משדות לחבורות) בטענה שאם יש לי $H \leq G$ חבורת p אז קיימת שרשרת $H_1 \subset H_2 \subset \cdots \subset G$ מאינדקס p.

43 תרגול 11 – 18/06

43.1 משהו

44 תרגיל 10

44.1 טריקים

44.2 מסקנות