מבנים אלגבריים 2, 80446 — סיכום

30 באפריל 2025

תוכן עניינים

1 הרצאה 1 – 24/03

1.1 מבוא להרחבת שדות

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

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

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

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

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

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

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

1.2 בניות

2 הרצאה 2 – 25/03

3 הרצאה 3 – 31/03

4 הרצאה 4 – 07/04

5 הרצאה 5 – 08/04

להשלים הקדמה

5.1 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 5.1 (תכולה): עבור פולינום $f(t)\in\mathbb{Z}[t]$ (תזכורת: $f(t)=\sum_{i=0}^{n}a_it^i$) נגדיר **תכולה** של f להיות

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

הגדרה 5.2 (פולינום פרימיטיבי): פולינום $f(t)\in\mathbb{Z}[t]$ יקרא **פרימיטיבי** אם $\mathrm{cont}(f)=1$.

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

משפט 5.1 (למת גאוס הראשונה): אם $f,g\in\mathbb{Z}[t]$ אזי $\mathrm{cont}(fg)=\mathrm{cont}(f)\cdot\mathrm{cont}(g)$. בפרט, fg פרימיטיבי אם ורק אם f ו־g פרימיטיביים.

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

נניח שלא ולכן קיים $p\in\mathbb{N}$ ראשוני כך שמתקיים $p\mid\mathrm{cont}(f_0\cdot g_0)$, אבל $f_0=\sum_{i=0}^{n}a_it^i,g_0=\sum_{j=0}^{m}b_jt^j$ הם פולינומים פרימיטיביים (ולכן לא כל a_i,b_j מתחלקים ב־p) ולכן נוכל לבחור m,n מינימליים כך ש־$p\nmid a_n$ ו־$p\nmid b_m$.

נסתכל על המקדם של t^{m+n} של $c=\sum_{k=0}^{m+n}a_kb_{m+n-k}$ ב־$f_0\cdot g_0$, נכתוב אותו מפרושות:

$$\underbrace{a_0b_{m+n}+...+a_{n-1}b_{m+1}}_{\text{מתחלקים ב־}p\text{ כי } p|a_k \text{ לכל } k<n}+a_nb_m+\underbrace{a_{n+1}b_{m-1}+...+a_{m+n}+b_0}_{\text{מתחלקים ב־}p\text{ כי } p|b_k \text{ לכל } k>n}$$

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

מסקנה 5.1: כל ראשוני $p\in\mathbb{Z}$ ראשוני ב־$\mathbb{Z}[t]$ (לא ראינו בהרצאה, מסקנה 1.2.5 בסיכום של מיכאל).

הוכחה: נשים לב ש־$\mathbb{Z}[t]^x=\mathbb{Z}^x\not\ni p$ ולכן p מחלק פולינום $h\in\mathbb{Z}[t]$ אם ורק אם $p\mid\mathrm{cont}(h)$.
אם $p\mid f\cdot g$ אז מלמת גאוס הראשונה נובע $p\mid\mathrm{cont}(f)\cdot\mathrm{cont}(g)$ ולכן $p\mid f$ או $p\mid g$. $\square$

משפט 5.2 (למת גאוס השנייה): יהי $f\in\mathbb{Z}[t]$ פולינום לא קבוע. נזכור כי $\mathbb{Q}[t]$ הוא $\mathrm{Frac}(\mathbb{Z})$, שדה השברים של $\mathbb{Z}[t]$. אז

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

הוכחה:

1. ניקח את הפירוק $f=g\cdot h$ עבור $g,h\in\mathbb{Q}[t]$ וניקח $m,n\in\mathbb{Z}>0$ כך ש־$m\cdot g,n\cdot h\in\mathbb{Z}[t]$ ואז נקבל פירוק $m\cdot n\cdot f=m\cdot g\cdot n\cdot h$.
נסמן $\ell=\mathrm{cont}(f),\alpha=\mathrm{cont}(m\cdot g),\beta=\mathrm{cont}(n\cdot h)$. מלמת גאוס הראשונה נקבל עם כפליות התכולה
$$\mathrm{cont}(m\cdot n\cdot f)=m\cdot n\cdot\ell=\alpha\cdot\beta=\mathrm{cont}(m\cdot g\cdot n\cdot h)$$
אם כך, ניקח $m\cdot n\cdot f=m\cdot g\cdot n\cdot h$ ונחלק ב־$\alpha\beta=m\cdot n\cdot\ell$ 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 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 $g=\sum_{i=1}^{n}a_it^i,h=\sum_{j=1}^{m}b_jt^j$. היות ו־$f$ מתוקן נובע כי $a_nb_m=1$ ולכן בהכרח $a_n=b_m=1$, ו־$c\cdot g,c^{-1}\cdot h$ עדיין פולינומים מתוקנים ולכן $c=\pm1$ ולכן $g,h\in\mathbb{Z}[t]$.
3. (הוכח בהרצאה 6)

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

פרימיטיבי.

