מבנים אלגבריים 2, 80446 סיכום

2025 באפריל 30



תוכן עניינים

3		1
מבת שדות	1.1 מבוא להר	
3	בניות	
4	3 – 2 הרצאה	2
5	3 – 3 הרצאה	3
6	$04-4$ הרצאה $^{-4}$	4
7	04 – 5 הרצאה .	5
7	5.1 למות גאונ	
9	04 – 6 הרצאה	6
$\mathbb{Q}[t]$ ים לאי־פריקות ב $\mathbb{Q}[t]$		
ברי	6.2 סגור אלגנ	
12	04 – 7 הרצאה <i>"</i>	7
13	04 – 8 הרצאה 3	8
14	04 – 9 הרצאה	9
15 Waka doing	g some stuff 1	n

24/03 - 1 הרצאה 1

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).

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

אלדוגמה של הומומורפיזם של הוגים): בים הוא אל הומומורפיזם של חוגים של חוגים אלדוגמה (לא הומומורפיזם של חוגים) אלדוגמה (לא הומומורפיזם של חוגים)

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

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

.1 הוא המקדם המקדם אם מתוקן הוא כי כי ניזכר הוא הוא הוא הוא ניזכר כי ניזכר כי ניזכר כי פולינום, ניזכר פולינום, יהי לינום מתוקן): יהי לינום, פולינום מתוקן אם המקדם המוביל שלו הוא 1.1 הגדרה 1.1 ו

r= אם מתוך משמע, אם מחוד פריק איננו הפיך איננו הפיך איננו (irreducible) נקרא אי־פריק (קרא אי־פריק נקרא אי־פריק בקריק) או נקרא אי־פריק (t=0 בובע ש־t=0 או t=0 משמע אור משמע t=0 או t=0 משמע אור משמע t=0 או אי־פריק (t=0 או t=0 משמע אי־פריק).

1.2 בניות

25/03 - 2 הרצאה 2

31/03 - 3 הרצאה 3

07/04 - 4 הרצאה 4

08/04 - 5 הרצאה 5

להשלים הקדמה

5.1 למות גאוס

תחום פריקות יחידה (למשל, תחום באותה צורה תחום פריקות (פרק 1) מופיע שאפשר לחקור אותה צורה את $\mathbb{Z}[t]$ אבל ברשומות (פרק 1) מופיע שאפשר לחקור באותה צורה את ראשי).

> היות של f של תכולה) ($f(t)=\sum_{i=0}^n a_i t^i$ (תכולה) הזכורת: עבור פולינום (תכולה) עבור פולינום (תכולה) אונים (תכולה) (תכולה) אונים (תכולה $cont(f) = \gcd(a_0, a_1, ..., a_n)$

> > $\mathrm{cont}(f)=1$ אם פרימיטיבי $f(t)\in\mathbb{Z}[t]$ פולינום פרימיטיבי: פולינום פרימיטיבי: פולינום פרימיטיבי:

. ביטיבים פרימיטיבי באשר $f = \mathrm{cont}(f) \cdot f_0(t)$ הנתון על־ידי בירוק פרימיטיבי $f = \mathrm{cont}(f) \cdot f_0(t)$ הנתון על־ידי פרימיטיבי

. בפרט, fg פרימיטיבי אם ורק אם fg פרימיטיבי בפרט, fg פרימיטיביים. בפרט, אזו אזי אזי פרימיטיביים אזי $f,g\in\mathbb{Z}[t]$ אזי אזי פרימיטיביים. אזי פרימיטיביים אזי פרימיטיביים אזי אזי פרימיטיביים אוויים פרימיטיביים אינים פרימיטיביים אוויים פרימיטים פרימיטיביים אוויים אוויים פרימיטיביים אוויים פרימיטיביים אוויים אוויים אוויים פרימיטיביים אוויים פרימיטיביים אוויים אינים פרימיטיביים אוויים אוויים פרימיטיביים אוויים אוויים אינים פרימיטיביים אינים א

: ברימיטיבי: הוא פרימיטיבי להוכיח ליי $f\cdot g=\mathrm{cont}(f)\cdot\mathrm{cont}(g)$ ברימיטיבי מתקיים לעיל מההערה לעיל הוכחה: הוכחה לייטיבי

 $p \nmid b_m$ ו לא כל a_i, b_j בית מרחלקים ביק ולכן נוכל לבחור m,n מינימליים כך מתחלקים ביק ולכן נוכל לבחור לבחור a_i,b_j בית מפרושות: נסתכל על המקדם של של $c=\sum_{k=0}^{m+n}a_kb_{m+n-k}$ נכתוב אותו מפרושות:

$$\underbrace{a_0b_{m+n}+\ldots+a_{n-1}b_{m+1}}_{\text{kn}}+\underbrace{a_{n+1}b_{m-1}+\ldots+a_{m+n}+b_0}_{\text{k}}$$

