# מכנים אלגבריים 2, 80446 סיכום מבנים אלגבריים א

18 ביולי 2025



# תוכן עניינים

5		הרצא	1
5	מבוא להרחבת שדות	1.1	
5	בניות	1.2	
6	שדות ראשוניים	1.3	
7		הרצא	2
7	הרחבת שדות	2.1	
7	יוצרים של הרחבות	2.2	
9		תרגוק	3
9	חוג הפולינומים – תזכורת	3.1	
9	בניית שדות בעזרת מנות של חוגי פולינומים	3.2	
9	E=F[x]/(f) חישוב בשדה	3.3	
10		תרגיל	4
10	טריקים	4.1	
10	מסקנות	4.2	
11		הרצא	5
11	הרחבות אלגבריות	5.1	
14		תרגוק	6
14	משהומשהו	6.1	
15		הרצא	7
15	שימושים בסיסיים של תורת השדות – בניות עם סרגל ומחוגה	7.1	
			8
	למות גאום		
			9
	משהו		
			10
	טריקים		
	מסקנות		
			11
	$\mathbb{Q}[t]$ בריטריונים לאי־פריקות ב $\mathbb{Q}[t]$		
	קו שו זב או כו קווב נון שם סגור אלגברי		
23	22/04 – 7 7		19
	יין די בעוסב (די הייבות סגור אלגברי		14
	23/04 – 4		12
	שדות פיצול		13
	באר 28/04 – 8 מה 28/04 – 8 מה		1 /
	יוו 7 - 26/04 – פקום ויחידות סגור אלגברי – המשך		14
	,		
	$\overline{K}/K$ אוטומורפיזמים של		
	ה 9 – 29/04 – 29/04 – 3		15
	$\overline{K}/K$ אוטומורפּיזמים של – $\overline{K}/K$ אוטומורפּיזמים.		
	הרחבות נורמליות		
			16
	טריקים		
	מסקנות		
			17
31	הרחבות נורמליות – המשך	17.1	
21	ייודות תוצור	17 2	

32	שורשי יחידה 17.3
35	
35	18.1 שורשי יחידה – המשך
35	שדות סופיים
38	
38	משהו
39	
39	
39	,
40	•
40	
42	1
42	
42	,
43	· ·
43	
	·
44	
44	,
44	
45	
45	,
45	,
48	
48	, , ,
49	
49	
50	
50	טריקים 28.1
50	28.2 מסקנות
51	26/05 – 16 הרצאה 29
51	(purely inseparable) הרחבות אי־פרידות בטהרה 29.1
51	29.2 תורת גלואה
51	29.3 התאמת גלואה
52	27/05 – 17 הרצאה 30
52	התאמת גלואה – המשך 30.1
53	31 תרגול <b>28/05 – 28/05</b>
53	משהו 31.1
54	32 תרגיל 7
54	
54	·
55	
55	
56	
56	
57	
58	
58	
JO	מסקנות

59	שעת קבי	36
קנות	36.1 מס	
60	9 הרצאה	37
י עובדות על התאמת גלואה	עוז 37.1	
מושים של תורת גלואה	שיט 37.2	
61	0 הרצאה	38
ות של מצולעים משוכללים	38.1 בני	
62	תרגול 10	39
62	39.1 הדי	
64	תרגיל 9	40
64	שר 40.1	
קבות	40.2 מס	
65	1 הרצאה	41
65	41.1 סכ	
חבות ציקליות ופתירות ברדיקלים	41.2 הר	
68		
חבות ציקליות ופתירות ברדיקלים – המשך	42.1 הר	
70		
70		
71		
יקים		
קבות		

#### 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 של הומומורפיזם של הוא סוגים:  $\varphi:\mathbb{Z} \to 0$  הוא חוגים של חוגים.

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

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) 1.2 דוגמה

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

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

אם איננו הפיך ואין לו פריק (irreducible) א קיפריק  $r.0 \neq r \in R$  תחום שלמות וR (אי־פריק). תחום שלמות וR הגדרה 1.2 (אי־פריק). . (משמע, אם מתוך קראנו קראנו לזה החס  $a\sim r$  משמע, או  $a\in R^{ imes}$  נובע ש $a\in R^{ imes}$  נובע ש $a\in R^{ imes}$  או  $a\in R^{ imes}$ 

מסקנה K: 1.1 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

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

 $rac{s_1}{r_1}\simrac{s_2}{r_2}\Longleftrightarrow s_1r_2=s_2r_1$  כאשר שקילות שקילות שקילות המקיים

 $R\subset\operatorname{Frac}(R)\hookrightarrow K$  ויחיד פיקטור שדה, קיים לאשר א כאשר באשר ויחיד כאשר: 1.1 למה 1.1 לכל שיכון

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

$$K(S) := \operatorname{Frac}(K[S])$$

.S של במשתנים אל מעל רציונליות רציונליות פונקציות הדה

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

K(y)(x) = K(x)(y) מתקיים : 1.1 מתגיל

.
$$\operatorname{Frac}(K[x,y]) = K(x,y) = K(y,x) = K(x)(y) = K(y)(x)$$
 ולכן ולכן  $K[x,y] = K[y,x]$ 

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

הוא שדה K=R/M אידיאל מקסימלי אידיאל Mחוג ו־R אם .1

הוא שדה K[t]/(f(t)) אזי מעליו אי־פריק פולינום f(t) הוא הוא K[t]/(f(t)) אם .2

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

# : 1.3 דוגמה

$$(t^2+1=0\Rightarrow t=i$$
 וחייבנו וחייבנו אחרות, במילים (במילים במילים) ווחייבנו  $\mathbb{C}=\mathbb{R}[t]/(t^2+1)$  .1

$$\mathbb{Q}\left(\sqrt{2}\right) = \mathbb{Q}(t)/(t^2 - 2) .2$$

$$\mathbb{Q}\left(\sqrt[3]{3}\right) = \mathbb{Q}(t)/(t^3 - 3) .3$$

$$\mathbb{Q}(\sqrt[3]{3}) = \mathbb{Q}(t)/(t^3 - 3) .3$$

#### : 1.2 תרגיל

$$\mathbb{F}_3(t)/(t^2+1) = \mathbb{F}_9 = \mathbb{F}_3\left[\sqrt{-1}\right] .1$$

$$\mathbb{F}_2(t)/(t^2+t+1) = \mathbb{F}_4(\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}) . 2$$

:הוכחה

ולפן  $t^2=2$  ולכן  $-1\equiv 2 \pmod 3$  אבל  $t^2+1=0 \Longleftrightarrow t^2=-1$  אז מתקיים אז מתקיים  $t^2+1$  אם נסתכל על הפולינום  $t^2+1$  אז מתקיים  $t^2+1$  און שורשים ב- $\mathbb{F}_3$  (פשוט להציב  $t^2+1$ ). ולפולינום  $t^2+1$ 

טנים, ואנחנו לסכומים אפשרויות אפשרויות שנים,  $a,b\in\mathbb{F}_3$  עבור a+bt אפשרויות לסכומים מכיל את מכיל את  $\mathbb{F}_3(t)/(t^2+1)$ , קומבינטורית שזה גם הגודל של השדה  $\mathbb{F}_9$  ועל־כן הם שקולים.

$$t^2=-1$$
ברור מכך ברור  $F_3(t)/(t^2+1)=\mathbb{F}_3\left[\sqrt{-1}
ight]$  המקרה של

.2 על אותו רעיון כמו המקרה הקודם.

#### 1.3 שדות ראשוניים

. בלבד ששדה הוא עמה פאבר (שדה תאשוני): נגיד ששדה הוא הוא אדה האשוני אם הוא שדה הוא שדה הוא נגיד ששדה הוא נגיד ששדה הוא הוא שדה הוא ש

. הכלה: ביחס מנימליים מבית אדות שדות ובפרט ובפרט אדות הת-שדה הת-שדה תת-שדה הת-שדה למה 1.2 לכל הכלה: למה למה להכלה: למה אחרים ויחיד הת-שדה החיד המוני א

ונחלק למקרים:  $\ker(\varphi)=(n)$  ואז ואלכן תחום אוקלידי וולכן עכן  $\mathbb{Z} \to \mathbb{Z}/\ker(\varphi) \subset R$ ו־ע $\varphi:\mathbb{Z} \to K$  וינחלק למקרים: בפרט, יש הומומורפיזם יחיד

$$\operatorname{Frac}(\mathbb{Z})=\mathbb{Q}\hookrightarrow R$$
 ולכן גם  $\mathbb{Z}\hookrightarrow R$  אזי  $n=0$  .1

 $\mathbb{F}_p=\mathbb{Z}/p\hookrightarrow K$ יש אומר וזה תחום תחום כי כי האשוני כי תאשוני חp=p אז או $p\neq 0$  אם .2

. כמובן, אף  $\mathbb{Q}$  או שכן אחד האר מהרשימה אחר מכיל אז לא  $\mathbb{Q}$  או  $\mathbb{F}_n$  אף כמובן, אף

הוא K שדה של של המציין: המציין 1.6 המציין הגדרה

 $\mathbb{Q} \subseteq K$  אם  $\operatorname{char}(K) = 0$  .1

$$\mathbb{F}_p\subseteq K$$
 אם  $\mathrm{char}(K)=p$  .2

אם לא קיים אור  $\operatorname{char}(K)=0$  ו־ $0=p\in K$  הקטן ביותר כך החיובי המספר החיובי הוא המספר המינה. אלטרנטיבית למציין:

 $\ker(\mathbb{Z} \to K) = (\operatorname{char}(K))$  אראינו מהלמה שראינו:

pב ב'ת (אזהרה): בשדה ממציין pהדבר הכי חשוב לעשות זה לא לחלק ב'-p

. ערכית.  $\varphi$  אזי אזי אזי אזי חד־חד ערכית. אזי  $\varphi:K o R$  אזי אזי אזי ערכית. אזי פיזם אזי  $\varphi:K o R$ 

אידיאל.  $I = \ker(\varphi) \subseteq K$  אידיאל.

אם סתירה. R=0 ולכן R=0 ואז וווו סתירה. אם שמתקיים אוווו סתירה. ערכית וסיימנו, או

. $\operatorname{End}(K)$  ומסומן נקרא אנדומורפיזם בקרא נקרא נקרא הומומורפיזם: הומומורפיזם: אוטומורפיזם, אוטומורפיזם הגדרה 1.8 הגדרה

(שזו כמובן חבורה)  $\operatorname{Aut}(K)$  בי ומסומן בי נקרא אוטומורפיזם או הפיך אז  $\varphi$  הפיך אז  $\varphi$  הפיך אז

. (עוד נתעסק בו בהמשך). נניה ש־K לעצמו (עוד נתעסק בו בהמשך). אזי  $\mathrm{Fr}(x)=x^p$  אזי הודיר אנדומורפיזם מ־K נניה ש־K נניה ש-K לעצמו (עוד נתעסק בו בהמשך).

pמתחלק ב־ $(xy)^p=x^py^p$  ונשים לב ש־ $(xy)^p=x^py^p$  מתחלק ב־ $(xy)^p=x^py^p$  ונשים לב ש־ $(xy)^p=x^py^p$  מתחלק ב־ $(xy)^p=x^py^p$  וואז  $i
otin\{0,p\}$  מתחלק ב־ $(xy)^p=x^p+y^p$  במספר שלם כאשר  $(xy)^p=x^p+y^p$  וואז וואז אבנו  $(xy)^p=x^p+y^p$  בכל שדה שבנו

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

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

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

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

#### 25/03 - 2 הרצאה 2

#### 2.1 הרחבת שדות

פרק 3 ברשומות של מיכאל.

היא החבת שדות. אז אומרים L/K היא הרחבת שדות. היא תת־שדה (קבוצה סגורה לפעולות) אז אומרים שL/K היא הרחבת שדות.

השיכון בפועל מהשיכון אבל בפועל בפועל מרכות אבל ממעט ממיד אנחנו בונים אבל בפועל הרחבות ולבנות הרחבות אבל בפועל מהשיכון הדרך-כלל, נרצה להתחיל מKKב־עלידי החלפה של לבנות הרחבה לבנות הרחבה לבנות אפשר  $\varphi:K o L$ 

קבarphi:F o L אזי F-הומומורפיזם מ־F הומומורפיזם של איז T-שתי החבות של איז שדות): אם L/K,F/K שתי החבות של איז איז הומומורפיזם בין שדות): אם L/K,F/K $arphi|_K=\mathrm{Id}$  שמתקיים

 $\operatorname{Aut}(L/K)$ או או  $\operatorname{Aut}_K(L)$ ב של  $\operatorname{Aut}_K(L)$ הרחבת או הבורת כל אוטומורפיזמים של הרחבת שדות, נסמן את חבורת כל

- (כי שורשים של פולינום הולכים של אורשים (כי שורשים אורשים  $\operatorname{Aut}_{\mathbb{R}}(\mathbb{C})=\mathbb{Z}/2\mathbb{Z}$  .1
  - הוא ענק ולא נחמד  $\operatorname{Aut}_{\mathbb{O}}(\mathbb{C})$  .2
    - $\operatorname{Aut}_{\mathbb{C}}(\mathbb{C}) = 1$  .3
- עם ההצמדה  $a+b\sqrt{2}\mapsto a-b\sqrt{2}$  עם ההצמדה  $\mathrm{Aut}_\mathbb{Q}ig(\mathbb{Q}ig(\sqrt{2}ig)ig)=\mathbb{Z}/2\mathbb{Z}$  .4

#### 2.2 יוצרים של הרחבות

תת־קבוצה, אז  $S\subseteq L$ יו ( $K\subseteq L$ ) הרחבת שדות (גניח ש־L/K: נניח ש $S\subseteq L$ יו (K[S],K(S)) מת־קבוצה, אז

- ביותר הקטן והוא ו-S והוא שמכיל שמכיל של L שמכיל K[S] .1
  - S ואת את המכיל המכיל ביותר הקטן הקטן K(S) .2

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

$$K[S] = \left\{ f(s) \mid f \in K[x_s]_{s \in S} \right\} . 1$$

$$K[S] = \left\{ f(s) \mid f \in K[x_s]_{s \in S} \right\} . 1$$

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

הוכחה: להשלים, למה 3.1.23 אצל מיכאל.