נניח ש־f פריק ב־$\mathbb{Q}[t]$ ולכן יש $f = g \cdot h$ כך ש־$\deg(g), \deg(h) > 0$ ולכן מ־(1) לעיל נקבל $f = c \cdot g \cdot c^{-1} \cdot h$ עם דרגות גדולות מ־0 ב־$\mathbb{Z}[t]$ משמע הוא פריק בו, וזאת סתירה.

$\Longleftarrow$ 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 5.2: $\mathbb{Z}[t]$ 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).

6 הרצאה 6 – 21/04

6.1 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 6.1: 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 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 6.1: $\mathbb{F}_p[t] = \mathbb{Z}[t]/p\mathbb{Z}[t]$

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 $\operatorname{Ker}(\varphi) = \left\{ f(t) \in \mathbb{Z}[t] \mid \varphi(f) = 0 \in \mathbb{F}_p[t] \right\}$ אלו כל הפולינומים שבמודלו p הם מתאפסים משמע מתחלקים ב־p ולכן $\operatorname{Ker}(\varphi) = p\mathbb{Z}[t]$. ממשפט האיזומורפיזם הראשון לחוגים נקבל

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

$\square$

משפט 6.1 (קריטריון אייזנשטיין): נניח ש־$f = \sum_{i=0}^n a_i t^i \ni \mathbb{Z}[t]$ ו־$p \in \mathbb{N}$ ראשוני כך שמתקיימים הבאים
1. $p \nmid a_n$
2. $p \mid a_i$ לכל $0 \le i < n$
3. $p^2 \nmid a_0$

אז f אי־פריק.

הוכחה: נניח בשלילה שלא כך, ולכן מהלמות של גאוס נובע שמתקיים $f = g \cdot h = \sum_{j=1}^m b_j t^j \sum_{k=1}^l c_k^{t^k}$.
היות ו־$a_0 = b_0 c_0$ ו־$p \mid a_0$ נובע כי $p \mid b_0$ או $p \mid c_0$. בלי הגבת הכללית, נניח כי $p \mid b_0$ ו־$p \nmid c_0$ (שכן $p \mid a_0$ אבל $p \nmid a_0$ ולכן לא ניתן שגם $p \mid b_0$ וגם $p \mid c_0$).
ניקח את ה־$i \le m$ הקטן ביותר כך ש־$p \mid b_i$ שקיים מהיות $b_m c_l = a_n$ ולכן $p \nmid b_m$.
כעת, בביטוי $a_i = b_i c_0 + \underbrace{b_{i-1} c_1 + \ldots + b_0 c_i}_{\text{מתחלקים ב־p}}$ אבל אז $p \nmid a_i$ וזאת סתירה.

אז f לא מתפרק לגורמים מדרגה גדולה מ־0 ואז f אי־פריק ב־$\mathbb{Z}[t]$ ומהלמה של גאוס נובע כי הוא גם אי־פריק ב־$\mathbb{Q}[t]$. $\square$

דוגמה 6.1: 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 6.1: $x^2 - m^2, x^2 + 4$ תמיד פריקים: אם $p \mid m^2$ אז גם $p \mid m$.

הגדרה 6.1 (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 הפרמטיביים מסדר n. משמע $\Phi_n(X) = \prod_\omega (X - \omega)$ כאשר ω עובר על כל השורשים הפרימיטיביים מסדר n.

דוגמה 6.2:

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

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

למה 6.2: לכל $p \in \mathbb{N}$, הפולינום הציקלוטומי $\Phi_p(t) = \frac{t^p-1}{t-1}$ אי־פריק מעל $\mathbb{Q}$.