את סתירה. $p \nmid c$ ולכן ב־p לחלוקה לחלוקה אבל $a_n b_m$

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

 $p \mid \mathrm{cont}(h)$ אם ורק אם $h \in \mathbb{Z}[t]$ מחלק פולינום $p \notin \mathbb{Z}^x = \mathbb{Z}[t]^x$ אם ורק הוכחה: $p \mid g$ או $p \mid f$ ולכן $p \mid \mathrm{cont}(f) \cdot \mathrm{cont}(g)$ או הראשונה גאוס הלמת או מלמת או מלמת אום או מ

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

- $\mathbb{Z}[t]$ פירוק ב־ $f=(c\cdot g)\cdot (c^{-1}\cdot h)$ ולכן $c\cdot g,c^{-1}\cdot h\in \mathbb{Z}[t]$ כך ש־ $0
 eq c\in \mathbb{Q}^x$ אזי קיים $\mathfrak{g}[t]$ אזי קיים $f=g\cdot h$ בר
 - $g,h\in\mathbb{Z}[t]$ אזי f,g מתוקנים) פירוק מתוקן $f=g\cdot h\in\mathbb{Q}[t]$ ו אזי פולינום מתוקן בf
 - $\mathbb{Q}[t]$ ב אי־פריק פרימטיבי אי־פריק אם ורק אם $\mathbb{Z}[t]$ אם אי־פריק פולינום אי־פריק מוע .3

:הוכחה

 $m\cdot n\cdot f=m\cdot g\cdot n\cdot h$ ואז נקבל פירוק וויקם עב כך כך שי $m\cdot g,n\cdot h\in\mathbb{Z}[t]$ כך שי $g,h\in\mathbb{Q}[t]$ עבור $g,h\in\mathbb{Q}[t]$ את הפירוק. 1 נסמן התכולה נקבל עם כפליות התכולה $\ell=\mathrm{cont}(f), \alpha=\mathrm{cont}(m\cdot g), \beta=\mathrm{cont}(n\cdot h)$ נסמן

$$cont(m \cdot n \cdot f) = m \cdot n \cdot \ell = \alpha \cdot \beta = cont(m \cdot g \cdot n \cdot h)$$

 $f=\ellrac{m}{lpha}\cdot g\cdotrac{n}{eta}\cdot h$ משמע לוך, ניקה $f=rac{m\cdot n\cdot f}{m\cdot n\cdot \ell}=\underbrace{rac{m}{lpha}\cdot g\cdotrac{n}{eta}\cdot h}_{\in\mathbb{Z}[t]}$ אם כך, ניקה לוך בי $m\cdot n\cdot f=m\cdot g\cdot n\cdot h$ ונחלק בי $m\cdot n\cdot \ell=\alpha$ ונחלק בי $m\cdot n\cdot \ell=\alpha$ ונחלק בי

. מתוקנים. g,h עם $f=g\cdot h\in \mathbb{Q}[t]$ פירוק פירוק פרימיטיבי, ולכן בפרט הוא פרימיטיבי, ולכן גניח שf $f=c\cdot g\cdot c^{-1}\cdot h$ בר שך כך כך כך $c\cdot g\cdot c^{-1}\cdot h\in \mathbb{Z}[t]$ כך כך כך כך מקיים לפי (1) לפי לפי

נסמן פולינומים עדיין $c\cdot g,c^{-1}\cdot h$ י וים, $a_n=b_m=1$ ולכן בהכרח מתוקן נובע כי fינומים היות וים, $g=\sum_{i=1}^n a_it^i,h=\sum_{j=1}^m b_jt^j$ נסמן נסמן נובע היות וים, $g=\sum_{i=1}^n a_it^i,h=\sum_{j=1}^m b_jt^j$ נסמן נובע היות וים, אוויין פולינומים מעדיין פולינומים מעדיים מעדיים פולינומים מעדיים מעדיים פולינומים מעדיים פולינומים מעדיים פולינומים מעדיים פולינומים פולינומים מעדיים פולינומים $g,h\in\mathbb{Z}[t]$ ולכן ולכן בין ולכן מתוקנים ולכן

(6 הוכח בהרצאה) .3

f ולכן $\mathrm{cont}(f)$ ולכן ולכן $\mathrm{deg}\Big(rac{f}{\mathrm{cont}(f)}\Big)>0$ בניח כי פירוק טריוויאלי פירוק ולכן אי־פריק ב $\mathbb{Z}[t]$ ולכן ולכן בין אי־פריק בי

פרימיטיבי.

נניח ש־ $f=c\cdot g\cdot c^{-1}\cdot h$ נניח ש $f=c\cdot g\cdot c^{-1}\cdot h$ לעיל נקבל לעיל ($f=g(g),\deg(g),\deg(h)>0$ כך ש־ $f=g\cdot h$ עם דרגות נניח פריק ב-g משמע הוא פריק בו, וזאת סתירה.