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

L[S]=L טופית כך שמתקיים בא קיים קיים מוצרת סופית כך שמתקיים בא נוצרת נוצרת סופית לברת בין נוצרת הרחבה לברת בין נוצרת נוצרת החבה לברת לברת בין נוצרת הרחבה לברת לברת הרחבה לברת מוצרת הרחבה לברת בין מוצרת הרחבה לברת הרח

. חופית. נוצר וקטורי נוצר אפילו  $\mathbb{C}=\mathbb{R}[i]=\mathbb{R}(i)$ רי נוצר וקטורי נוצר אפילו כוצר רוב אפילו כוצר כופית. כוצר סופית.

נוצר סופית כשדה אבל לא נוצר סופית כחוג (דורש הוכחה) ואפילו  $\mathbb{C}[t]/\mathbb{C}$  לא נוצר סופית כפולינומים.

ולכן K או הרחבה באכו הרחבה של הממנה בינות, אז הדרגה של הדרגה של הרחבה שנסמנה בינות הרחבה של מרחב וקטורי מעל L $.\mathrm{dim}_K\,L=[L:K]$ 

$$\mathbb{Q}[\mathbb{C}:\mathbb{R}]=2$$
 (כמו ש־ $\mathbb{Q}\left(\sqrt{3}
ight):\mathbb{Q}$ ) (כמו ש- $\mathbb{R}$ ) (כמו ש- $\mathbb{R}$ ) (כמו

$$\left[\mathbb{Q}\left(\sqrt[3]{2}:\mathbb{Q}
ight)
ight]=3$$
 נראה בהמשך שמתקיים. 2

$$[K(t):K] = \infty .3$$

L/K בקראת סופית): הרחבה שדות סופית): הרחבה בתרה L/K נקראת הרחבה טופית שדות סופית)

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

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

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

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

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

K אם מעל גם הוא נוצר הוא בסיס של F/K סופי ו־L סופי ולכן אולכן בסיס של הבסיס של הבסיס מעל אולכן ולכן אולכן אולכן לכן או הבסיס מעל אולכן הרחבות סופיות אז השיוויון ממתקיים. נראה זאת באמצעות בניית בסיס:

 $\gamma_{ij}=lpha_ieta_j$ נוכיח ש", F/L בסיס של היים בסיס של בסיס מל בסיס מל בסיס ונבחר בסיס ונבחר בסיס ונבחר בסיס של בסיס ונבחר בסיס של בסיס ונבחר שפורש ובלתי־תלוי לינארית:

עם א $a_{ij}\in K$  עם א $b_j=\sum_{i=1}^n a_{ij}\alpha_i$  אז א $b_j\in L$  עם אב כ $c=\sum_{j=1}^m b_j\beta_j$  עם לייצוג על־ידי כל כל כל ניתן לייצוג על־ידי אוג על־ידי אוא מייצוג על־ידי אויצוג על־ידי אייצוג על־ידי אויצוג על־ידי אויצוג על־ידי אייצוג על־ידי אייצוג

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

.F/K את פורש  $\gamma_{ij}$  ולכן

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

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

ולכן שנעלם הביטוי אנא  $a_{ij}$  אז איז לינארית מעל בלתי־תלויים המכים, אבל אפסים, הם כולם הם הביטוי שנעלם אז אז א די אבל אבל בלתי־תלויים לינארית מעל אז אז אולכן זה מהווה בסיס מעל הם בלתי־תלויים לינארית מעל אז ולכן זה מהווה בסיס מעל הם בלתי־תלויים לינארית מעל אז איז המהווה בסיס מעל הם בלתי־תלויים לינארית מעל אז הם בלתי־תלויים לינארית מעל אז המהווה בסיס מעל הם בלתי־תלויים לינארית מעל אז המהווה בסיס מעל הם בלתי־תלויים לינארית מעל אז הם בלתי־תלויים לינארית מעל אז המהווה בסיס מעל הם בלתי־תלויים לינארית מעל אז המהווה בסיס מעל הם בלתי־תלויים לינארית מעל אז הם בלתי־תלויים בלתי־תלי־תלויים בלתי־תלויים בלתי־תליים בלתי־תלויים בלתי־תלויים בלתי־תלי

- 26/03 1 מרגול 3
- 3.1 חוג הפולינומים תזכורת
- 3.2 בניית שדות בעזרת מנות של חוגי פולינומים
  - E=F[x]/(f) חישוב בשדה 3.3

להשלים

1 תרגיל 4

טריקים 4.1

להשלים

4.2 מסקנות

להשלים

#### 31/03 - 3 הרצאה 5

#### 5.1 הרחבות אלגבריות

פרק 3.2 ברשומות של מיכאל.

כך שמתקיים להול אום אלגברי מעל איבר שר $\alpha$  נגיד ש $\alpha$  נגיד להול ו- $\alpha$  נגיד בהינתן בהינתן בהינתן: בהינתן כך בהינתן אוברי מעל אום אלגברי מעל אוברי מעל אוברי מעל אורת נגיד ש $\alpha$  נקרא טרנסצנדנטי מעל  $\alpha$ .

. $\mathbb Q$  אלגברי או טרנסצנדנטי אם אלגברי או טרנסצנדנטי אלגברי או אלגברי מעל  $lpha\in L$  אז אז  $lpha\in L$ 

.i אגם נוכיח שגם ב- $\frac{1}{778}, \sqrt[3]{5}, \sqrt[5]{3}+\sqrt[3]{5}:\mathbb{C}^{-}$ אלגבריים אלגבריים אלגבריים יובה :5.1 אלגבריים ב-

. טרנסצנדנטי או אלגברי, כי- זה מספר אי־רציונלי). אפילו אם  $e+\pi$  הוא אפילו אפילו מעניינת: לא ידוע עובדה מעניינת: אפילו אפילו אפילו אפילו או פרנסצנדנטי או אלגברי, כי- אי

. (ברור שאני בשדה שאני תלוי בשדה איבר אלגברי (ברור שלהיות  $\mathbb{Q}(e), \mathbb{Q}(e^5+e)$  ואפילו מעל  $\mathbb{R}^-$ ו ואפילו מעל שים אלגברי אלגברי אלגברי מעל

. מספר ליובים – כמו אוז – טרנסצנדנטי מדי" מובים "טובים רציונליים קירובים שאם שאם שאם הכללי הוא הרעיון מדי" או קירובים הציונליים אווליים מספר הרעיון הכללי הוא אווליים אווליים הישוא מספר היובים אווליים מספר הרעיון הכללי הוא שאם אווליים הרעיון הרעיון הכללי הוא שאם הרעיון הרעי

הגדרה של הבן־מנייה הגיוני: יש מספר בן־מנייה שלה שדה שהוא שדה ואף בן־מנייה הגיוני: יש מספר בן־מנייה של הגדרה 5.2  $\overline{\mathbb{Q}}$ :  $\overline{\mathbb{Q}}$ : יש מספר בן־מנייה של מספרים אלגבריים מעל  $\mathbb{Q}$ ).

Lב־ב.  $I=\{f\in K[t]\mid f(lpha)=0\}$  כאשר K[lpha]=K[t]/Iר שונית הרחבה  $I=\{f\in K[t]\mid f(lpha)=0\}$  כאשר  $I=\{f\in K[t]\mid f(lpha)=0\}$  הרחבה  $I=\{f\in K[t]\mid f(lpha)=0\}$  הוא אידיאל ראשי (נוצר על־ידי איבר אחד) כך ש $I=\{f\in K[t]\}$  חוג ראשי ו $I=\{f\in K[t]\}$  תחום שלמות אידיאל ראשוני אם ורק אם  $I=\{f\in K[t]\}$  תחום שלמות).  $I=\{f\in K[t]\}$  או אידיאל מקסימלי).  $I=\{f\in K[t]\}$  באשר  $I=\{f\in K[t]\}$  הוא אי־פריק או  $I=\{f\in K[t]\}$  ובכלל זה אידיאל מקסימלי).

אם  $\alpha$  אז  $\alpha$  אלגברי. אז  $\alpha$  טרנסצנדנטי ואם  $\alpha$  הוא אי־פריק אז  $\alpha$  אלגברי.

 $m{K}$  אם  $m{lpha}$  של מעל של הפולינומים שונים שונים פולינומים מינימלי של פולינום מתוקן מינימלי מינימלי מינימלי של  $m{lpha}$  אם קיימים פולינומים שונים מאפס שמתאפסים ב־ $m{lpha}$  אז יש פולינום מתוקן מינימלי מונימלי איזה שדה אנחנו מדברים (כאשר האחרון זו הצורה המועדפת), ברשומות מדי פעם זה מופיע גם בתור  $f_{m{lpha},K}$  או  $f_{m{lpha}}$  כדי להדגיש מעל איזה שדה אנחנו מדברים (כאשר האחרון זו הצורה המועדפת).

: עריך להתקיים: אריך מינימלי) אוא פולינום של- $f_{lpha/K}$  של-מנת על-מנת מינימלי) על-מנת מינימלי: על-מנת מינימלי: אריך להתקיים:

- $f_{\alpha/K}(\alpha) = 0$  .1
- פולינום מתוקן f .2
  - אי־פריק f .3

. (שדה יותר קטן) אם  $\deg(f)=1$  עם  $t-\sqrt{2}=f_{\sqrt{2}/\mathbb{Q}(\sqrt{2})}$  ,  $\deg(f)=2$  עם ב $t^2-2=f_{\sqrt{2}/\mathbb{Q}}$  : 5.2 אותר קטן).

 $f_{lpha/L}$ הוא מתחלק ולכן וגם  $f_{lpha/K}(lpha)=0$  וגם וגם הוא הוכחה:

. (או lpha אם lpha הוא טרנסצנדנטי) שמתאפסים ב־lpha (או lpha האידיאל של כל הפולינומים מעל a שמתאפסים ב־a האידיאל של האידיאל של הפולינומים מעל א

 $lpha \in L$ ו הרחבה ו-L/K למה :5.2 למה

- בסיס של 1,  $\alpha,\cdots,\alpha^{d-1}$ ו ר $(\alpha)=K[lpha]=K[t]/(f_lpha)$  אזי אזי  $d=\deg f_lpha$ ור ההווים מינימלי 1,  $\alpha,\cdots,\alpha^{d-1}$ ו רבפרט מתקיים d=[K(lpha):K]ו בפרט מתקיים ובפרט K(lpha)/K
  - $[K(\alpha):K]=\infty$ רי הא $K(t)\underset{t\mapsto\alpha}{\simeq}K(\alpha)$  אז אז טרנסצנדנטי  $\alpha$  אם .2

:הוכחה

 $K(\alpha)=K[\alpha]$  שדה ו־ $K[\alpha]=K[t]/(f_{lpha})$  שדה ו- $K[\alpha]=K[t]/(f_{lpha})$  שדה ו- $K[\alpha]=K[t]/(f_{lpha})$  שדה ו- $K[\alpha]=K[t]/(f_{lpha})$  שרית. ברשיו נחשב את המימד של  $K(\alpha)=K[t]/(f_{lpha})$  ונראה שמתקיים נחשב את המימד של  $K(\alpha)=K[t]/(f_{lpha})$  ונראה שמתקיים לכל K(t)=t באשר K(t)=t היא החלוקה עם שארית. לכל K(t)=t פולינום קיימים ויחידים K(t)=t בראה שזו העתקה לינארית: K(t)=t הוא שזו העתקה לינארית:

. . אותו הדבר לכפל בסקלר וקיבלנו העתקה לינארית ועל.  $r_{g+h}=r_g+r_h$  ולכן ולכן  $r_{g+h}=r(r_g+r_h)$  מתקיים  $g,h\in K[t]$  ואז ואכן ואכן ולכן (כמרחבים וקטורים) ולכן (כמרחבים ולכן והבסיס באן הוא  $f_{\alpha}\cdot K[t]=m_{\alpha}$  והבסיס באן הוא הוא בסיס. הוא בסיס.

 $K[lpha]\subset K(lpha)$ ו־  $K[t]=\operatorname{Frac}(K[t])\simeq\operatorname{Frac}(K[lpha])=K(lpha)\subset L$ ולכן אולכן  $K[t]\simeq K[t]/m_lpha\simeq K[lpha]$  (כי  $K[t]\simeq K[lpha]$  וילכן  $K[t]\simeq K[lpha]$  וילכן הוא  $\infty$ .

L= סך שמתקיים  $lpha\in L$  קיים איבר אחד, כלומר על־ידי איבר אם היא נוצרת נקראת הרחבה פרימטיבית נקראת נקראת ברחבה פרימטיבית אם היא נוצרת על־ידי איבר אחד, כלומר קיים L/K נקראת הרחבה פרימטיבית אם היא נוצרת על־ידי איבר אחד, כלומר קיים L/K נקראת הרחבה פרימטיבית אם היא נוצרת על־ידי איבר אחד, כלומר קיים L/K נקראת הרחבה פרימטיבית אם היא נוצרת על־ידי איבר אחד, כלומר קיים L/K נקראת הרחבה פרימטיבית אם היא נוצרת על־ידי איבר אחד, כלומר קיים על־ידי איבר אחד, כלומר קיים ברומטיבית אחד, כלומר קיים ברומטיבית אם היא נוצרת על־ידי איבר אחד, כלומר קיים ברומטיבית אחד, ברומטיבית אורטיבית אחד, ברומטיבית אורטיבית אחד, ברומטיבית אחד, ברומטיבית אחד, ברומטיבית אחד, ברומטיבית אחד, ברומטיבית אחד, ברומטיבית אורטיבית אחד, ברומטיבית אחד, ברומטיבית אחד, ברומטיבית אחד, ברומטיבית אורטיבית אחד, ברומטיבית אורטיבית אחד, ברומטיבית אחד, ברומטיבית אחד, ברומטיבית אחד, ברומטיבית אורטיבית אור

Lב שורש ב' f כך של כ' כ' אם ב' ב' או אי־פריק אז קיימת אי־פריק איי־אי־פריק אי־פריק אי־פריק אי־פרי

מלמה f, מלמה הרחבה פרמיטיבית הנוצר על-ידי שורשי  $g:K \to L'$  שהוא שיכון על-ידי שורשי L'=K[t]/(f(t)) הוא הרחבה פרמיטיבית הנוצר על-ידי שורשי L/K היא הרחבה פרימיטיבית הנוצרת של מיכאל), יש הרחבה על-ידי שורש של L/K ולכן L/K היא הרחבה פרימיטיבית הנוצרת על-ידי שורש של  $f_{\alpha}=f$  הא הרחבה פרימיטיבית שורשי של  $f_{\alpha}=f$  הא הרחבה פרימיטיבית של  $f_{\alpha}=f$  הרחבה פרי

(K[lpha]:K אומר זה אומר שראינו מהלמה של איבר) איבר (מהלמה של lpha/K היא הדרגה של הדרגה של איבר): עבור אלגברי, הדרגה של מארגברי היא היא ממר (מהלמה שראינו איבר) אומר הדרגה אומר אומר (מהלמה שראינו איבר).