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

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

אז $f(x)$ אי־פריק לפי קריטריון אייזנשטיין שכן p מקדם חופשי מתוקן ו־$p \mid \binom{p}{i}$ לכל $0 < i < p$.
אם $\Phi_p(t)$ לא אי־פריק, אז קיימים $\Phi_p(t) = g(t)\cdot h(t) = g(x+1)\cdot h(x+1)$ וזאת סתירה. $\square$

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

6.2 סגור אלגברי

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

הגדרה 6.2 (שדה סגור אלגברי)**:** שדה K נקרא **שדה סגור אלגברית** אם לכל פולינום לא קבוע מעל K יש שורש ב־K.

הגדרה 6.3 (פולינום מתפצל לחלוטין)**:** נגיד K שדה, נגיד כי $f \in K[t]$ **פולינום מתפצל לחלוטין** אם הוא מתפרק לגורמים לינאריים.
משמע, $f = c\prod_{i=1}^{\deg(f)}(t-a_i)$ כאשר $c \in K^x$ ו־$a_i \in K$ לכל i.

למה 6.3: עבור שדה K הבאים שקולים

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

הוכחה: $(3) \iff (2)$ כי תמיד יש פירוק לפולינומים אי־פריקים.
$(2) \Longleftarrow (1)$: אם יש פירוק מלא, נובע מהגדרה שיש לי שורש.
$(1) \Longrightarrow (2)$: נובע שלכל $f = g(t-a)$ יש פירוק כאשר $\deg g < \deg f$ ומסיימים את הטיעון עם אינדוקציה על $\deg(f)$.
$(4) \Longleftarrow (1)$: אם קיימת הרחבה אלגברית לא טריוויאלית L/K ניקבל $\alpha \in L \setminus K$ ואז הפולינום $f_{\alpha/K}$ אי־פריק מדרגה $1 < [K(\alpha) : K]$.
$(1) \Longrightarrow (4)$: אם f אי־פריק ו־$\deg(f) > 1$ נגדיר $L = K[t]/(f)$ ו־$[L : K] = \deg(f) > 1$. $\square$

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

משפט 6.2 (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 6.1:

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

הוכחה: נשים לב $2 \iff 1$ ברור, ולכן מספיק שנוכיח רק את 1: נשים לב $f = \overline{f} = \mathbb{R}[t] \subseteq \mathbb{C}[t]$ ולכן ההצמדה רק מחליפה את השורשים של $f = c\prod_{i=1}^{n}(t-a_i)$ (נשים לב שההצמדה היא בעצם תמורה, כי ההצמדה רק יכולה לשנות מיקום לשורשים אך לא את השורשים עצמם).
לטובת מי מבנינו שמתעב מרוכבים, ניזכר במספר עובדות קצרות. הצמוד המרוכב של מספר ממשי הוא ממשי. כמו־כן, הצמוד המרוכב סגור לחיבור וכפל, כלומר הצמוד של מכפלה שווה למכפלה של צמודים, ואותו הדבר לחיבור. המשמעות היא שאם $f \in \mathbb{R}[x]$ פולינום ממשי, אז כפולינום מעל המרוכבים נקבל ש־$f = \overline{f}$. בשל סגירות זו, גם בפירוק לגורמים לינאריים מעל המרוכבים מתקיים

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

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

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

כלומר f הוא מכפלה של גורמים לינאריים ממשיים ושל

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

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

מסקנה 6.2: נניח כי L/K הרחבה, L סגור אלגברית ונגדיר $F = \{\alpha \in L \mid K \text{ אלגברי מעל } \alpha\}$.
אז F סגור אלגברית וזה נקרא **הסגור האלגברי** (Algebraic closure) של K ב־L.

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

דוגמה 6.3: $\overline{\mathbb{Q}}$ הוא הסגור האלגברי של $\mathbb{Q}$ ולכן גם סגור אלגברית מעל $\mathbb{Q}$.

7 הרצאה 7 – 22/04

הרצאה 8 – 28/04

9 הרצאה 9 – 29/04

Waka, doing some stuff 10

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

אלדוגמה 10.1 (לא הומומורפיזם של חוגים): $\varphi : 0 \to \mathbb{Z}$ הוא לא הומומורפיזם של חוגים.

דוגמה 10.2 (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 10.2 (לא שדות): $0, \mathbb{F}[X], M_{n\times n}(\mathbb{F})$

הגדרה 10.1 (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 10.2 (אי־פריק): R תחום שלמות ו־$0 \neq r \in R$. r נקרא **אי־פריק (irreducible)** אם איננו הפיך ואין לו פריק אמיתי. משמע, אם מתוך $r = ab$ נובע ש־$a \in R^x$ או $b \in R^x$ (משמע $r \sim a$ או $r \sim b$).