:ביים: אפשריים: מקרים מקרים עם g,h עם $f=g\cdot h$ ולכן ולכן פריק פריק מקרים שני, נניח השני, נניח ש $\mathbb{Z}[t]$

סתירה וזאת פרוק על־ידי פירוק פריק פריק פריק וובע כי $\deg(f), \deg(g) > 0$ אם .1

חירה שוב סתיכי וזאת אל f אבל אז f אבל אול לכן ולכן $\deg(h) = 0, \deg(g) > 0$ ולכן .2

 \mathbb{Z} של יחידה אי־פריקים אי־פריקים של הם פולינומים שלו הראשוניים של הראשוניים של פריקים הראשוניים של מסקנה ביים אי־פריקים והראשוניים של

21/04 - 6 הרצאה 6

$\mathbb{Q}[t]$ קריטריונים לאי־פריקות ב6.1

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 $.t^4 + 4$

> \overline{R} נסמן \overline{a} נסמן $a\in R$ ועבור $R/I=\overline{R}$ נסמן את התחום $I\subseteq R$ נסמן אידיאל אידיאל בהינתן עבור $R/I=\overline{R}$

. אי־פריק. של חוגים של הומומורפיזם $\overline{f}\in\mathbb{F}_pt$ שר־פריק. ראשוני כך שר $p\in\mathbb{N}$ פולינום מתוקן, $f\in\mathbb{Z}[t]$ פולינום מתוקן. $\mathbb{Q}[t]$ ־ביק פריק פריק

 $\mathbb{Q}[t]$ ולכן קיים פירוק ($\mathbb{Q}[t]$ מתפרק ב' $\mathbb{Q}[t]$ מתפרק ב' $\mathbb{Q}[t]$ ולכן קיים פירוק מתוקן. oxdot בי הפולינומים מתוקנים וזאת סתירה. $\overline{f}=\overline{g}\cdot\overline{h}\in\mathbb{F}_p[t]$ שם $f=g\cdot h\in\mathbb{Z}[t]$ כי הפולינומים מתוקנים וזאת סתירה. $f=g\cdot h\in\mathbb{Z}[t]$

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

p למודלו f(t) באשר כל מקדם כל על־ידי הפחת המתקבל אה הפולינום לא הפולינום לא על־ידי $f(t) \mapsto \tilde{f}(t)$ על־ידי על־ידי על־ידי גגדיר גגדיר גדיר גדיר אונריידי לא על־ידי לא על־ידי לא על־ידי לא הפולינום המתקבל אונריידי לא על־ידי הפחת כל מקדם ב־ $f(t) \mapsto \tilde{f}(t)$ הם שבמודלו קינומים אלו כל הפולינומים אלו $\mathrm{Ker}(arphi)=\left\{f(t)\in\mathbb{Z}[t]\mid arphi(f)=0\in\mathbb{F}_p[t]
ight\}$ הם שבמודלו כל הפולינומים שבמודלו קלה מראה כי זה אכן הומומורפיזם ונשים לב כי מתאפסים משמע מתחלקים ב־p ולכן ולכן $p\mathbb{Z}[t]$ ממשפט האיזומורפיזם ולכן מתאפסים נקבל

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

 $0 \leq i < n$ לכל $p \mid a_i$.2

 $p^2 \nmid a_0$.3

.אז f אי־פריק

 $f=g\cdot h=\sum_{j=1}^m b_j t^j \sum_{k=1}^l c_k^{t^k}$ שמתקיים של גאוס נובע מהלמות כך, ולכן שלא בשלילה נניח נניח נוניח $p \mid$ שגם $p \mid a_0$ אבל $p \mid a_0$ אבל $p \mid a_0$ אבל $p \mid a_0$ אבל $p \mid a_0$ בובע כי $p \mid a_0$ בלית, נניח כי $p \mid a_0$ בלית, b_0 וגם b_0

 $.p \nmid b_m$ ולכן $b_m c_l = a_n$ מהיות שקיים $p \mid b_i$ ש כך ביותר הקטן הקטו $i \leq m$ הת את ניקח ניקח את ביותר ה

. כעת, בביטוי $p \nmid a_i$ אבל אז $a_i = b_i c_0 + \underbrace{b_{i-1} c_1 + ... + b_0 c_i}_{\text{מתחלקים ב־q}}$ מתחלקים ב־ $\mathbb{Z}[t]$ אי־פריק ב־ $\mathbb{Z}[t]$ אי־פריק ב־ $\mathbb{Z}[t]$ ומהלמה של גאוס נובע כי הוא גם אי־פריק ב־f אי־פריק ב־f אי־פריק בי־ק

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

 $p\mid m$ גם אם $p\mid m^2$ אז גם $p\mid m^2$ אז גם x^2-m^2, x^2+4 : 6.1 אלדוגמה

הגדרה 6.1 (פולינום ציקלוטומי): לפולינום מינימלי של שורש יחידה מעל $\mathbb Q$ נקרא פולינום ציקלוטומי): לפולינום מינימלי