K הרחבות שדות. (גיד שההרחבה אלגברית הברות: תהיי אלגברית שדות. הרחבות שדות. הרחבות הרחבות הרחבות אלגברית מעל

למה שדות, שדות, אז L/K יהרחבות שדות, אז

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

:הוכחה

- . $\alpha$ מתאפס של ל-ט מדרגה קטנה/שווה פולינום איברים) של תלות לינארית של איברים) איברים (ש כאן d+1 איברים) איברים לוע ביך .d+1 איברים לראות את לראות את זה  $\deg_K(\alpha) = [K(\alpha):K] \mid [L:K]$  איברים אפשר לראות את זה
  - 2. מתקיים

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

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 K אלגבריים מעל  $\alpha, \beta \in L$ יו האחרון מוגדר) אם אלגבריים מעל  $\alpha, \beta \in L$ יו מעל אזי מסקנה בי-1.3 אלגבריים מעל  $\alpha, \beta \in L$ יו אלגבריים מעל אווה ל $\deg_K(\alpha) \cdot \deg_K(\beta)$ , שקטנה שווה ל $\deg_K(\alpha) \cdot \deg_K(\beta)$ , ובפרט קבוצת כל המספרים האלגבריים בי-1 מעל

על יש חסם על אלגברי ואפילו כל  $\gamma \in K(\alpha,\beta)$  ולכן כל  $\deg_K(\alpha) \cdot \deg_K(\beta) \geq [K(\alpha,\beta):K]$  אלגברי ואפילו יש חסם על  $\deg_K(\gamma) \leq \deg_K(\alpha) \cdot \deg_K(\beta)$  הדרגה שלו, הדרגה שלו, ואפילו יש הסם על

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

 $\deg_{\mathbb{Q}}\left(\sqrt[3]{3}+3\right)$  ולכן מהמסקנה ( $x^3-3,x^2-2$  הוכחה: זה נובע מכך שלגבריים שניהם אלגבריים בהרחבה השורשים של הפולינומים  $\sqrt[3]{3}+3$  הם שניהם אלגבריים בהרחבה (השורשים של  $\sqrt[3]{2}+3$ 

השיוויון 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).

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

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

מסקנה שקולים עבור הרחבת שדות שדות :5.2 עבור הרחבת מסקנה יעבור הרחבת שקולים מסקנה אוני שקולים יעבור הרחבת שדות שחורים יעבור הרחבת שקולים יעבור הרחבת שחורים יעבור הרחבת שקולים יעבור הרחבת שחורים יעבור הרחבת שחורים יעבור יע

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

12

. (אפילו כמרחב אלגברית (שראינו לעיל) ונוצרת שראינו (מהלמה על הדרגות לאגברית מהלמה אלגברית אז היא אלגברית סופית ונוצרת סופית אלגברית (מהלמה על הדרגות שראינו לעיל) אונים אלגברית (מהלמה אלגברית מהלמה שראינו לעיל) ונוצרת אונים אלגברית (מהלמה שראינו לעיל) אונים אלגברית (מהלמה שראינו לעיל) ונוצרת הוא אלגברית הוא אלגברית (מהלמה שראינו לעיל) ונוצרת הוא אלגברית הוא אלגבר

. מיידי מהגדרה:  $2 \Rightarrow 3$ 

 $\square$  . ולכן סופית. [L:K]  $\leq \prod_{i=1}^n \deg_K(lpha_i) < \infty$  שראינו אזי מהלמה אלגבריים. אלגבריים כאשר באלגבריים כאשר באנית בול באלגבריים לאלגבריים. כאשר באלגבריים לאלגבריים באלגבריים לאלגבריים לאלגבריים וולכן פופית.

מסקנה אלגבריים אר ורק אם ורק אלגבריים מגדל הרחבות. היהיה אלגבריות: יהיה אלגבריות: הרחבות אלגבריות אלגבריות: אלגבריות: אלגבריות: אלגבריות אלגבריות אלגבריות: אלגבריות מגדל הרחבות אלגבריות: אלגבריו

הורות שירות שירות אלגבריות ברוב ברות שירות אלגבריות אלגבריות שירות אלגבריות אלגבריות אלגבריות הוכחה:

$$.\beta_1,\cdots,\beta_d\in L$$
עם  $0=\alpha^d+\beta_1\alpha^{d-1}+\cdots+\beta_d=0$ 

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

אלגברי) אלגברי מהיות פרימטיבית סופיות סופיות סופיות מגדל הרחבות מגדל שקיבלנו מגדל טופיות לב

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

אז מהלמה שראינו על כפליות הדרגה

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

נשים לב שהוכחנו שמחלקות של הרחבות סופיות ואלגבריות היינן שלמות.

02/04 - 2 תרגול 6

6.1 משהו

להשלים

# 07/04 - 4 הרצאה 7

# 7.1 שימושים בסיסיים של תורת השדות – בניות עם סרגל ומחוגה

אני לא אוהבת לצייר, אז אני אוותר.

#### 08/04 - 5 הרצאה 8

#### 8.1 למות גאוס

הערה: אנחנו נעבוד 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).

היות של f של תכולה) נגדיר ( $f(t) = \sum_{i=0}^n a_i t^i$  (תזכורת:  $f(t) \in \mathbb{Z}[t]$  עבור פולינום עבור (תכולה) אודרה 8.1 (תכולה) פולינום (תכולה) אודרה אודרה (תכולה) אודרה

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

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

. בייטיבים פרימיטיבי אוא פולינום כאשר  $f=\mathrm{cont}(f)\cdot f_0(t)$  בידי על־ידי בירוק פרימיטיבי פירוק פרימיטיבי. לכל פולינום פרימיטיבי

. פרימיטיבי אם f ורק אם f ורק אם הראשונה): אז הראשונה): אזי פרימיטיבי אזי אזי פרימיטיבי אזי פרימיטיביים.

: ברימיטיבי הוא  $f \cdot g = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$  הוא פרימים לעיל מההערה הוכחה: הוכחה הוא פרימיטיבי

נניח שלא ולכן קיים  $f_0=\sum_{i=0}^n a_it^i, g_0=\sum_{j=0}^m b_jt^j$  אבל  $p\mid \mathrm{cont}(f_0\cdot g_0)$  הם פרימטיביים פרימטיביים עלא ולכן קיים  $p\notin \mathbb{N}$  הם פרימטיביים  $p\nmid a_n$  מינימליים כך שm,n מינימליים ב־ $(p\mid a_i,b_j)$  מתחלקים ב־ $(p\mid a_i,b_j)$  ולכן נוכל לבחור מינימליים כך ש

נסתכל על המקדם של  $f_0\cdot g_0$ ב ב'  $t^{m+n}$  של  $c=\sum_{k=0}^{m+n}a_kb_{m+n-k}$  נסתכל על המקדם של

$$\underbrace{a_0b_{m+n}+...+a_{n-1}b_{m+1}}_{\text{kn}}$$
מתהלקים ב־ק כי  $p|a_k$  לכל מ-ג לכל מרא מתהלקים ב-ק כי  $p|b_k$  לכל מ-ג לכל מרא מתהלקים ב-ק כי  $a_nb_m$ 

. הירה סתירה אבל  $p\nmid c$ ולכן ב־<br/> pלהלוקה לחלוקה זר  $a_nb_m$ אבל

. מסקנה 1.2.5 ברשומות של מיכאל).  $\mathbb{Z}[t]$  (לא ראינו ב-ברצאה, מסקנה 1.2.5 ברשומות של מיכאל). מסקנה 1.2.5 באשוני ב-

 $p \mid \mathrm{cont}(h)$  אם ורק אם  $h \in \mathbb{Z}[t]$  מחלק פולינום  $p \notin \mathbb{Z}^{ imes} = \mathbb{Z}[t]^{ imes}$  אם ורק הוכחה: נשים לב

 $p\mid g$  או  $p\mid f$  ולכן  $p\mid \mathrm{cont}(f)\cdot\mathrm{cont}(g)$  אם אונה הראשונה אוס אז מלמת או  $p\mid f\cdot g$  אם

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

 $\mathbb{Z}[t]$ 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  $0
eq c\in \mathbb{Q}^{ imes}$  אזי קיים  $\mathbb{Q}[t]$  אזי קיים  $f=g\cdot h$  אם .1

 $g,h\in\mathbb{Z}[t]$  אזי אחוקנים) אויי הרוק פירוק פירוק פירוק  $f=g\cdot h\in\mathbb{Q}[t]$ ו אזי מתוקנים בולינום f. 2

 $\mathbb{Q}[t]$ ב-יק הי־פריק פרימטיבי f אם ורק אם  $\mathbb{Z}[t]$ ב- הי־פריק פולינום f אם .3

הוכחה:

 $m\cdot n\cdot f=m\cdot g\cdot n\cdot h$  אוז נקבל פירוק וויקם  $m\cdot g,n\cdot h\in\mathbb{Z}[t]$  כך ש־ $0< m,n\in\mathbb{Z}$  וניקה  $g,h\in\mathbb{Q}[t]$  עבור  $f=g\cdot h$  את הפירוק .1 ניקה את גאוס הראשונה נקבל עם כפליות התכולה  $\ell=\mathrm{cont}(f), \alpha=\mathrm{cont}(m\cdot g), \beta=\mathrm{cont}(n\cdot h)$  נסמן

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

 $f = \ell \frac{m}{lpha} \cdot g \cdot \frac{n}{eta} \cdot h$  משמע ונחלק ב $\ell = \frac{m \cdot n \cdot f}{m \cdot n \cdot \ell} = \underbrace{\frac{m}{lpha} \cdot g \cdot \frac{n}{eta} \cdot h}_{\in \mathbb{Z}[t]}$  ונחלק ב $\ell = 0$  ונחלק ב

. עם g,h עם  $f=g\cdot h\in \mathbb{Q}[t]$  עם פרימיטיבי, ולכן פרימיטיבי, ולכן בפרט הוא מתוקן, ולכן בפרט הוא 2.

 $f=c\cdot g\cdot c^{-1}\cdot h$ כך שיר כך כך כך ער כך כך ער כך כך כך כך כך כך כלפי (1) נובע שקיים לפי

נסמן פולינומים  $a_nb_m=1$  היות היות  $g=\sum_{i=1}^na_it^i,h=\sum_{j=1}^mb_jt^j$  נסמן נסמן  $g,h\in\mathbb{Z}[t]$  היות היות היות  $g,h\in\mathbb{Z}[t]$  מתוקנים ולכן בהכרח היות ולכן בובע כי  $g,h\in\mathbb{Z}[t]$ 

3. (הוכח בהרצאה 6)

f ולכן  $\mathrm{cont}(f)$  ולכן לכן  $\mathrm{cont}(f)$  ולכן לבים הפיך לביח פירוץ פירוק שירוויאלי ונשים לב $\mathrm{cont}(f) \cdot \frac{f}{\mathrm{cont}(f)}$  ולכן  $\mathbb{Z}[t]$  ולכן ביינון לבין לביח הפירואיניני

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

:פעריים: 2 מקרים עם פעריים: עם g,hעם לg,hעם לכן ולכן פריק פריק פריק פריק אפשריים: שבייום:  $\mathbb{Z}[t]$ 

חאת סתירה פירוק על־ידי פירוק פריק פריק פריק וואת פובע אם  $\deg(f), \deg(g) > 0$  .1

סתירה שוב וזאת אל f אבל או  $1 < h \in \mathbb{Z}_+$ ולכן ולכן ולפת שוב וזאת הכלליות בליטיבי וזאת ולכן .2

 $\mathbb{Z}$  של הוא חוג פריקים אי־פריקים שלו הם פולינומים שלו הם הראשוניים של פריקות יחידה והראשוניים שלו הם פולינומים פריקים הוא מסקנה  $\mathbb{Z}[t]$  הוא גם תחום פריקות יחידה מוכיחים שאם R תחום פריקות יחידה אזי גם  $R[t_1,...,t_n]$  הוא גם תחום פריקות יחידה שאם מסקנה שלו פריקות יחידה אזי גם הוא גם תחום פריקות יחידה שאם מסקנה שלו פריקות יחידה אזי גם מסקנה באותה בשום פריקות יחידה שלו פריקות פריקות שלו פריקות שלו פריקות שלו פריקות פריקות שלו פריקות שליקות שלו פריקות שלו פריקות של פריקות של פריקות של פריקות של פריקות שליקות של

9 תרגול 3 – 90/04

9.1 משהו

להשלים

2 תרגיל 10

10.1 טריקים

להשלים

10.2 מסקנות

להשלים

#### 21/04 - 6 הרצאה 11

## $\mathbb{Q}[t]$ ־קריטריונים לאי־פריקות ב11.1

המוטיבציה שלנו היא מקיום שורש ב־ $\mathbb{Q}$ : דוגמה 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  $R/I=\overline{R}$  $a_i f = \sum_{i=0}^n a_i t^i \mapsto \sum_{i=0}^n \overline{a_i} t^i = \overline{f}$  כאשר  $R[t] o \overline{R}[t]$  מתרחב להומומורפיזם מתרחב להומומורפיזם

א־פריק. אי־פריק הומומורפיזם של זה הומומורפיזם  $\overline{f}\in\mathbb{F}_{p}[t](t)$  אי־פריק. ראשוני כך פולינום מתוקן, אי־פריק. פולינום מתוקן פולינום מתוקן.  $\mathbb{Q}[t]$ אזי f אי־פריק ב

 $\mathbb{Q}[t]$  ולכן קיים פירוק מתוקן  $\mathbb{Q}[t]$  מתפרק ב־ $\mathbb{Q}[t]$  מתפרק בין ולכן קיים פירוק מתוקן מתוקן מתפרק בי

(2) בלמת גאוס השנייה נובע כי  $f=g\cdot \overline{h}\in \mathbb{F}_p[t]$  ואז  $f=g\cdot h\in \mathbb{Z}[t]$  כי הפולינומים מתוקנים וזאת סתירה.  $f=g\cdot h\in \mathbb{Z}[t]$  $\mathbb{F}_p[t] = \mathbb{Z}[t]/p\mathbb{Z}[t]$  : 11.1 תרגיל

f(t) המתקבל על־ידי הפחת כל מקדם ב־f(t) המודלו אה הפולינום המתקבל על־ידי  $\varphi: \mathbb{Z}[t] o \mathbb{F}_n[t]$  המודלו למודלו גדיר הם שבמודלו קלה אלו כל הפולינומים שבמודלו אלו  $\ker(arphi)=\{f(t)\in\mathbb{Z}[t]\mid arphi(f)=0\in\mathbb{F}_p[t]\}$  אלו כל הפולינומים שבמודלו קלה מראה כי זה אכן הומומורפיזם ונשים לב כי מתאפסים משמע מתחלקים ב $p^-$  ולכן  $p^-$ ולכן  $p^-$  ממשפט האיזומורפיזם ולכן מתאפסים נקבל מתאפסים משמע מתחלקים ב