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 10.3 (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

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

הגדרה 10.4 (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 10.1 (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 מפרושות:

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

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

מסקנה 10.1: כל ראשוני $p \in \mathbb{Z}$ ראשוני ב־$\mathbb{Z}[t]$ (לא ראינו בהרצאה, מסקנה 1.2.5 בסיכום של מיכאל).

הוכחה: נשים לב ש־$\mathbb{Z}[t]^x = \mathbb{Z}^x \not\ni p$ 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 $p \mid g$. □

משפט 10.2 (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 $0 \neq c \in \mathbb{Q}^x$ כך ש־$c \cdot g, c^{-1} \cdot h \in \mathbb{Z}[t]$ ולכן $f = (c \cdot g) \cdot (c^{-1} \cdot h)$ פירוק ב־$\mathbb{Z}[t]$
2. אם f פולינום מתוקן ו־$f = g \cdot h \in \mathbb{Q}[t]$ פירוק מתוקן (דהיינו f, g מתוקנים) אזי $g, h \in \mathbb{Z}[t]$
3. אם f פולינום אי־פריק ב־$\mathbb{Z}[t]$ אם ורק אם f פרימטיבי ואי־פריק ב־$\mathbb{Q}[t]$

הוכחה:

1. ניקח את הפירוק $f = g \cdot h$ עבור $g, h \in \mathbb{Q}[t]$ וניקח $m, n \in \mathbb{Z}$ כך ש־$0 < m, n$ כך ש־$m \cdot g, n \cdot h \in \mathbb{Z}[t]$ ואז נקבל פירוק $m \cdot n \cdot f = m \cdot g \cdot n \cdot h$.
נסמן $\ell = \operatorname{cont}(f), \alpha = \operatorname{cont}(m \cdot g), \beta = \operatorname{cont}(n \cdot h)$. 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 ש־$c \cdot g \cdot c^{-1} \cdot h \in \mathbb{Z}[t]$ כך ש־$f = c \cdot g \cdot c^{-1} \cdot h$.
נסמן $g = \sum_{i=1}^{n} a_i t^i, h = \sum_{j=1}^{m} b_j t^j$. היות ו־$f$ מתוקן נובע כי $a_n b_m = 1$ ולכן בהכרח $a_n = b_m = 1$, ו־$c \cdot g, c^{-1} \cdot h$ עדיין פולינומים מתוקנים ולכן $c = \pm 1$ ולכן $g, h \in \mathbb{Z}[t]$.
3. (הוכח בהרצאה 6)
$\Longleftarrow$ נניח כי f אי־פריק ב־$\mathbb{Z}[t]$ ולכן $f = \operatorname{cont}(f) \cdot \frac{f}{\operatorname{cont}(f)}$ פירוק טריוויאלי ונשים לב $\deg\left(\frac{f}{\operatorname{cont}(f)}\right) > 0$ 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.
$\Longrightarrow$ בכיוון השני, נניח ש־f פריק ב־$\mathbb{Z}[t]$ ולכן $f = g \cdot h$ עם g, h לא הפיכים. יש 2 מקרים אפשריים:
   1. אם $\deg(f), \deg(g) > 0$ ואז נובע כי f פריק ב־$\mathbb{Q}[t]$ על־ידי פירוק זה וזאת סתירה
   2. בלי הגבלת הכלליות $\deg(h) = 0, \deg(g) > 0$ ולכן $1 < h \in \mathbb{Z}_+$ אבל אז f לא פרימיטיבי וזאת שוב סתירה

□

מסקנה 10.2: $\mathbb{Z}[t]$ הוא חוג פריקות יחידה והראשוניים שלו הם הפולינומים פרמיטיביים 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).

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 10.1: 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 פריק ב־$\mathbb{Q}[t]$

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

תרגיל 10.1: $\mathbb{F}_p[t] = \mathbb{Z}[t]/p\mathbb{Z}[t]$

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 $\operatorname{Ker}(\varphi) = \left\{ f(t) \in \mathbb{Z}[t] \mid \varphi(f) = 0 \in \mathbb{F}_p[t] \right\}$ אלו כל הפולינומים שבמודלו p הם מתאפסים משמע מתחלקים ב־p ולכן $\operatorname{Ker}(\varphi) = p\mathbb{Z}[t]$. ממשפט האיזומורפיזם הראשון לחוגים נקבל

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

□

משפט 10.3 (קריטריון אייזנשטיין): נניח ש־$\mathbb{Z}[t] \ni f = \sum_{i=0}^{n} a_i t^i$ ו־$p \in \mathbb{N}$ ראשוני כך שמתקיימים הבאים
1. $p \nmid a_n$
2. $p \mid a_i$ לכל $0 \leq i < n$
3. $p^2 \nmid a_0$

אז f אי־פריק.