לכל של המינימים המינימים שלמים שלמים מתוקן בעל מקדמים שהוא פולינום שהוא שהוא שהוא פולינום שהוא פולינום שהוא פולינום מתוקן על מחדשים לכל תחושים שהוא פולינום המינימלי של המינימלי של א n מסדר מסדר הפרימיטיביים הפרימיטיביים עובר על עובר ω עובר $\Phi_n(X) = \prod_{\omega} (X - \omega)$ משמע מסדר הפרמיטיביים הפרמיטיביים

:6.2 דוגמה

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

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

 \mathbb{Q} אי־פריק למה אי־פריק אי־טריק א

ואז נקבל ואז t=x+1 ואז x=t-1 המתנה משתנה זה טריק, נשנה הוכחה:

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

0 < i < pלכל $p \mid \binom{p}{i}$ רים מתוקן חופשי מקדם שכן אייזנשטיין אייזנשטיין לפי אי־פריק אייפריק איי

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

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

6.2 סגור אלגברי

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

Kיש שורש ב' איש פולינום אם לכל פולינום אם אדה סגור שדה סגור (שדה מעל איש מעל איש מעל איש פולינום אגברית: שדה סגור אלגברי): איש שורש ב' א

הגדרה הוא מתפצל לחלוטין): נגיד על שדה, נגיד כי פולינום מתפצל לחלוטין אם הוא שדה, נגיד לנגיד שדה, נגיד לנגיד שדה, נגיד לחלוטין: נגיד א שדה, אורמים לינאריים.

$$a_i \in K$$
ים באשר $a_i \in K$ ר כאשר $c \in K^x$ כאשר $f = c \prod_{i=1}^{\deg(f)} (t - a_i)$ משמע,

למה שקולים הבאים K עבור שדה :6.3

- 1. סגור אלגברית
- וטין לחלוטין מתפצל מתפצל $0 \neq f \in K[t]$ מתפצל 2.
 - 1 אי־פריק הוא מדרגה $f \in K[t]$.3
- איות אל טריוויאליות אל אלגבריות אל החבות אין הרחבות K^{-1} .

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

- . שורש לי שיש מהגדרה מלא, נובע פירוק שיש לי $(1) \Leftarrow (2)$
- $\deg(f)$ יש פירוק אינדוקציה את מסיימים מ $\deg g < \deg f$ יש פירוק פירוק שלכל שלכל נובע שלכל נובע פירוק פירוק פירוק פירוק אונדי פירוק פירוק פירוק אונדי פירוק פירו
- 1<[K(lpha):K] אי־פריק מדרגה אי־פריק אי־פריק ואז הפולינום אי־פריק ניקבל ביקברית לא טריוויאלית ברחבה אלגברית לא מריוויאלית וויאלית ביקבל ביקברית ווא הפולינום אי־פריק מדרגה (4)
 - $.[L:K] = \deg(f) > 1$ ו ר־ L = K[t]/(f)נגדיר נגדיר לפריק ו־ אי־פריק ו' אם לפריק ו' ו $\deg(f) > 1$ ו אם לפריק ו' אם לפריק ו'

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

. סגור אלגברית. של האלגברה) המשפט 6.2 (המשפט היסודי של היסודי של האלגברה) המשפט

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.

:6.1 מסקנה

- .1 בינאריים לינאריים לינאריים של מתפרק מתפרק מתפרק $\mathbb{R}[t]$ מתפרק לא פולינום לינאריים.
 - (דיסקרמיננטה) $\mathrm{dic} < 0$ עם וריבועיים לינאריים הם $\mathbb{R}[t]$ הם ב-פריקים .2

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

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

 $\overline{a_i} \in \{a_i \mid 0 \leq i \leq n\}$ וכן $a_i \in \mathbb{C}$ או ש־ $a_i \in \mathbb{R}$ או ש־ $1 \leq i \leq n$ גוכל לאמוד, כלומר לצמוד, כלומר לכל מחיקת אם כך שהפירוק הלינארי אינווריאנטי לצמוד, כלומר לכל (תוך מחיקת הצמודים), ונקבל, ונקבל,

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

ישל ממשיים לינאריים לינאריים של מכפלה הוא לכלומר לינאריים של מכפלה ל

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

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

 $.F = \{\alpha \in L \mid K$ מסקנה אלגברי מעל אלגברית סגור סגור סגור הרחבה, ברחבה נניח כי נניח מסקנה (ה

Lב K של (Algebraic closure) של הסגור הסגור הסגור נקרא נקרא אז F אז F

אבל שורש, אבל סגור אלגברית, כלומר f אי־פריק עם דרגה גדולה מ־1. אז יש ל־f שורש ב־f לא סגור אלגברית, כלומר $f(t) \in F[t]$ אי־פריק עם דרגה גדולה מ־f אלגברי מעל f וזאת סתירה. $\alpha \in F$ אלגברי מעל f וואת סתירה.

 \mathbb{Q} הוא סגור אלגברית של \mathbb{Q} ולכן האלגברית מעל הסגור הוא הסגור הוא דוגמה הוא דוגמה דוגמה

22/04 - 7 הרצאה 7

28/04 - 8 הרצאה 8

29/04 - 9 הרצאה 9

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).