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

באים הבאים כך שמתקיימים ראשוני כך פניח אייזנשטיין ((Eisenstein's criterion) נניח הבאים: ( $p\in\mathbb{N}$ ריטריון אייזנשטיין: (נניח ש־11.1 (קריטריון אייזנשטיין) אייזנשטיין וניח ש

 $p \nmid a_n$  .1

 $0 \leq i < n$  לכל  $p \mid a_i$  .2

 $p^2 \nmid a_0$  .3

.אז f אי־פריק

 $f=g\cdot h=\sum_{j=1}^m b_j t^j \sum_{k=1}^l c_k^{t^k}$  הוכחה: נניח בשלילה שלא כך, ולכן מהלמות של גאוס נובע שמתקיים ב"ב מתקיים הוכחה: נניח בשלילה שלא כך, ולכן מהלמות של גאוס נובע מיניח ב"ב הגבלת הכלליות, נניח כי  $p \mid a_0$  ולכן אבל  $p \mid a_0$  אבל  $p \mid a_0$  ולכן לא ניתן שגם היות ור $a_0=b_0c_0$ ורים ב"ב מיניח ב"ב הגבלת הכלליות, נניח כי מיניח ב"ב  $.(p \mid c_0$  וגם  $p \mid b_0$ 

 $.p \nmid b_m$ ולכן  $b_m c_l = a_n$ מהיות מהיים  $p \mid b_i$ יש כך ביותר הקטן הקטו ניקה את ניקה ניקה את ה

כעת, בביטוי  $p \nmid a_i$  אבל אז  $a_i = b_i c_0 + \underbrace{b_{i-1} c_1 + ... + b_0 c_i}_{\text{מתחלקים ב־q}}$  כעת, בביטוי מתחלקים ב־ק  $a_i = b_i c_0$  אז  $a_i = b_i c_0$ 

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

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

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

לכל של המינימלי המינימלי של שלמים שלמים מתוקן בעל פולינום שהוא פולינום שהוא שהוא פולינום שהוא פולינום שהוא חבר שהוא לכל של שהוא פולינום שהוא פולינום שהוא פולינום מתוקן שהוא לכל של כל השורשים שהוא פולינום מתוקן בעל מקדמים שהוא פולינום מתוקן שהוא פולינום מתוקן בעל מקדמים שהוא פולינום מתוקן שהוא פולינום מתוקן בעל מקדמים שהוא פולינום מתוקן בעל מתוקן בעל מקדמים שהוא פולינום מתוקן בעל מתוקן ב a מסדר מסדר הפרימיטיביים מסדר על עובר על כאשר a עובר על השורשים מסדר חפרימיטיביים מסדר  $\Phi_n(X) = \prod_\omega (X-\omega)$ 

#### : 11.2 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  $p^n$  הוא מסדר מסדר פולינום הציקלוטומי, אז כל פולינום האיקוני, אז בור  $p\in\mathbb{N}$  השלמה מויקיפדיה עבור p ראשוני, אז אז  $p=\sum_{k=0}^{n-1}x^k$  עבור p עבור p עבור p עבור p עבור p בראשוני מתקיים p

20

 $\mathbb{Q}$  אי־פריק למה למה אי־פריק אי־אי־טריק אי־יק אי־אי־טריק אי־יק אי־טריק אי־יק אי־אי־טריק אי־טריק אי־טריק אי־טריק אי־טריק אי־טריק אי־טריק אי

ואז נקבל ואז t=x+1 ואז x=t-1 ואז נקבל משתנה זה זה טריק, נשנה משתנה או

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

0 < i < p לכל  $p \mid \binom{p}{i}$  אי־פריק מתוקן מקדם שכן שכן שכן אייזנשטיין לפי קריטריון איידפריק איז איז אייזנשטיין אייזנשטיין אייזנשטיין איי

האת סתירה פריק, אז  $\Phi_p(t) = g(t) \cdot h(t) = g(x+1) \cdot h(x+1)$  הואת קיימים לא  $\Phi_p(t)$ אם אם  $\Phi_p(t)$ 

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

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

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

 $x^p-a$ יש בקבל איזנשטיין אם קריטריון איזנשטיין אנחנו נעמוד בכל הדרישוני, אנחנו עבור a עבור עבור הפולינום איזנשטיין איזנשטיין איזנשטיין אנחנו עבור a עבור עבור  $x^p-a$  עבור  $x^p-a$  עבור איזנשטיין אנחנו בכל הדרישות איזפריק מעל  $x^p-a$  עבור  $x^p-a$  ע

תרגיל פעולת המתקבל המתקבל האה  $\overline{f}\in\mathbb{F}_p[x]$ . נסמן ב־ $f\in\mathbb{Z}[x]$  פולינום ויהי (האשוני ויהי בספר): יהי  $p\in\mathbb{N}$  יהי בספר): יהי מודלו (תרגיל 10.108 בי מודלו p

- . הוכיחו כי אם  $\overline{f}$  גם ג<br/>ם פריק, אז מם fפריק. 1
- . פריק, לאו דווקא f פריק, לאו פריק, אם  $\overline{f}$  פריק. 2

הוכחה: להשלים.

### 11.2 סגור אלגברי

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

Kיש שורש ב־K שורש כלכל פולינום אם לכל פולינום לא נקרא שדה סגור אלגברי): שדה א נקרא שדה סגור אלגברית אם לכל פולינום אורש ב

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

$$a_i \in K$$
בל האשר  $a_i \in K^ imes$  רכל  $f = c \prod_{i=1}^{\deg(f)} (t - a_i)$  משמע,

לים שקולים הבאים אבור שדה בור יעבור יעבור למה למה לור: 11.3

- 1. סגור אלגברית
- טין לחלוטין מתפצל מתפצל  $f \in K[t]$  מתפצל לחלוטין .2
  - 1 אי־פריק הוא מדרגה  $f \in K[t]$  .3
- אין הרחבות אלגבריות לא טריוויאליות K- 4
- הירפריקים. שכן ממיד ש פירוק לפולינומים אי־פריקים. שכן  $(2) \Longleftrightarrow (3)$ 
  - . שורש לי שיש מהגדרה נובע פירוק פירוק פירוק אם יש פירוק: $(1) \Longleftarrow (2)$
- $\deg(f)$ עם אינדוקציה את ומסיימים  $\deg g < \deg f$ יש פירוק פירוק שלכל שלכל נובע שלכל יש פירוק פירוק פירוק פירוק יש יש פירוק וובע שלכל (2)
- 1 < [K(lpha):K] אי־פריק מדרגה אי־פריק אוז הפולינום אי ניקבל ביקב ניקבל עריוויאלית אלגברית אל מריוויאלית מרחבה אלגברית מיימת הרחבה אלגברית אל מריוויאלית ביקבל אוויאלית מרייע מיימת הרחבה אלגברית אל מרייע מיימת ביקב אוויאלית מרייע מיימת אלגברית אל מרייע מיימת מי
  - $.[L:K] = \deg(f) > 1$ ו בL = K[t]/(f) נגדיר נגדיר פריק וי $\deg(f) > 1$ ים אי־פריק וי $\deg(f) > 1$ : אם אי־פריק וי

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

משפט ברית.  $\mathbb{C}$  המשפט היסודי של האלגברה):  $\mathbb{C}$  המשפט 11.2

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.

#### : 11.1 מסקנה

- . בועיים וריבועיים של גורמים מכפלה מתפרק מתפרק מתפרק  $\mathbb{R}[t]$  מתפרע היים פולינום ל
  - (דיסקרמיננטה)  $\mathrm{dic} < 0$  עם וריבועיים וריבאריים הם  $\mathbb{R}[t]$ הם ב-

השורשים אל האמדה רק ההצמדה לב  $f=\overline{f}=\mathbb{R}[t]\subseteq\mathbb{C}[t]$  נשים לב 1: נשים לק מספיק שנוכיח רק מספיק שנוכיח לב ברור, ולכן מספיק שנוכיח רק את  $f=\overline{f}=\mathbb{R}[t]$  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

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

 $\overline{a_i} \in \{a_i \mid 0 \leq i \leq n\}$  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,

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

ושל ממשיים ממשיים לינאריים של מכפלה של הוא f הוא כלומר

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

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

 $F=\{lpha\in L\mid K$  מסקנה מעל אלגברי סגור אלגברית סגור סגור סגור הרחבה, לוניח כי בניח נניח מסקנה ונגדיר לא

.Lב־ל (Algebraic closure) של הסגור האלגברי נקרא נקרא נקרא אל על אלגברית סגור אלגברית אלגברית אל

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

#### : 11.3 דוגמה

 $\mathbb{Q}$  אלגברית מעל  $\mathbb{Q}$  ולכן גם סגור אלגברית מעל .1

$$\mathbb{C}=\overline{\mathbb{R}}=\overline{\mathbb{C}}$$
 .2

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

#### 22/04 - 7 הרצאה 12

#### 12.1 קיום ויחידות סגור אלגברי

. סגור אלגברי,  $\overline{K}$  סגור איזומורפיזם עד־כדי היחיד עד־כדי שלנו הקרוב המטרה שלנו בזמן הקרוב זה להראות שלכל שדה איזומורפיזם המטרה שלנו בזמן הקרוב זה להראות שלכל היחיד עד־כדי איזומורפיזם המטרה 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.

 $_{i}B$ יבר ב־ $_{i}B$ , של הפונקציה הוא תת־קבוצה של  $_{i}B$  שהיא קבוצות של המקורות של איבר ב- $_{i}B$ , סיב ב- $_{i}B$ , סיב ב-וצת המקורות של איבר ב- $_{i}B$ , סיב ב-וצת המקורות של איבר ב- $_{i}B$ , סיב ב-וצת 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  $\varphi:G o H$  הם בידיוק המחלקות של הגרעין G/Nיש מבנה של חבורה.

 $|L| \leq \max\{\kappa, leph_0\}$  אזי ו $\kappa = |K|$ , אלגברית, הרחבה L/Kה שדה למה 12.1 נניח כי

המנייה. בת־מנייה ו־L|X| > |K| מופית היחידי שיתקיים לכן, המקרה היחידי שיתקיים לכן, המקרה היחידי שיתקיים

 $\kappa^{d+1}$  של מעוצמה איז לכל היותר לכל מדרגה הפולינומים הפולינומים K[t] את גבחן את הוכחה:

. $|K[t]|=\kappa$  ולכן של של איז בן־מנייה איחוד במקרה שבו גם במקרה וזה נכון משיקולי עוצמות משיקולי אינסופית, אז אינסופית, אז אינסופית או אינסופית או אינסופית או נכון אינסופית או אינסופית אינסופית או אינסופית או אינסופית אינסופית או או אינסופית או או אינסופית או אינסופית או אינסופית או אינסופית או אונסופית או אינסופית או

נשים לב שהעתקה זאת ממפה לסיבים סופיםם (שכן המקור של כל פולינום  $f\in K[t]$  מכיל את כל השורשים שלו ב- $(L^-)$ , ולכן

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

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

.(universe כאשר U מלשון (כאשר  $U > \max\{|K|, \aleph_0\}$ כך ש־ $K \subset U$  מלשון הוכחה:

בהן את V, קבוצת כל השלשות  $(L,+,\cdot)$  משמע קבוצת כל תתי־הקבוצות את את  $K\subseteq L\subset U$  ופעולות משמע קבוצת כל משמע השלשות ( $L,+,\cdot$ ) משמע קבוצת כל הרחבה ארגברית L (L בפרט את L בפרט את L לשדה ואפילו להרחבה אלגברית ארגברית ובפרט בפרט את בפ

נסדר באמצעות על (משמע F/L הרחבת שדות אם הפעולות על מסכימות על הרחבת הרחבת אם הרחבת  $L\subseteq F$  אם הרחבת שדות ולא הרחבת הרחבת קבוצות) ולכן C היא קבוצה סדורה חלקית.

נניח בנוסף כי  $a,b\in L$  מוכל ב $I_i$  שרשרת של שדות ולכן קיים לה חסם עליון  $L=\cup_{i\in I}L_i$  (ואכן, כל  $I_i$  מוכל ב $I_i$  עבור  $I_i$  עבור  $I_i$  כלשהו,  $I_i$  בניח בנוסף כי  $I_i$  שרשרת של שדות ולכן קיים לה חסם עליון  $I_i$  מוכל ב $I_i$  כלשהו ולכן אלגברי מעל  $I_i$ . ונגדיר מכפלה ואז נקבל כי  $I_i$  הוא סגור אלגברית ולכן אלגברי מעל  $I_i$ : נניח שלא כך, ולכן קיימת הרחבה לפי הלמה של צורן, קיים איבר מקסימלי  $I_i$ :  $I_i$ : מהלמה לעיל נובע שקיים שיכון (של קבוצות)  $I_i$ : שמרחיב את ההכלה  $I_i$ : אוז סתירה להנחה כי  $I_i$ : חסם-עליון.

. הרחבות. לעיל ש $L/\overline{K}/K$  מגדל הרחבה אלגברית שכן הרחבות לעיל שלישל ההוכחה השתמשנו השתמשנו הרחבות.