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

דוגמה 10.3: 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 10.3: $x^2 - m^2, x^2 + 4$ תמיד פריקים: אם $p \mid m^2$ אז גם $p \mid m$.

הגדרה 10.5 (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 10.4:

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

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

למה 10.2: לכל $p \in \mathbb{N}$, הפולינום הציקלוטומי $\Phi_p(t) = \frac{t^p-1}{t-1}$ אי־פריק מעל $\mathbb{Q}$.

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

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

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.

הגדרה 10.6 (שדה סגור אלגברי): שדה K נקרא **שדה סגור אלגברית** אם לכל פולינום לא קבוע מעל K יש שורש ב־K.

הגדרה 10.7 (פולינום מתפצל לחלוטין): נגיד K שדה, נגיד כי $f \in K[t]$ **פולינום מתפצל לחלוטין** אם הוא מתפרק לגורמים לינאריים.
משמע, $f = c \prod_{i=1}^{\deg(f)} (t - a_i)$ כאשר $c \in K^x$ ו־$a_i \in K$ לכל i.

למה 10.3: 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 טריוואליות

הוכחה: $(3) \iff (2)$ כי תמיד יש פירוק לפולינומים אי־פריקים.
$(2) \Longleftarrow (1)$: אם יש פירוק מלא, נובע מהגדרה שיש לי שורש.
$(1) \Longrightarrow (2)$: נובע שלכל $f = g(t-a)$ יש פירוק כאשר $\deg g < \deg f$ ומסיימים את הטיעון עם אינדוקציה על $\deg(f)$.
$(4) \Longleftarrow (1)$: אם קיימת הרחבה אלגברית לא טריוויאלית L/K ניקבל $\alpha \in L \setminus K$ ואז הפולינום $f_{\alpha/K}$ אי־פריק מדרגה $1 < [K(\alpha) : K]$.
$(1) \Longrightarrow (4)$: אם f אי־פריק ו־$\deg(f) > 1$ נגדיר $L = K[t]/(f)$ ו־$[L : K] = \deg(f) > 1$. $\square$

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

משפט 10.4 (המשפט היסודי של האלגברה): $\mathbb{C}$ סגור אלגברית.

מסקנה 10.3:

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

הוכחה: נשים לב $2 \iff 1$ ברור, ולכן מספיק שנוכיח רק את 1: נשים לב $f = \overline{f} = \mathbb{R}[t] \subseteq \mathbb{C}[t]$ ולכן ההצמדה רק מחליפה את השורשים של $f = c\prod_{i=1}^{n}(t-a_i)$ (נשים לב שההצמדה היא בעצם תמורה, כי ההצמדה רק יכולה לשנות מיקום לשורשים אך לא את השורשים עצמם).
לטובת מי מבנינו שמתעב מרוכבים, ניזכר במספר עובדות קצרות. הצמוד המרוכב של מספר ממשי הוא ממשי. כמו־כן, הצמוד המרוכב סגור לחיבור וכפל, כלומר הצמוד של מכפלה שווה למכפלה של צמודים, ואותו הדבר לחיבור. המשמעות היא שאם $f \in \mathbb{R}[x]$ פולינום ממשי, אז כפולינום מעל המרוכבים נקבל ש־$f = \overline{f}$. בשל סגירות זו, גם בפירוק לגורמים לינאריים מעל המרוכבים מתקיים

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

נוכל להסיק אם כך שהפירוק הלינארי אינווריאנטי לצמוד, כלומר לכל $1 \le i \le n$ 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 10.4: נניח כי L/K הרחבה, L סגור אלגברית ונגדיר $F = \{\alpha \in L \mid K \text{ אלגברי מעל } \alpha\}$.
אז F סגור אלגברית וזה נקרא **הסגור האלגברי** (Algebraic closure) של K ב־L.

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

דוגמה 10.5: $\overline{\mathbb{Q}}$ הוא הסגור האלגברי של $\mathbb{Q}$ ולכן גם סגור אלגברית מעל $\mathbb{Q}$.