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

אלדוגמה לא הומומורפיזם של חוגים): $\varphi:0 o\mathbb{Z}$ הוא אל חוגים של חוגים של חוגים אלדוגמה 10.1 אלדוגמה

. ראשוני בלבד אשוני $p\in\mathbb{N}$ עבור $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z},\mathbb{Q}ig(\sqrt{2}ig),\mathbb{Q},\mathbb{R},\mathbb{C}:$ (שדות) אוני בלבד.

 $0,\mathbb{F}[X],M_{n imes n}(\mathbb{F}):$ לא שדות) ווס.2 אלדוגמה 10.2 אלדוגמה

.1 אוא המקדם המקדם אם מתוקן הוא הוא f כי נגיד בי $f=\sum_{i=1}^n a_i x^i$ כי פולינום, ניזכר פולינום מתוקן: יהי יהי פולינום, ניזכר כי יהי ווא הוא פולינום מתוקן.

אם מתוך משמע, אם איננו הפיך אי־פריק (irreducible) נקרא אי־פריק (נקרא אי־פריק בקריק) אי־פריק (נקרא אי־פריק) אי־פריק (נקרא

הערה: אנחנו בעבוד עם $\mathbb{Z}[t]$ אבל ברשומות (פרק 1) מופיע שאפשר לחקור באותה צורה את $\mathbb{Z}[t]$ כאשר $\mathbb{Z}[t]$ אבל ברשומות (פרק 1) מופיע שאפשר לחקור באותה צורה את ראשי).

להיות של f של תכולה) ($f(t)=\sum_{i=0}^n a_i t^i$ הזכורת: $f(t)\in\mathbb{Z}[t]$ בגדיר עבור פולינום (תכולה) אותר ככחt ($f(t)=\gcd(a_0,a_1,...,a_n)$

 $\mathrm{cont}(f)=1$ אם פרימיטיבי אקרא קולונום פולינום פולינום פרימיטיבי): פולינום פרימיטיבי: פולינום פרימיטיבי): פולינום

. בימיטיבים פולינום פולינום לא הוא בכל פולינום לא בכחל כחול לא הנתון על־ידי על־ידי בינות פרימיטיבי. לכל פולינום לו פרימיטיבי $\mathcal{Z}[t]$ הנתון על־ידי לכל פולינום ליש

. בפרט, f פרימיטיבי אם ורק אם f ווg פרימיטיבי הם ורק פרימיטיבי משפט 10.1 (למת אוז f אזי ורק אם f אזי f אזי f אזי f אזי ורק אם ורק אם f פרימיטיביים.

 $p
mid b_m$ י הראים כך שי a_n ים מינימליים החתים (נוכל לבחור m,n ולא כל $p
mid a_i,b_j$ המתחלקים בי a_i,b_j ולכן נוכל לבחור המקדם של המקדם של $c=\sum_{k=0}^{m+n}a_kb_{m+n-k}$ נסתכל על המקדם של

$$\underbrace{a_0b_{m+n}+\ldots+a_{n-1}b_{m+1}}_{\text{kn}}$$
מתחלקים ב־ק כי $p|a_k$ לכל $p|b_k$ לכל $p|b_k$

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

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

 $p \mid \mathrm{cont}(h)$ אם ורק אם $h \in \mathbb{Z}[t]$ מחלק פולינום $p \notin \mathbb{Z}^x = \mathbb{Z}[t]^x$ אם ורק הוכחה: נשים לב שי $p \mid p \mid \mathrm{cont}(f) \cdot \mathrm{cont}(g)$ אם אם אז מלמת גאוס הראשונה נובע $p \mid f \cdot g$ אם אז מלמת גאוס הראשונה נובע

אז השברים של $\mathbb{Z}[t]$ שדה השברים של האוס (למת גאוס השנייה): יהי $f \in \mathbb{Z}[t]$ יהי יהי (למת גאוס השנייה) אוז משפט 10.2 פולינום לא קבוע. נזכור בי

 $\mathbb{Z}[t]$ פירוק ב־ $f=(c\cdot g)\cdot \left(c^{-1}\cdot h
ight)$ ולכן $c\cdot g,c^{-1}\cdot h\in \mathbb{Z}[t]$ כך שי $0
eq c\in \mathbb{Q}^x$ אזי קיים $\mathbb{Q}[t]$ אזי קיים $f=g\cdot h$ אם .1

 $g,h\in\mathbb{Z}[t]$ אזי מתוקנים) אינו פירוק מתוקן פירוק פירוק $f=g\cdot h\in\mathbb{Q}[t]$ אזי פולינום פולינום פולינום 2.

 $\mathbb{Q}[t]$ אם אי־פריק פרימטיבי או פרימטיבי אם ורק אם $\mathbb{Z}[t]$ אם אי־פריק פולינום אי־פריק 3.