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

K ושיכון של  $F_i\subseteq L$  התרישדות הרמה מקסימלית את לה הסתכל על הסתכל על התתישדות התחה אל להערישדות הרמה המסימלית הרמה המסימלית בסתכל להערישדות בסתכל המסימלית החלקי:  $\{(F_i,\phi_i)\}_{i\in I}$  אם החלקי:  $\{(F_i,\phi_i)\}_{i\in I}$  אם החלקי:  $\{(F_i,\phi_i)\}_{i\in I}$  היותר מזה לכל שרשרת החלקי:  $\{(F_i,\phi_i)\}_{i\in I}$  המסת עליון הנתון על-ידי  $\{(F_i,\phi_i)\}_{i\in I}$  היותר אם החלקיים המסת עליון הנתון על-ידי החלקיים החלקים החלקיים החלקים החלקי

: מהלמה של איבר איבר מקסימלי ( $F,\phi$ ) ונטען כי ונטען איבר השיכון איבר מקסימלי איבר ונטען ( $F,\phi$ ) ונטען איבר מקסימלי

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

של מתירה מתירה את אבל אבל , $\psi:F(lpha) \hookrightarrow F'(eta) \subseteq E$  משמע אל של על־ידי שליחה של על־ידי אבל אנחנו יכולים להרים אנחנו על־ידי שליחה על על־ידי אליחה על על־ידי אנחנו יכולים ( $F,\phi$ )

.28/04 ב-22/04 התחילה בהרצאה של ה-22/04 הסתיימה ב-28/04

# 23/04 – 4 תרגול 13

## 13.1 שדות פיצול

$$\omega=rac{1}{2}+\sqrt{rac{3}{4}}i$$
 כאשר  $\sqrt[3]{2},\omega\sqrt[3]{2},\omega\sqrt[3]{2}$  הם  $f(x)=x^2-2\in\mathbb{Q}[x]$  כאשר ווגמה 13.1 השורשים של  $L=\mathbb{Q}\left(\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}
ight)$  הוא  $f$  הוא  $f$  הוא ל

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

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

להשלים

#### 28/04 - 8 הרצאה 14

#### 14.1 קיום ויחידות סגור אלגברי – המשך

המינימלי הפולינום המינימלי ההרמה) בנוסף למת ההרמה): בנוסף להנחות של למת ההרמה, נניח כי גם מתקיים בוסף למת ההרמה): בנוסף להנחות של למת ההרמה, נניח כי גם מתקיים ל $\varphi:L\hookrightarrow E$  שיכון לבחור את ה־E שיכון לבחור את ה־E ביE ביE ביE בית לבחור את ה־E בית לבחור את ה-E בית לבחור

 $.\phi_0:K(lpha)\hookrightarrow K(eta)\subseteq E$  הוימומורפיזם ולכן של לנו הפיך, של לנו אי־הפיך פולינום של פולינום אי־הפיך על את הפולינום המינימלי של כל  $f_eta=f_lpha$  מעל מעל מתפצל את מעל מעל אולכן מתפצל לחלוטין מעל מעל אולכן מתפצל לחלוטין מעל אולכן מתפצל לחלוטין מעל גיינום המינימלי של אולכן מתפצל לחלוטין מעל פולינום המינימלי של אולכן מתפצל לחלוטין מעל פולינום המינימלי של אולכן מתפצל לחלוטין מעל פולינום המינימלי של הפולינום המינימלי של האולכן מעל פולינום המינימלי של האולכן מעל פולינום המינימלי של פולינום המינימלים פולינום פול

. הנדרש.  $\phi$  את קיבלנו קיבלנו  $\phi L \hookrightarrow E$  הנדים להומומורם  $\phi_0: K(\alpha) \hookrightarrow E$  הנדים ההומומורפיזם לכן, מלמת ההרמה

 $.\phi:\overline{K}\hookrightarrow\overline{K}'$  שיכון  $\overline{K}'$  שיכון מלא מתפצל לחלוטין מעל  $\overline{K}'$ , מלמת ההרמה וכקבל פולינום  $f\in K[t]$  מתפצל פולינום ההרמה (bootstrap) אבל הוא סגור אלגברית ומלמת ההרמה ( $\overline{K}'/\phi(\overline{K})$  הוא אלגברית האלגברית ומלמת ההרמה ( $\overline{K}'/\phi(\overline{K})$  הוא אלגברית ומלמת החים ( $\overline{K}'/\phi(\overline{K})$ 

היא  $\overline{K}'/K$  היחבה שההרחבה אלגברי מעל אלגברי הוא לא אלגברי מעל  $\overline{K}$  כי  $\overline{K}$  סגור אלגברי מעל אם לא, שבל הנחנו שההרחבה  $x\in \overline{K}'\setminus \overline{K}$  היא אלגברית וזו סתירה.

:דינו אל  $\sigma$  אבל סגור איזומורפיזם עד־כדי יחיד היינו היינו אלגברי אלגברי הערה:

ניתן לקחת את  $\mathbb Q$  ולבנות ממנו את  $\mathbb R$ , אבל אין לו אוטומורפיזמים.

."נכון".  $\mathbb C$  ואז אין  $lpha\mapsto\overlinelpha$  ואז אר ההצמדה אוטומורפיזם אוטומורפיזמים אוטומורפיים אוטומומורפיים אוטומומורפיים אוטומומיים אוטומומומיים אוטומורפיים אוטומורפיים אוטומומורפיים אוטומו

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

פרק 5.5 ברשומות של מיכאל.

 $\operatorname{Aut}_K(L)$  בתור הרחבת לפעמים את לפעמים את נסמן לעלו נסמן לבות נסמן לעלות נסמן לעלות לעלות את נסמן לעלות את סימון: עבור הרחבת שדות לעלות נסמן את נסמן לעלות את החבת שדות לעלות לעלות לעלות החבת לעלות לעלות את החבת לעלות לעלות

 $f_{lpha/K}=f_{eta/K}$  אם אם צמודים החבת כי בי כי גיד לגיד, עבור הרחבת שבור אבור (איברים צמודים אברים לאבור הרחבת שדות אבור הרחבת שדות אבור (איברים צמודים אם אבור הרחבת שדות אבור הרחבת אב

הצמודים שלו (קבוצת כל השורשים שלו ב-L/K מתפצל לחלוטין הרחבת שלו (קבוצת כל הצמודים) אז קבוצת כל האורשים שלו (קבוצת כל הצמודים) אז קבוצת ב-L/K מחלקת אמידות של  $(C_{lpha})$  מסומנת ב- $(C_{lpha})$ , מחלקת שלי של מסומנת ב- $(C_{lpha})$ 

 $C_{lpha}$  משפט 14.2 אם  $Autig(\overline{K}/Kig)$  אם המסלול שלו תחת הפעולה  $\alpha\in\overline{K}$  אז לכל אז לכל  $\overline{K}/K$  סגור אלגברי שלו, אז לכל  $\overline{K}/K$  המסלול שלו תחת הפעולה של  $\overline{K}/K$  מינה מחלקת צמידות של  $\overline{K}/K$  אז הוכחה: בכיוון הראשון, אם  $\overline{K}/K$  אם  $\overline{K}/K$  אז  $\overline{K}/K$  אז  $\overline{K}/K$  שכן  $\overline{K}/K$  שכן  $\overline{K}/K$  אם  $\overline{K}/K$  אז  $\overline{K}/K$  אז  $\overline{K}/K$  שכן  $\overline{K}/K$  שכן  $\overline{K}/K$  הוכחה: בכיוון הראשון, אם  $\overline{K}/K$  המסלול של  $\overline{K}/K$  שייך ל- $\overline{K}/K$  שייך ל- $\overline{K}/K$  המסלול של  $\overline{K}/K$  שייך ל- $\overline{K}/K$  המסלול של  $\overline{K}/K$ 

מעל מעל סגור אלגברית האר סגור סגור מעל  $\overline{K}$  סגור ש"ס (bootstrap) מיז  $\overline{K}$  קיים  $\overline{K}$  סיים אחר של  $\alpha'\in C_{\alpha}$  מהיות שבור כל  $\alpha'\in C_{\alpha}$  מהיחם שבי (bootstrap). קיים  $\overline{K}$  אוטומורפיזם ההרחבה  $\overline{K}/\sigma(\overline{K})$  מהיא אוטומורפיזם.

. הרחבה F/K כי ונניח מדרגה אחד) מדרגה פשוטה (נוצרת של-ידי אלגברית הרחבה אלגברית הרחבה אלגברית בוניח ונניח בוניח ונניח בוניח אלגברית פשוטה אלגברית פשוטה ונוצרת אחד) אונניח בוניח בוניח ונניח בוניח אחד.

ערכית חד־הד העתקה משרה משרה,  $f_{\alpha/K}$ של  $\phi(\alpha)$ לשורש את לוקח לוקח  $\phi:L\hookrightarrow F$ שיכון כל אזי כל אזי כל ליוקח את

$$\operatorname{Hom}_{K}(L, F) \simeq \{ \beta \in F \mid f_{\alpha}(\beta) = 0 \}$$

.(חסם על כמות ההרמות)  $|\mathrm{Hom}_K(L,F)| \leq d$  ובפרט מתקיים

מתקיים של של של שורש  $\beta\in F$  ולכל  $arphiig(f_{lpha/K}ig)=f_{lpha/K}$  שורש של הוא אכן אכן הוכחה:

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

נקבע ביחידות על-ידי  $\sum_{i=0}^{n-1}a_ilpha^i$  יש יצוג יחיד מעל אולכן לכל  $A\in L$  מעל מעל זה בסיס של הבסיס לוה ביחידות אול-ידי  $A\in L$  מעל זה בסיס של הבסיס לוה ביחידות על-ידי A כך שA מקרים A מקרים A מקרים A מעל A מעל מעל הביחים A מעל מעל הביחים של הביחים לוה מעל הביחים מעל

d עם דרגה אלגברי מעל אלגברי (דרגה אי־ספרבילית, דרגה אי־ספרבילית, אלגברי מעל 14.3 אלגברי מעל אווא הגדרה 14.3 אי־ספרבילית, אי־ספרבילית, דרגה אי־ספרבילית

הדרגה מיכאל של בסימוני ההרצאות של מולקות של מולקות העוצמה לפ $\deg_s(lpha)=\deg_{K,s}(lpha)$  שתסומן א מיכאל מיכאל מיכאל מולקות העמידות של מיכאל שתסומן ( $\deg_s(lpha)=\deg_{K,s}(lpha)=\log_{K,s}(lpha)$ 

פירוק פירוק: $f_{lpha}$ ב ב' של הריבוי האי- $\deg_i(lpha)=\deg_{K,i}(lpha)$  שתסומן K מעל של מעל הדרגה האי-ספרבילית של מעל

$$f_{\alpha} = (t - \alpha)^{d_1} \cdot \dots \cdot (t - \alpha)^{d_n}$$

 $\deg_i(lpha)=d_1=\cdots=d_n$  ואז

ואז  $\sigma(\alpha)=\alpha'$  כך כך  $\sigma\in {\rm Aut}\big(\overline{K}/K\big)$ קיים  $\alpha,\alpha'\in\mathcal{C}$ לכל הערה: לכל

$$(t-\alpha)^{d_{\alpha}}-(t-\alpha')^{d_{\alpha'}}\cdots=f_{\alpha}=\sigma(f_{\alpha})=(t-\alpha')^{d_{\alpha'}}\cdots$$

עבור g עבור עבור פולינום פולינום אורשים וולכן לכן ולכן וולכן לכן וולכן ל $d_{\alpha}=\deg_i(\alpha), d_{\alpha}=d_{\alpha'}$ עבור עבור

 $.lpha=a+b\sqrt{d},\overline{lpha}=a-b\sqrt{d}$  וניקח ( $\sqrt{d}
otin K$ ) הרחבה הרחבה  $L=Kig(\sqrt{d}ig):$  14.1 דוגמה

 $\sigma(\sqrt{d})=-\sqrt{d}, \sigma(lpha=\overline{lpha})$  אם lpha
eqlpha'ולכן lpha
eqlpha'ולכן נניח lpha
eqlpha'ולכן מניח lpha
eqlpha'ולכן מניח lpha
eqlpha'ולכן מכיח המקרה הטריוויאלי ולכן נניח אם lpha

ונקבל  $lpha=\overline{lpha},+=-$  ונקבל  $\deg_i(lpha)=2$  אז  $\operatorname{char}(K)=2$  אז ונקבל  $\operatorname{char}(K)\neq 2$  אז  $\operatorname{char}(K)\neq 2$  אז  $\operatorname{char}(K)\neq 0$  ונקבל  $\operatorname{char}(K)\neq 0$  ונקבל  $\operatorname{char}(K)\neq 0$  ווינקבל  $\operatorname{char}(K)\neq 0$  ווינקבל אוטומורפיזמים לא טריוויאלים.

,1 הוא פריד): פולינום של כל השורשים מעל (ספרבילי) הוא הוא קספרבילי) נקרא פריד (קריבוי של כל השורשים הוא  $\overline{K}$  (ריבוי של כל השורשים הוא  $f(t) \in K[t]$  נקרא  $f(t) \in K[t]$  נקרא אי־פריק!)

 $a=a^{rac{1}{p^n}}$  הזו  $p^n$  יום שורש שורש  $t^{p^n}-a$  יש שורש לכל פולינום (t-lpha) ובפרט  $(t-lpha)^{p^n}=t^{p^n}-lpha^{p^n}$  אז  $\mathrm{char}(K)=p, lpha\in\overline{K}$  יש שורש בריבוי יש יודע בריבוי

#### 29/04 - 9 הרצאה 15

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

רחבת שבות שבה fמתפצל, הרחבת הרחבת ו־L/Kו ממעלה פולינום פולינום לה שדה שדה שדה שדה לה שדה וידי הייו אור פולינום ממעלה אור שבה לה שדה שדה אור שבה לה שדה אור ב

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

. האדרה שורש פשוט): נאמר שירש פשוט (simple root) אורש פשוט (האמר שירש פשוט): נאמר שירש פשוט): נאמר מופיע בידיוק פעם אחת בפיצול.  $(t-\alpha)^2 \nmid f$  אבל אור, אבל אור, אבל פעם אחת בפיצול.

. בפיצול לכל הפחות מרובה של (multiple root) הגדרה מרובה הוא שורש מרובה (שורש מרובה מרובה) או הגדרה מרובה (שורש מרובה  $lpha=lpha_i\in L$  המר של הפחות פעמיים.  $(t-lpha)^2\mid f$  בלומר אם

שבו שבו מרובים מרובים אין לו שורשים (Separable נקרא פריד (ספרבילי): הפולינום (שורשים מרובים לו  $f \in K[t]$  נקרא פריד (ספרבילי): הפולינום לו שורשים מרובים בשדה ההרחבה לו שבו מחפצל

. שבו הוא מתפצל. שבו בשדה בשדה אינה פולינום של פולינות הספרביליות של הספרב: תכונת בשדה בשדה ההרחבה L

(f) אם הנגזרת של f' כאשר (כאשר f' הוא פריד הוא הנגזרת של הוא פריד הוא הנגזרת של פריד הוא פריד הוא הנגזרת של פריד הוא הנגזרת הוא הנגזרת של פריד הוא הנגזרת הוא

 $\gcd(f,f')=1$  כניה כי $\Longrightarrow:$ הוכחה:

 $.\overline{K}$ מההנחה נובע  $1=uf+vf'\in K[t]$  מההנחה נובע

. מתירה,  $t-a\mid 1=uf+vg$ ולכן ( $t-\alpha)\mid f'$ ולכן ולכן ו $t-\alpha)^2\mid f\in \overline{K}[t]$  כי נניח אי־פריד נובע כי וניח אי־פריד נובע ה

. נניח כי  $f \in K[t]$  הוא פריד.