:הוכחה

 $m \cdot n \cdot f = m \cdot g \cdot n \cdot h$ אוז נקבל פירוק $m \cdot g, n \cdot h \in \mathbb{Z}[t]$ כך ש־ $0 < m, n \in \mathbb{Z}$ וניקח $g, h \in \mathbb{Q}[t]$ עבור $f = g \cdot h$ את הפירוק $f = g \cdot h$ ניסמן $f = g \cdot h$ מלמת גאוס הראשונה נקבל עם כפליות התכולה $\ell = \operatorname{cont}(f), \alpha = \operatorname{cont}(m \cdot g), \beta = \operatorname{cont}(n \cdot h)$

$$cont(m \cdot n \cdot f) = m \cdot n \cdot \ell = \alpha \cdot \beta = cont(m \cdot g \cdot n \cdot h)$$

 $f = \ell \frac{m}{lpha} \cdot g \cdot rac{n}{eta} \cdot h$ משמע שמע ל $f = \frac{m \cdot n \cdot f}{m \cdot n \cdot \ell} = \underbrace{\frac{m}{lpha} \cdot g \cdot rac{n}{eta} \cdot h}_{\in \mathbb{Z}[t]}$ ונהלק ב־ $m \cdot n \cdot \ell = \alpha eta$ ונהלק ב $m \cdot n \cdot \ell = m \cdot g \cdot n \cdot h$ משמע מע

.2 עם g,h עם $f=g\cdot h\in\mathbb{Q}[t]$ קיים פירוק ולכן פרימיטיבי, ולכן בפרט הוא פרימיטיבי, ולכן קיים פירוק פרים גם מתוקן, ולכן בפרט הוא פרימיטיבי, ולכן $c\cdot g\cdot c^{-1}\cdot h\in\mathbb{Z}[t]$ כך ש־ $c,c^{-1}\in\mathbb{Z}$ שקיים לפי (1) נובע שקיים ב

עדיין פולינומים $a_nb_m=1$ ולכן בהכרח $a_nb_m=1$ היות ו $a_nb_m=1$ היות ו

3. (הוכח בהרצאה 6)

f ולכן $\det(f)$ ולכן ולכן $\det(\frac{f}{\operatorname{cont}(f)}) > 0$ בניח כי $f = \operatorname{cont}(f) \cdot \frac{f}{\operatorname{cont}(f)}$ ולכן $\mathbb{Z}[t]$ ולכן בי $f = \operatorname{cont}(f)$ הפיך ולכן פרומיטירי

נניח ש־0 בר עם דרגות גדולות מ־0 בר $f=c\cdot g\cdot c^{-1}\cdot h$ לעיל נקבל לעיל $\deg(g),\deg(h)>0$ בר כך ש־ $f=g\cdot h$ עם דרגות מ־0 בניח פריק בר פריק בין, וזאת סתירה.

אפשריים: מקרים מקרים ביים: g,h עם $f=g\cdot h$ ולכן ב־ $\mathbb{Z}[t]$ ולכן פריק ביf פריק ביים: \Longrightarrow

סתירה זה וזאת פירוק על־ידי פריק ב־ $\mathbb{Q}[t]$ פריק כי וואת נובע כי $\deg(f), \deg(g) > 0$.1

סתירה שוב וזאת פרימיטיבי אז או אבל אז אבל ולכן אבל אולכן ולכן $\deg(h)=0,\deg(g)>0$ אבל הכלליות בלי בלי הגבלת בליות .2

 $\mathbb{Z}[t]$ מסקנה $\mathbb{Z}[t]: 10.2$ הוא חוג פריקות יחידה והראשוניים שלו הם פולינומים פרימטיביים אי־פריקים והראשוניים של

.(n באינדוקציה באים פריקות תחום פריקות הוא גם ווערה: באותה אזי גם היידה אזי מחום פריקות החום פריקות אזי באותה אזי גם ווערה: באותה שאם אם תחום פריקות היידה אזי גם $R[t_1,...,t_n]$

 \overline{R} נסמן \overline{a} בתמונה של $a\in R$ ועבור $R/I=\overline{R}$ נסמן את התחום $I\subseteq R$ נסמן אידיאל אידיאל בהינתן על מימון: R $a_i = \sum_{i=0}^n a_i t^i \mapsto \sum_{i=0}^n \overline{a_i} t^i = \overline{f}$ כמו כן, הההומורפיזם להומומורפיזם מתרחב להומומורפיזם $R \to \overline{R}$

א־פריק. אי־פריק של חוגים של $\overline{f}\in\mathbb{F}_pt$ מודלו כך האשוני כך פולינום מתוקן, אי־פריק. פולינום מתוקן, אי־פריק. פולינום מתוקן, אי־פריק. $\mathbb{Q}[t]$ ־ביק פריק פריק