מתקיים  $f' = ((t - a_i)q)' = q'(())$  נסמן

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

אבל

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

היא: ⇒ ברשומות של מיכאל, ההוכחה המפורטת בכיוון

. נניח כי  $f \in K[t]$  הוא פריד.

 $g\mid f'=$ ו היים  $g\in K[t]$  מחלק אי־פריק. אז  $g\in K[t]$  וניח בשלילה כי  $f'=(t-\alpha_i)g)'=g'(t-a_i)+g$  מתקיים בי  $f'=(t-\alpha_i)g)'=g'(t-a_i)+g$  מתקיים היים  $f'=(t-\alpha_i)g$ 

 $g \mid g'$ או ש־  $g \mid h$ או ש' קולכן או פובע מכך מכך ולכן או או פובע

. הירה וזו סתירה אי־פריד כי ולכן ולכן  $g^2\mid f$ , הראשון, במקרה במקרה ב

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 במקרה השני,  $g=\left(\sum_{j=0}^{\frac{d}{p}}c_{pj}^{\frac{1}{p}}t^j\right)^p$  אבל אז  $g=\left(\sum_{j=0}^{d}c_{pj}^{\frac{1}{p}}t^j\right)^p$  אבל אז  $g=\left(\sum_{j=0}^{d}c_{pj}^{\frac{1}{p}}t^j\right)^p$  הוא אי־פריד וזו סתירה.

 $\overline{K}[t]$ והן ב־K[t]והן הוא אותו  $\gcd(f,f')$ : 15.1 תרגיל

האינו למציאת שראינו של  $\overline{K}$  בf' שורש של בהא גם שורש של שורש של שורשים, ואם השורשים, ואת על-ידי השורשים, פכל בקבוע של פכל בקבוע שאיננו  $\overline{K}$  ב-ידי שהמקדמים יהיו בשדה, אבל גם  $\overline{K}$  מתבסס על חלוקת פולינומים ורק מצריכים שהמקדמים יהיו בשדה, אבל גם  $\overline{K}$ 

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

- $\deg_i(\alpha) = \deg(f) = \deg_K(\alpha)$ וא הם פרידים אז f אז  $\operatorname{char}(K) = 0$ . .1
- $f(t)=gig(t^{p^l}ig)$ כך ש־  $l\geq 0$ ו ר $g\in K[t]$  ופריד פולינום אי־פרים פולינום איchar(K)=p .2

יתרה מכך, אם  $\alpha_j=\beta_j^{\frac{1}{p^l}}$  הם מזה מהם אז ל־ $n=\deg(g)$  אז ל־ $n=\deg(g)$  כאשר מהם של הם וכל אחד מהם מכך, אם  $\alpha_j=\beta_j^{\frac{1}{p^l}}$  וכל אחד מהם הוא מריבוי (משמע וכל  $n=\deg(g)$  משמע וכל אחד מהם הוא מריבוי (משמע וכל אחד מהם הוא מריבוי וכל אחד מריבוי וכל אחד מהם הוא מריבוי וכל אחד מ

$$\deg_s(\alpha) = n, \deg_i(\alpha) = p^l, \deg(\alpha) = np^l$$
בפרט, מתקיים

. הכל טריוויאלי. עכן אחרת כי d>1 ונניח כי  $d=\deg(f)$  נסמן הכל הוכחה:

ולכן ל־  $0 < \deg(\gcd(f,f')) \le \deg(f') < \deg(f)$  אז  $0 < \deg(f,f') = 1$  אם זה קורה אם  $\gcd(f,f') = 1$  אי־פריד אם ורק אם  $\gcd(f,f') = 1$ f'=0 אם ורק אם  $\gcd(f,f') 
eq 1$  ולכן אי־פריד) מיירה (כי f אם סתירה לא טריוויאלי זו מיירה לא טריוויאלי זו אי־פריד) אי־פריד אי־פריד לא טריוויאלי ווא מיירה לא

. פריד.  $\deg(f') = \deg(f) - 1$  ולכן ולכן  $\gcd(K) = 0$  אז הבאן, אם מכאן, אם

f'=0אם או פריד וסיימנ או ה $\operatorname{char}(K)=p$  אם

 $a_{pj} \neq 0$  ולכן רק המקדמים  $i = 0 \in K$  בהכרח מתקיים i = 0 בהכרח אז אם i = 0 אז אם המקדמים לכל i = 0 אז לכל המקדמים אז לכל בהכרח מתקיים במילים אחרות מתקיים

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

. מובן סתירה  $f(t)=g(t^p)=g_1(t^p)g_2(t^p)$  ואז  $g(x)=g_1(x)g_2(x)$  אהרת אי־פריק: אהרת הוא  $g(x)=g_1(x)g_2(x)$  אבל  $g(x)=g_1(x)g_2(x)$  הוא אי־פריק: אהרת הוא אי־פריק: אחרת הוא אי־פריק: און אורת הוא אי־פריק: אורת הוא אי־פריק: און אורת הוא אי־פריק: און אורת הוא אי־פריק: אורת הוא אי־פריק: און אורת  $f = hig(t^{p^{m+1}}ig)$  ו־לכן פריד ולכן פריד ולכן לקבל  $\deg(g) < \deg(f)$  אז אי־פריק ובאינדוקציה על  $g = h(t^{p^m})$  נקבל f=tנסמן  $x=t^{p^l}$  ווש לו  $x=t^{p^l}$  שורשים שונים, ואם נבחר  $h(x)=\prod_{i=1}^n(x-eta_i)$  פריד ולכן  $h(x)=t^n$  פריד ולכן פריד ולכן אינים, ואם נבחר  $t^n$ וסיימנו.  $\prod_{i=1}^n \left(t-lpha_i
ight)^{p^l}=f$  היא (פרובניוס) ואז המכפלה  $lpha_i=eta_i^{rac{1}{p^l}}\in\overline{K}$  וויקח,  $\prod_{i=1}^n \left(t^{p^l}-eta_i
ight)$ 

#### 15.2 הרחבות נורמליות

פרק 5.6 ברשומות של מיכאל.

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

משפט באים הבאים אלגברית אלגברית עבור הרחבה באים באים משפט בור הרחבה משפט בL/K

נורמלית L/K .1

אותו) אותו את את לעצמו לא לוקחת אותן או<br/>  $\operatorname{Aut}\!\left(\overline{L}/L\right)$ אזי אוLאלגברי אלגברי סגור סגור א<br/>ו $\overline{L}/L$  אם .2

Lב מתפצל לחלוטין ב־ $f_{\alpha/K}$  , $\alpha \in L$  לכל .3

ולכן  $\sigma(L)\subseteq\overline{L}$  אחר שיכון שיכון  $\sigma\in\mathrm{Aut}ig(\overline{L}/Kig)$ , ואז כל מיחידות עד־כדי איזומורפיזם), אחר אלגברי של זה גם סגור אלגברי של  $\sigma(L)\subseteq\overline{L}$  אחר אלגברי של זה בעצם. בעצם, ואז כל מיחידות עד־כדי איזומורפיזם אוז כל מיחידות שיכון אחר אלגברי של מיחידות עד־כדי איזומורפיזם.

.Lב לחלוטין מתפצל מתפצל ש־ $f_{\alpha/K}$ ש בידיוק וזה בידיוק הוזה  $\sigma(\alpha)=\alpha'$  כך כך

. לא תלוי בשיכון לא  $\cup_{lpha \in L} C_{f_{lpha/K}}$ 

הערה:  $\phi:L oup \overline{L}$  שיכון קיים איט ולכן היא את הכיוון בשלילה: נניח שלו בשלילה: נניח שלו בשלילה: מיכאל הוכיח מיכאל הוכיח ברשומות שלו בשלילה: היא את הכיוון  $\phi:L oup \overline{L}$  $.\phi(L) \neq L$ 

אלגברית של סגור אלגברית של זו הרחבה  $\overline{L}/\sigma(\overline{L})$  שחייב להיות איזומורפיזם  $\sigma:\overline{L} \hookrightarrow \overline{L}$  שדות של שדות ל-Kשדות, ולכן הרחבה טריוויאלית.

 $\sigma \in \mathrm{Aut}_K(\overline{L})$  לכן  $\sigma \in \mathrm{Aut}_K(\overline{L})$  לא משמר את להנחה של

### 3 תרגיל 16

#### 16.1 טריקים

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

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

 $(a_n=1$  בהם בהקרים הנראה שזה ככל מניחה אניז אייזנשטיין אייזנשטיין לא לקיים אבל א־פריק אבל להיות יכול פולינום אייזנשטיין .4

#### 16.2 מסקנות

הוא  $\mathbb{Q}ig(\sqrt{p_1},...,\sqrt{p_n}ig)$  ובסיס ל־ $ig(\mathbb{Q}ig(\sqrt{p_1},...,\sqrt{p_n}ig):\mathbb{Q}ig]=2^n$  הוא מזה מזה מונים שונים  $p_1,...,p_n$  ובסיס. 1

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

#### 05/05 - 10 הרצאה 17

#### 17.1 הרחבות נורמליות – המשך

.  $\mathcal{C}_lpha$  מסקנה  $\mathrm{Aut}(L/K)$ ו ר $\mathcal{C}_lpha\subset L$ ו התפצל לחלוטין מתפצל לחלוטיבית על בורמלית, אזי וורמלית, אזי בורמלית, אזי וורמלית, אזי בורמלית, אזי וורמלית, אזי בורמלית, בורמלית

פועלת Aut(L/K) פועלת אוז  $\sigma(\alpha')=\alpha$  כך שמתקיים  $\sigma\in {\rm Aut}(\overline{L}/K)$  פיים שראינו: קיים אוז פועלת פועלת סרנזטיבית על פועלת  $\sigma(\alpha')=\alpha$  סרנזטיבית על  $\sigma(\alpha')=\alpha$  פועלת סרנזטיבית שראינו: פועלת סרנזטיבית של טרנזטיבית שלי

. הזהות קיז היא האוטומורפיזמים חבורת תבורת,  $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$  אבור בוגמה דוגמה יעבור יעבור

**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.

- $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$  ו-L/F ו לא הרחבה נוען כי עטען ניטען נורמליות, נוער הרחבות וורמליות. 1
- . בהכרח אבל תת־הרחבה לא נורמלית האז  $\overline{K}/K$  נורמלית בהכרח שלא בהכרח לא נורמלית נטען נורמלית נניח L/K
- L/T בי מתפצל לחלוטין כי הוא מתפצל לחלוטין בי ולכן הוא מתפצל לחלוטין בי בי גניח כי בי הוא מתפצל לחלוטין כי בי בי כי בי בי גניח כי L/F נורמלית ונטען כי L/F כי כל L/F מתפצל לחלוטין ב-3.

. (אנלוגי היא מאינדקס 2 היא מאינדקס וורמלית (אנלוגי לחבורה L/K בורמלית גורר כי L/K הרחבה ריבועית הרחבה וורמלית היא נורמלית

הוכחה: להשלים

#### 17.2 שדות פיצול

פרק מספר 5.6 ברשומות של מיכאל.

.0-ם שונה פיצול): נניח K שדה ו-L/K הרחבה ברול (שדה פיצול): נניח א שדה ו-L/K שדה הגדרה 17.1 (שדה פיצול)

 $L=\{f\in P \$ מתפצל שלה ביצול שלה כל ב-L=K(S)ו ב־ב לחלוטין מתפצל מתפצל אם כל פל אם אם ביצול אדה נקרא נקרא נקרא ב-ל

בפרט, L/K אלגברית שכן היא אלגברית אלגברית בפרט,

למה 17.1: אם K שבדרך־כלל אינו שונה מ־0 אזי שדה פיצול של  $P\subseteq K[t]$  אינו שדה פולינומים שונה מ־t אינו שבדרך־כלל אינו יחיד)

. שדה פיצול. שדה  $K(S)=L\subseteq \overline{K}$  ואז  $\{f\in P\$ שה של השורשים כל השורשים ארור. ביקח ויקח של הוכחה: ניקח ארור.

כאשר  $K(\phi(S))=L'$  קיים הומומורפיזם ( $f\in P$  ספצל ב"ר ב"ר על־ידי הרמה לוצר מלמת ההרמה  $\phi:L\hookrightarrow L'$  מלמת הומומורפיזם לובסוף אם L' אם L' אם L' באשר L' הב השורשים ולכן L'

הערה: סגור אלגברי הוא שדה פיצול של כל הפולינומים.

#### : 17.1 משפט

- 0 שאינם  $P\subseteq K[t]$  של שדה פיצול אם ורק אם ורק אם נורמלית היינה בורמלית היינה בורמלית אם ורק אם L/K
- (ואולי אף פריק) פולינום אלגברית של פריקו של הוא אדה אות וחופית וסופית היינה נורמלית היינה אלגברית אלגברית וחופית אם ורק אם ורק אם בודד וחופית אף פריקו ואולי אף פריקו ההרחבה לבוד וואולי אף פריקו וואולי וואולים וואולים וואולי וואולי וואולי וואולים וואול
- . נורמלית אזי L הוא שדה פיצול של  $\{f_{lpha/K}\mid lpha\in L\}$  כי כל  $\{f_{lpha/K}\mid lpha\in L\}$  הוא שדה פיצול אזי L/K הוא מתקיים S=S כאשר S=S בניח שדה פיצול של S=S באשר S=S באשר שורשי S=S באשר S=S באשר של לנורמליות נקבל של S=S מתקיים S=S מתקיים S=S ולכן S=S מתקיים S=S מתקיים S=S ולכן של S=S מתקיים S=S ולכן לפי התנאים השקולים לנורמליות נקבל של S=S מתקיים S=S ולכן לפי התנאים השקולים לנורמליות נקבל של S=S מתקיים כל לוכן לפי התנאים השקולים לנורמליות נקבל של מורמליות בארט מורמליות בארט
- . וניקח לחלוטין.  $f=\prod_{i=1}^n f_{\alpha_i/K}$  וניקח וניקח יוצרים f מתפצל שורשים מf אז כל הז כל  $f=\prod_{i=1}^n f_{\alpha_i/K}$  וניקח וניקח יוצרים וניקח יוצרים באר באר וניקח וניקח אלגברית וגם נוצרת באם f אם ביצול של  $f\in K[t]$  אלגברית וגם נוצרת ביצול של  $f\in K[t]$  אלגברית וגם נוצרת הפיצול וולכן סופית ולכן סופית ולכן הארב באר ביצול של הארב באר ביצול של הארב ביצול ביצול ביצול של הארב ביצול של הארב ביצול ב

עד־כדי עד־כדי P)  $P=\left\{f_{lpha/K}\mid lpha\in L
ight\}$  שדה פיצול של  $L^{nor}$ , (K- מון (תלוי גם ב-L), הרחבה אלגברית, ניקח (תלוי גם ב-L), שיזומורפיזם).