 $\mathbb{Q}[t]$ ולכן קיים פירוק מתוקן $\mathbb{Q}[t]$ מתפרק ב־ $\mathbb{Q}[t]$ מתפרק בין ולכן קיים פירוק מתוקן מתוקן מתפרק בי oxdot בי הפולינומים מתוקנים וזאת סתירה. $\overline{f}=\overline{g}\cdot\overline{h}\in\mathbb{F}_n[t]$ שם $f=g\cdot h\in\mathbb{Z}[t]$ כי הפולינומים מתוקנים וזאת סתירה. $f=g\cdot h\in\mathbb{Z}[t]$

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

p למודלו f(t) באשר ב־לידי הפחת על־ידי הפחת המתקבל זה הפולינום האס, האשר $ilde{f}(t)$ כאשר f(t) למודלו $\varphi: \mathbb{Z}[t] o \mathbb{F}_p[t]$ למודלו גדיר נגדיר הם p אלו כל הפולינומים אלו $\operatorname{Ker}(\varphi)=\left\{f(t)\in\mathbb{Z}[t]\mid \varphi(f)=0\in\mathbb{F}_p[t]
ight\}$ הביקה הפולינומים אלו כל הפולינומים שבמודלו ממשפט האיזומורפיזם הראשון לחוגים נקבל . $\mathrm{Ker}(arphi)=p\mathbb{Z}[t]$ ולכן ב־pים מחלקים משמע מתאפסים משמע

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

הבאים המתקיימים כך אשוני כך וי $p\in\mathbb{N}$ ו־ו $\mathbb{Z}[t]\ni f=\sum_{i=0}^n a_it^i$: נניח הניחניים: (קריטריון אייזנשטיין: נניח משפט 10.3

 $p \nmid a_n$.1

 $0 \leq i < n$ לכל $p \mid a_i$.2

 $p^2 \nmid a_0$.3

.אז f אי־פריק

 $.p \nmid b_m$ ולכן $b_m c_l = a_n$ מהיות שקיים $p \mid b_i$ שר כך ביותר הקטן ולכן הד $i \leq m$ את ניקה ניקה ניקה את

תירה. $p \nmid a_i$ מתחלקים בי $p \nmid a_i$ אבל אז $a_i = b_i c_0 + \underbrace{b_{i-1} c_1 + ... + b_0 c_i}_{\text{endiffice cross}}$ כעת, בביטוי מתחלקים בי $p \nmid a_i$ אי־פריק בי $p \mid a_i$ ומהלמה של גאוס נובע כי הוא גם אי־פריק בי $p \mid a_i$ אז $p \nmid a_i$ מתפרק לגורמים מדרגה גדולה מ־0 ואז $p \mid a_i$ אי־פריק בי $p \mid a_i$ ומהלמה של גאוס נובע כי הוא גם אי־פריק בי $p \mid a_i$ אז $p \mid a_i$ לא מתפרק לגורמים מדרגה גדולה מ־0 ואז $p \mid a_i$ אי־פריק בי $p \mid a_i$

. (ולא רק חסר שורשים) אי־פריק x^n-m אז $p^2 \nmid m$ ורשים כך שר $p \in \mathbb{N}$ וקיים וקיים x^n-m יהי x^n-m אי־פריק (ולא רק חסר שורשים).

 $p\mid m$ גם אז גם $p\mid m^2$ אל פריקים: אמיד x^2-m^2, x^2+4 : אלדוגמה אלדוגמה

הגדרה מעל $\mathbb Q$ נקרא פולינום ציקלוטומי): לפולינום מינימלי של שורש יחידה מעל $\mathbb Q$ נקרא פולינום ציקלוטומי.

לכל של המינימים הפולינום שלמים שלמים מתוקן בעל מתוקן פולינום שלהוא של יחיד ביקלוטומי יחיד Φ_n שהוא פולינום מתוקן לכל $n\in\mathbb{Z}$ לכל השורשים הפרימיטיביים מסדר $\Phi_n(X)=\prod_\omega(X-\omega)$ באשר $\Phi_n(X)=\prod_\omega(X-\omega)$

: 10.4 דוגמה

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

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

 $\mathbb Q$ אי־פריק אי־פריק אי־פריק אי־פריק אי־פריק אי־פריק הפולינום הציקלוטומי אי־פריק למה לכל : 10.2 למה למה

ואז נקבל אז t=x+1 ואז x=t-1יאז משתנה ל-1 הוכחה: זה טריק, נשנה מהכחה

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

0 < i < pלכל $p \mid \binom{p}{i}$ ריטריון חופשי מתוקן שכן שכן שכן אייזנשטיין לפי אי־פריק אי־פריק איד אייזנשטיין אייזנשטיין אייזנשטיין איי

האת סתירה. האר $\Phi_p(t)=g(t)\cdot h(t)=g(x+1)\cdot h(x+1)$ האת קיימים אז $\Phi_p(t)$ אם אם לא $\Phi_p(t)$

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

Kיש שורש ב־א נקרא של אלגברי): שדה K נקרא שדה סגור אלגברית אם לכל פולינום לא קבוע מעל א נשדה K יש שורש ב־

תפרק לגורמים אם הוא מתפצל (פולינום מתפצל אדרה 10.7 (פולינום מתפצל אדרה בגיד לחלוטין): נגיד עדה, נגיד עד שדה, נגיד עד שדה (פולינום מתפצל אחלוטין): נגיד עד האדרה 10.7 (פולינום מתפצל לחלוטין): נגיד עד האדרה באררה $a_i \in K^x$ שדרה בארר לחלוטין אם הוא מתפרק לגורמים לינאריים. וויים $a_i \in K^x$ באשר לכל לחלוטין אם הוא מתפרק לגורמים לינאריים.