.K מעל של של הסגור הנורמלי הסגור  $L^{nor}$ 

L את המכילה המכלה) מינימלית נורמלית וו הרחבה את  $L^{nor}/K$  : 17.2 למה

. שדה פיצול (P שדה פיצול בורמלית ולכן נורמלית  $L^{nor}/K$ 

 $L\subseteq L^{nor}$  נמובן,  $L\subset P$  זה שורשי מזה באשר באשר באסר כמובן, כמובן

 $F=L^{nor}$  ולכן ב־F מתפצל לחלוטין מינבע כי כל בי נורמלית, נובע כי כאשר לארוטין ב-F/K כאשר לבסוף, אם לבסוף, אם

$$\mathbb{Q}ig(\sqrt[3]{2},\omegaig)=L^{nor}/L=\mathbb{Q}ig(\sqrt[3]{2}ig)/K=\mathbb{Q}$$
: 17.3 דוגמה

השלים ציור

? להשלים ציור  $L^{nor}=\mathbb{Q}ig(\sqrt[4]{2},iig)$  ואז  $L=\mathbb{Q}ig(\sqrt[4]{2}ig)$  : 17.4 דוגמה

אזי  $C_f = \{f \text{ wirth } d \in K[t] \text{ .coal} \}$  נסמן  $f \in K[t]$  שדה פיצול של פולינום מדרגה פולינום מדרגה פולינום מדרגה  $f \in K[t]$  שדה פיצול של ו־: 17.3 של  $C_f = \{f \text{ wirth } d \in K[t] \text{ or } t \in K[t] \text{ or }$ 

 $\operatorname{Aut}_K(L) o \operatorname{Perm}ig(C_fig) = \operatorname{Aut}ig(C_fig) = S_n$ בל הצמצום הצמצום על הוממורה על  $\sigma \in \operatorname{Aut}_K(L) = \operatorname{Aut}(L/K)$  .2 .2 .2 ... שיכון.

- הורחה

ולכן  $L/K_{n-1}/\cdots/K$  הרחבות מגדל מגדל ונקבל ה $K_i=K(\alpha_1,\cdots,\alpha_i), K=K_0$  .1 נגדיר גדיר 1.

$$[L:K] = \prod_{i=0}^{n-1} [K_{+1}:K_i]$$

אבל כל  $lpha_{i+1}$  היא שורש אל כל אבל

$$f_i(t) = \frac{f(t)}{(t-\alpha_1)\cdot\dots\cdot(t-\alpha_i)} \in K_i[t]$$

ולכן

$$[K_i:K_{i-1}]=\deg_{K_i}\bigl(\alpha_{i+1}\bigr)\leq \deg(f_i)=d-i$$

ולכן

$$[L:K] \le d(d-1)\cdots(d-n+1) \le d!$$

 $\sigma\mapsto\sigma|_{C_f}$  על־ידי  $\operatorname{Aut}_K(L) o\operatorname{Perm}ig(C_fig)=S_n$  במצום צמצום ולכן יש הומומורפיזם ( $\sigma(f)=f$  כל  $\sigma$  לוקח את לעצמה (כל  $\sigma(f)=f$  ולכן יש הומומורפיזם את הצורה  $f,g\in K[t_1,\cdots,t_n]$  כאשר ביחידות על־ידי הצמצום: זה כי כל  $\sigma$  הוא מהצורה ביחידות על־ידי הצמצום: זה כי כל  $\sigma$  הוא מהצורה ביחידות על־ידי הצמצום: זה כי כל  $\sigma$ 

$$\sigma(x) = \frac{\sigma(f(\alpha_1, \cdots, \alpha_n))}{\sigma(g(\alpha_1, \cdots, \alpha_n))} = \frac{f(\sigma(\alpha_1), \cdots, \sigma(\alpha_n))}{g(\sigma(\alpha_1), \cdots, \sigma(\alpha_n))}$$

 $\sigma(\alpha_1), \cdots, \sigma(\alpha_n)$  ולכן הוא נקבע על־ידי

17.3 שורשי יחידה

פרק 6.1 ברשומות של מיכאל.

 $\xi^n=1$  שמקיים  $\xi\in\overline{K}$  הוא בתוך בתוך מסדר  $\overline{K}$  שמקיים ויהי  $n\in\mathbb{N}$  היהי מסדר מסדר שורש יחידה מסדר (שורש יחידה מסדר  $\overline{K}$ 

נגדיר בורת שורש היחידה מסדר שורש שורש ויחידה מסדר,  $\mu_n$ חבורת חבורת הגדרה נגדיר מסדר שורש חבורת וויחידה אנדרה ויחידה מסדר וויחידה אנדרה וויחידה מסדר וויחידה אנדרה וויחידה וויחידה אנדרה וויחידה וויחידה וויחידה וויחידה אנדרה וויחידה וויחי

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

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

. נשים אבלית חבורה חבורה מסדר מסדר אמחלק את מסדר מסדר של אבלית הת-חבורה אבלית היא  $\mu_n(K)$ יש לב לב שי

ונגיד (K שם הרחבה תחת התחתה של של (שכן שכן ב־K נסמן ב־K מתפצל לחלוטין ב־ $x^n-1$  אם  $1\leq n\in\mathbb{N}$ , אם רחבה של M ונגיד במקרה זה ש $\mu_n$  מתפצל ב-K

#### : 17.5 דוגמה

$$\begin{split} \mu_{\infty}(\mathbb{R}) &= \mu_{\infty}(\mathbb{Q}) = \{\pm 1\} = \mu_2 \\ \mu_{\infty} &= \mu_{\infty}(\mathbb{C}) = \left\{ e^{\frac{2\pi i m}{n}} \mid 1 \leq m \leq n, (m,n) = 1 \right\} \end{split}$$

תרגיל 17.2: (בהרצאה מיכאל נתן את זה כדוגמה ופירט קצת, ברשומות שלו זה מופיע כתרגיל אז נוכיח במסודר)

- $\mu_\inftyig(\mathbb{Q}ig(\sqrt{-3}ig)ig)=\mu_6$  נראה שמתקיים .1 d=-1 אם  $\mu_\inftyig(\mathbb{Q}ig(\sqrt{-3}ig)ig)=\mu_4$  מם .2
- $d \notin \{-1, -3\}$  לכל לכל  $\mu_{\infty}ig(\mathbb{Q}ig(\sqrt{d}ig)ig) = \mu_2$  מתקיים .3
- $\mathbb{Q}/\mathbb{Z} \hookrightarrow \mu_{\infty}(\mathbb{C})$  בראה איזומורפיזם  $x \mapsto e^{((2\pi i x)^{-}}$ . 4

:הוכחה

1. נשים לב שמתקיים

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

.  $\mathbb{Q}\left(\sqrt{-3}\right)$ ב ב־מצאים ב- $\mu_6$  שכן שלא כל השורשים משמע כל שכן שכן שכן  $\mathbb{Q}(\omega)=\mathbb{Q}\left(\sqrt{-3}\right)$  נשים לב שמתקיים שלאינו ב- $\mathbb{Q}(\omega)$ 

 $\mu_4\subseteq\mu_\infty(\mathbb{Q}(i))$  ולכן  $\mu_4\subset\mathbb{Q}(i)$  ולכן  $\mu_4=\{1,-1,i,-i\}$  ובגלל ש $\mu_4=\{1,-1,i,-i\}$  ובגלל ש $\mu_4=\{1,-1,i,-i\}$  ובגלל ש $\mu_4=\{1,-1,i,-i\}$  ובגלל ש .2-עבור ההכלה בכיוון השני, ניזכר ש $\mathbb{Q}[\mathbb{Q}(i):\mathbb{Q}]=2$ ולכן נבחן את כל הפולינומים הציקלוטומיים שדרגתם קטנה או שווה ל  $n \in \{1, 2, 3, 4, 5, 6\}$  שנסתכל מספיק שנסתכל מדרגה הביקלוטומיים הם מדרגה ביקלוטומיים הביקלוטומיים הביקלוטומים ה

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.  $\Phi_6(x) = x^2 - x + 1 \Rightarrow \deg(\Phi_6(x)) = 2$ 

1.  $\Phi_1(x) = x - 1 \Rightarrow \deg(\Phi_1(x)) = 1$ 

 $n \in \{1, 2, 3, 4, 6\}$  המועמדים היחידים שלנו המועמדים ולכן

 $\mathbb{Q}(i)$ ־בן כן האחרים לא אפשריים, אבל ה $\frac{\pm 1 \pm \sqrt{-3}}{2} 
otin מתקיים לה מתקיים על הקרה לא אפשריים, כי כפי שראינו בתרגול במקרה או מתקיים לבר של <math>\Phi_3(x), \Phi_6(x)$  אבל ה־4 אנחנו יודעים כבר כי בידיוק  $\{\pm 1, \pm i\}$  ולכן נקבל גם את ההכלה השנייה.

 $\mu_\infty(\mathbb{Q}(i))=\mu_4$  בסה"כ מצאנו כי

ש ל $d \notin \{-1, -3\}$ ש ההנחה שהפעיף לבדיקה להגיד שלא ייתכן להגיד שלא אנחנו כבר אנחנו כבר יודעים אנחנו כבר יודעים להגיד שלא

$$\mu_{\infty} \! \left( \mathbb{Q} \! \left( \sqrt{d} \right) \right) = \mu_6 \vee \mu_{\infty} \! \left( \mathbb{Q} \! \left( \sqrt{d} \right) \right) = \mu_3 \vee \mu_{\infty} \! \left( \mathbb{Q} \! \left( \sqrt{d} \right) \right) = \mu_4$$

 $\mu_\infty\big(\mathbb{Q}\big(\sqrt{d}\big)\big)=\mu_1$  או  $\mu_\infty\big(\mathbb{Q}\big(\sqrt{d}\big)\big)=\mu_2$  אם הקל עם גישאר רק עם העל ,  $\big[\mathbb{Q}\big(\sqrt{d}\big):\mathbb{Q}\big]\leq 2$  ובגלל ש־2 בבירור אי ייתכן ש $\mu_\infty\big(\mathbb{Q}\big(\sqrt{d}\big)\big)=\mu_2$  שכן  $\mu_\infty\big(\mathbb{Q}\big(\sqrt{d}\big)\big)=\mu_2$  ולכן בסך־הכל נקבל  $\mu_\infty$ 

 $\widehat{\varphi}(x+\mathbb{Z})=e^{2\pi ix}$  על־ידי  $arphi:\mathbb{Q}/\mathbb{Z} o\mu_\infty(\mathbb{C})$  גגדיר. 4.

אז  $x \equiv u \operatorname{mod} \mathbb{Z}$  אז מוגדר היטב. כי אם

$$x-y\in\mathbb{Z}\Rightarrow e^{2\pi ix}=e^{2\pi iy}\cdot e^{2\pi i(x-y)}=e^{2\pi iy}\cdot 1=e^{2\pi iy}$$

זה גם אכן הומומורפיזם

$$\varphi((x+\mathbb{Z})+(y+\mathbb{Z}))=\varphi((x+y)+\mathbb{Z})=e^{2\pi i(x+y)}=e^{2\pi ix}\cdot e^{2\pi iy}=\varphi(x+\mathbb{Z})\cdot \varphi(y+\mathbb{Z})$$

הוא גם חד־חד ערכי כי הגרעין הוא טריוויאלי, שכן מתקיים

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

כך שמתקיים כל מספיק מספיק מספיק לל, ולכן כל אבור הוא מהצורה, ולכן הוא מהצורה אולכן הוא אול אורש אורש הוא הוא  $\xi\in\mu_\infty(\mathbb{C})$  אוא אכן על, כי כל על, כי כל ל  $.\varphi(\frac{k}{\pi} + \mathbb{Z}) = \xi$ 

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

אם הסדר של (torison) נקרא איבר  $g \in G$  נקרא איבר הבורה. איבר G סופי. (איבר פיתול): איבר פיתול מיבר g

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.

#### : 17.6

- 1. כל חבורה סופית היא חבורת פיתול
  - פיתול חבורות חבורות פיתול  $\mathbb{O},\mathbb{Z}$  .2

A של של איברי איברי קבוצת אבלית, חבורת A חבור A צבור ועבור A

$$A_{tor} = \{ a \in A \mid \exists m \in \mathbb{N}_{>1} \ s.t. \ ma = 0 \}$$

. היא חסרת המנה  $A/A_{tor}$  היא הסרת־פיתול.

**הערה**: לא רק שחבורת שורשי היחידה היא חבורה אבלית תחת הכפל, זו תת־חבורת פיתול של חבורת ספירת היחידה

$$\mathbb{S}^1 = \mathbb{T} = \{ z \in \mathbb{C} \mid |z| = 1 \}$$

p הוא שסדרם שסדרם של כל האיבורה של כתת־החבורה נגדיר H[p] נגדיר אבלית שסדרם שסדרם ובור (H[p]) איבורה הגדרה הגדרה ביות

$$H[p] = \{ h \in H \mid h^p = 1 \}$$

.H[p]ב־ברים איברים שי  $p\mid |H|$ לכל אם ורק אם איברים איקלית אז Hאז

. בעצם, H[p] היא תת־חבורת פיתול

. איקלית עם עם היא ובפרט כל פרט ובפרט היא עם עם איק ובעצם איק איברים. אזי איברים עם עם איברים שדה ו $G \leqslant K^{\times}$ יהי ודי ודי איקלית. איברים איברים עם איברים איברים ובפרט איברים ובפרט איברים איברים ובפרט ובפרט איברים ובפרט איברי

 $\alpha \in G[p]$  עכי יש (כי שורשים, ולכן שורשים, שורשים אולכן של  $G[p] \subset \{x^p-1 \in K \$ שורשים של שורשים אזי  $p \mid n$  אוזי שהסדר שלו לא מחלק את המעלה, ולכן הוא מסדר גדול יותר, משמע יוצר של G[p].

x=1, אחד, שורש שורש אחד,  $x^{p^n}-1=(x-1)^{p^n}$  כי לפולינום לפולינום התקיים לפולינום, ס<br/> pיש הערה ממציין הערה מתקיים לפולינום לפולינום הערה:

 $m \in K^{ imes}$  ויהי הגדול ביותר של הגדול ביותר של מתפצל לחלוטין בי $m \in K^{ imes}$  ויהי הגדול ביותר של מתפצל ביותר של  $m \in K^{ imes}$  ויהי הגדול ביותר של  $m \in K^{ imes}$  מתפצל הארות:

- n=m נבחר  $\operatorname{char}(K)=0$  .1
- $\gcd(m,p)=1$  כאשר המר בהחר בהחר  $\operatorname{char}(K)=p$  אם .2

 $\mu_n \hookrightarrow \mathbb{Z}/m\mathbb{Z}$  אז מתקיים

הוא לא שורש.  $x^m-1$  והשורשים הם רק 0 ול $x^m-1$  והשורשים הם  $(m\in K^\times)$  טיש שורשים שורשים הוא אנחנו ודעים ש $(m\in K^\times)$  שורשים הוא איברים. לכן נובע כי  $(m\in K^\times)$  פריד עם שורשים, ולכן ל(f,f')=1 איברים.