לים שקולים הבאים K בבור עבור עבור: 10.3

- 1. סגור אלגברית
- טין לחלוטין מתפצל מתפצל $0 \neq f \in K[t]$ מתפצל 2.
 - 1 אי־פריק הוא אי־פריק אי־פריק אי־פריק .3
- אין הרחבות אלגבריות לא טריוויאליות K^{-1} . 4

היכחה: (2) \iff (3) מיד יש פירוק לפולינומים אי־פריקים.

- . שורש לי שיש מהגדרה מובע מלא, נובע פירוק שיש לי $(1) \longleftarrow (2)$
- $\deg(f)$ יש פירוק עם אינדוקציה את ומסיימים ומסיימים יש פירוק פירוק פירוק פירוק פירוק פירוק פירוק פירוק וובע שלכל יש פירוק פירו
- 1 < [K(lpha):K] אי־פריק מדרגה אי־פריק אוז הפולינום אי ואק ניקבל ביקב לא טריוויאלית ער ניקבל ביקב אוז הפולינום ווא אי־פריק מדרגה אלגברית אי־פריק אי־פריק וויאלית אי־פריק א
- $[L:K]=\deg(f)>1$ ר בL=K[t]/(f) נגדיר ווער בעריק וי $\deg(f)>1$ אם אי־פריק וי $\deg(f)>1$ בעריק וי

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

. סגור אלגברית. של היסודי של היסודי אלגברית. 10.4 משפט 10.4 המשפט היסודי של האלגברה)

: 10.3

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

הוכחה: נשים לב 0 ברור, ולכן מספיק שנוכיח רק את 1: נשים לב 0 ב0 ולכן ההצמדה רק מחליפה את השורשים של 0 ברור, ולכן מספיק שנוכיח רק את 1: נשים לב 0 בשים לשורשים אך לא את השורשים עצמם). 0 בעצם תמורה, כי ההצמדה רק יכולה לשנות מיקום לשורשים אך לא את השורשים עצמם). 0 לטובת מי מבנינו שמתעב מרוכבים, ניזכר במספר עובדות קצרות. הצמוד המרוכב של מספר ממשי הוא ממשי. כמו־כן, הצמוד המרוכב סגור לחיבור לטובת מי מבנינו שמתעב מרוכבים, ניזכר במספר של צמודים, ואותו הדבר לחיבור. המשמעות היא שאם 0 פולינום ממשי, אז כפולינום מעל המרוכבים נקבל 0 בשל סגירות זו, גם בפירוק לגורמים לינאריים מעל המרוכבים מתקיים.

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

 $\overline{a_i} \in \{a_i \mid 0 \leq i \leq n\}$ וכן $a_i \in \mathbb{C}$ או ש־ $a_i \in \mathbb{R}$ או ש־ $1 \leq i \leq n$ נוכל להסיק אמודי לצמוד, כלומר לצמוד, כלומר לכל $a_i \in \mathbb{R}$ או ש־ $a_i \in \mathbb{R}$ וכן לאמודים), מון מחיקת מחיקת מחיקת ממשיים כ־ a_i ואת המרוכבים כ־ a_i ואת המרוכבים כ־ a_i ואת המרוכבים כ־ a_i וכן לצמודים), ונקבל,

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

ושל ממשיים לינאריים גורמים של מכפלה של הוא כלומר לינאריים כלומר ל

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

П

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

 $A = \{ \alpha \in L \mid K$ מסקנה 10.4 מסקנה ברית מעל חגבר, סגור אלגברית סגור הרחבה, לניח כי $A \in L$ הרחבה, נניח מסקנה אז הסגור האלגברי (Algebraic closure) של אד ב־ $A \in L$

אבל שורש, אבל מיור אלגברית, כלומר $f(t) \in F[t]$ אי־פריק עם דרגה גדולה מי1. אז יש ל-f שורש ביט (כי $f(t) \in F[t]$ סגור אלגברית, כלומר $f(t) \in F[t]$ אי־פריק עם דרגה גדולה מי $f(t) \in F[t]$ אלגברי מעל $f(t) \in F[t]$ אלגברי מעל $f(t) \in F[t]$ אוזאת סתירה.

 \mathbb{Q} הוא סגור אלגברית של \mathbb{Q} ולכן האלגברי מעל הוא הסגור האלגברית מעל דוגמה הוא הוא דוגמה