שכן , $\mu_n=\mu_m\oplus\mu_p^l=\mu_m$  נבחר  $\operatorname{char}(K)=p$  אם סיימנו ואם  $\operatorname{char}(K)=0$ 

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

34

#### 06/05 - 11 הרצאה 18

#### 18.1 שורשי יחידה – המשך

מתקיים מסדר n < n שורש יחידה שלכל מסדר מסדר מחידה פרימיטיבי מסדר מורש יחידה פרימיטיבי מסדר (שורש יחידה פרימיטיבי מסדר n < n: יהי n < n: יהי שורש יחידה פרימיטיבי מסדר n < n: יהי שלכל n < n: יהי שלכל

.  $\mathbb{Q}$  שדה הרחבה מעל  $L=\mathbb{Q}(\xi)$  ואז p ואז פרימיטיבי מסדר אורש שורש המספר ב $\xi=e^{\frac{2\pi i}{p}}\in\mathbb{C}$  המספר באשוני, המספר ב $\xi=e^{\frac{2\pi i}{p}}\in\mathbb{C}$  הוא שדה הרחבה מעל  $\xi=0$  הוא שדה המינימלי של  $\xi$  מעל  $\xi$  מעל  $\xi$  הוא

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

מסקנה אם הפיך הוא הפיך ב־K אם מסדר מסדר מסדר שורש פרימיטיבי שורש פרימיטיבי אז הפיך ב־N אם אם הוא אם אם אם אם מסקנה אות אם אם אז שורש פרימיטיבי של אז שורש פרימיטיבי של אז אחרש פרימיטיבי שורש מסקנה אז אחרש מסקנה אז אחרש פרימיטיבי שורש פרימיטיבי שורש פרימיטיבי שורש מסקנה אז שורש פרימיטיבי שורש שורש שורש שורש שורש שורש שורש פרימיטיב

תרגיל שמתקיימים פניח סגור אלגברית כניח נניח נניח :18.1 תרגיל וניח כי

- $\mu_\infty(K) \backsimeq \mathbb{Q}/\mathbb{Z}$  אז  $\mathrm{char}(K) = 0$  .1
- $\mu_\infty(K) \cong \mathbb{Q}/\mathbb{Z}\left[rac{1}{p}
  ight]$  אז  $\mathrm{char}(K) = p > 0$  אם .2

:הוכחה

- ענות שנת היחיבות פיתול עם "עותק" לכל  $\mathbb{Q}/\mathbb{Z}$  הוא מסדר סופי ולכן  $\mathbb{Q}/\mathbb{Z}$  היא חבורת פיתול עם "עותק" לכל  $\kappa$  סגור אלגברית ולכן מכיל את כל שורשי היחידה  $\kappa$  לכל  $\kappa$  בידיוק  $\kappa$  הוא העותה שה הגדרנו בתרגיל הקודם, ונחדד אותו להיות  $\kappa$  בידיוק ( $\kappa$  בידיוק ( $\kappa$  באמת איזומורפיזם שה איזומורפיזם כמו שראינו.  $\kappa$  באמת איזומורפיזם כמו שראינו.
  - ולכן  $\operatorname{char}(K)=p$  כי  $(x^{p^n}-1)'=0$  אבל  $x^{p^n}-1$  שורש של  $\xi^{p^n}=1$  ולכן  $\xi^{p^n}=1$  משמע  $\xi^{p^n}=1$  כי  $\xi^{p^n}=1$  ולכן  $\operatorname{gcd}(x^{p^n}-1,(x^{p^n}-1)')=1$  פי  $\operatorname{gcd}(x^{p^n}-1,(x^{p^n}-1)')=1$

ולכן  $p^{-}$ , ולכן מסדר זר להיות להיות מסדר מנגד, ולכן מנגד, ולכן מנגד, ווידה במציין אויבים מנגד, ו

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

אבל זה בידיוק אומר ש־ $\xi_n \notin K$  אז  $p \mid n$  או  $x = \frac{a}{n} + \mathbb{Z}$  הוא מהצורה  $x \in \mathbb{Q}/\mathbb{Z}$ , שכן כל  $\mu_{\infty(K)} \hookrightarrow \mathbb{Q}/\mathbb{Z}\left[\frac{1}{p}\right]$  אומר שי $\chi_n \notin K$  אומר היים אומר עם  $\chi_n \notin K$  אומר היים אומר שעבורם פול משמע שעבורם אומר שעבורם אומר שעבורם פול משמע

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

הערק: מיכאל אמר של K ו־K ובחירה של אמר שבעיים" - הם "לא טבעיים, כי הם לא יחידים ולא הם לא יחידים הללו הם לא יחידים ולא קנונים, כי הם "לא טבעיים" - הם תלויים בבחירה של 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.

 $\mbox{.char}(K)=p>0$ עם אדה ש־<br/> Kשדה (ננים פרובניום אנדומורפיזם 18.1 למה למה למה

. נגדיר אנדומורפיזם אנדומורפיזם (Fr : K o K הומומורפיזם (הומורפיזם אנדומורפיזם וזהו אנדומורפיזם (הומומורפיזם היום אנדיר

. הוא אוטומורפיזם. ראשוני, זה  $\operatorname{Fr}$  הוא אוטומורפיזם. ראשוני, זה  $\operatorname{char}(K)=p$ 

 $K^{p^n}$ את התמונה של  $\mathrm{Fr}^n$  נסמן ב

:הוכחה

$$Fr(ab) = (ab)^p = a^p b^p = Fr(a) Fr(b)$$
.1

2. מנוסחת הבינום של ניוטון

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

 $\Box$ 

 ${
m Fr}(a)=a^p=0\Longleftrightarrow a=0$  ערכי שכן ערכי הד גם מחלקי מחלקי מחלקי שלמות שלמות בתחום בגלל אנחנו בגלל בגלל אפס, או

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

. (שאינו שאינו עד־כדי איזומורפיזם עם איברים שדה  $q=p^n$ עם עבור עבור עב־כדי עברים עם עבור  $q=p^n$  ויחיד). איברים עברט פרט, לכל ראשוני עד־כדי איזומורפי ל $\mathbb{F}_q$  כאשר q חזקה של ראשוני.

 $\mathbb{F}_q\setminus\{0\}=\mu_q$  ונגדיר הרחבה שלו שכן שכן  $t^{q-1}-1$  של של כשדה פיצול הרחבה וניקח ונגדיר הרחבה אכן שכן  $\mathbb{F}_p$  הוכחה:

 $.\mathrm{Fr}^{q(x)}=x$ בעצם חזה מיך ש־ט כך ה־xה כל היא מיק איברים איברים איברים איברים איברים מיך איברים נראה איברים איברים איברים איברים מיך מיש איברים מיך איברים איברים איברים איברים מיד מיד איברים איברים

נטען שכל האיברים שלקחנו הוא אופן נקבל בא  ${
m Fr}^q(x+y)=x+y$  ולכן  ${
m Fr}^q(y)=y$  וגם פל. אופן נקבל בא מהווים שדה: דין שלקחנו הוא אופן נקבל אופן באיברים  $\{x\mid x^q=x\}=\mathbb{F}_q\subset K$  לכן נקבל

.(gcd(f,f')=1 אם ורק אם פריד פריד (פולינום שלנו פריד ( $(x^q-x)'=1$  אם שכן הפתרונות הערה: כל הפתרונות שונים שכן

ולכן  $|F|=p^n$  ולכן את שדה סופי אזי המעל  $Fpprox \mathbb{F}_p$  כאשר הרצאה (ראינו בהרצאה) כhar F=p כאשר  $F_p$  מכיל את שדה סופי אזי  $Fpprox \mathbb{F}_p$  מכיל את האינו בהרצאה (ראינו בהרצאה) ראינו  $F=p^n$  מכיל את  $F=p^n$  ולכן  $F=p^n$  ולכן האינו  $F=p^n$  ולכן  $F=p^n$  ולכן האינו  $F=p^n$  ולכ

#### : 18.2 תרגיל

- $\mathbb{F}_9 = \mathbb{F}_3(i)$  .1
- .( $lpha\mapsto lpha+1$  באשר האוטומורפיזם (מה עוב  $lpha^2+lpha+1=0$  כאשר  $\mathbb{F}_4=\mathbb{F}_2(lpha)$  .2

:הוכחה

- .( $[\mathbb{F}_9:\mathbb{F}_3]=2$ ) ע מדרגה  $\mathbb{F}_3$  של (עד־כדי איזומורפיזם) אות ההרחבת הוא ההרחבת הוא ההרחבת בוב מדרגה  $\mathbb{F}_3$  מדרגה  $\mathbb{F}_3$  מדרגה במון את הפולינום  $a\in\mathbb{F}_3$  נשום לב שהוא לא מתאפס לאף  $a\in\mathbb{F}_3$  והוא אי־פריק מעל  $a+bi\in\mathbb{F}_3$  הוא מהצורים מקומבינטוריקה.  $\mathbb{F}_3$  ויש לנו 1 צירופים אפשריים מקומבינטוריקה.  $\mathbb{F}_3=\mathbb{F}_3$  ווא ליני לבקבל כי  $\mathbb{F}_3=\mathbb{F}_3$  אונים בי 1 מהמשפט לעיל נקבל כי 1
- $\alpha$  הובחו (ולכן הוא הם הידע וולכן) הידע לו פיתרונות פריק מעל אי־פריק שהוא אי־פריק וולכן הוא בר $x^2+x+1$  וולכן הוא .2 .כחר את הפולינום . $\alpha^2+\alpha+1=0$ המקיימת המקיימת

עכשיו,  $\alpha$ יו ונטען של 1 וי $\alpha$  ונטען דיים איברים לינאריים לינאריים לינאריים איברים מכיל 4 איברים לב שהוא מכיל 1 ווי $\alpha$  ונטען דיים איברים  $\mathbb{F}_2[\alpha]=\mathbb{F}_2[x]/(x^2+x+1)$  מהווים חבורה כפלית מסדר 3:

ולכן  $\alpha^2=\alpha+1$  אבחרנו שבחרנו על  $\alpha$ 

$$\alpha^3 = \alpha^2 + \alpha = (\alpha + 1) + \alpha = 2\alpha + 1 = 1 \pmod{2}$$

אז זה סגור לחיבור, כפל ויחידה וקיבלנו שזה אכן שדה.

 $\mathbb{F}_2[x]/(x^2+x+1)=\mathbb{F}_4$  מצאנו שדה לעיל ומהטענה איברים איברים איברים מצאנו

מסקנה 18.2 אם עד־כדי איזומורפיזם ובנוסף הרחבה אחת בידיוק אחת מדרגה  $K/\mathbb{F}_q$  מדרגה אחת בידיוק הרחבה או לכל  $n\geq 1$  שבידיוק אחת מסקנה 18.2 אם  $\mathbb{F}_q$  שבי מיטיבית (קיים  $\alpha$  כך בעשר  $\alpha$  כך כאשר  $\alpha$  פרימיטיבית (קיים מכך בעשר מכן בישר מכן בידיוק מדיים מחשבים אחת מסקנה בידיוק הרחבה אחת מסקנה מסקנ

 $\mathbb{F}_{q^n}^ imes$  שהוא יוצר של על־ידי מהמשפט לעיל ההרחבה ההרחבה ההרחבה ההרחבה ווצרת על־ידי שהוא יוצר של הוכחה: מהמשפט לעיל קיימת ויחידה ההרחבה ההרחבה ה

 $\degig(f_{lpha/\mathbb{F}_q}ig)=n$ הוא פריד ו־f'=-1 ולכן הוא פריד פריד הוא אבל אבל הוא  $f_{lpha/\mathbb{F}_q} \mid t^{q^n}-t=f$  מתקיים גם

: שקולים: הבאים שקולים:  $\mathbb{F}_q, \mathbb{F}_r$  נניח נניח: 18.3 מסקנה

- $\mathbb{F}_{q}\hookrightarrow\mathbb{F}_{r}$  קיים שיכון .1
- $d \in \mathbb{N}$  עבור  $r = q^d$  .2
- $m\mid n$  עבור  $q=p^m$ ו־  $r=p^n$  .3

. ברור.  $2 \Longleftrightarrow 3$  ברור.

 $r=q^d$  ולכן  $d=\left[\mathbb{F}_r:\mathbb{F}_q
ight]$  אם כמרחב וקטור כאשר  $\mathbb{F}_r\hookrightarrow\left(\mathbb{F}_q
ight)^d$  ולכן  $\phi:\mathbb{F}_q\hookrightarrow\mathbb{F}_r$  אם  $1\Longrightarrow 2$ 

ואז  $x^{q-1}-1\mid x^{r-1}-1$  ולכן  $q-1\mid r-1=q^d-1$  אבל  $\mathbb{F}_p$  אבל הרחבות הן הרחבות ההרחבות שתי ההרחבות  $x^{q-1}-1\mid x^{r-1}-1$  ולכן  $q-1\mid r-1=q^d-1$  ואבל בניח כי  $q-1\mid x^{q-1}-1\mid x^{r-1}-1$  מכיל את שדה הפיצול  $q-1\mid x^{q-1}-1\mid x^{q$ 

07/05 – 5 תרגול 19

19.1 משהו

להשלים

4 תרגיל 20

20.1 טריקים

להשלים

20.2 מסקנות

להשלים

## 12/05 - 12 הרצאה 21

## 21.1 הרחבות ציקלוטומיות

פרק 6.3 ברשומות של מיכאל.

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

הגדרה (נוצר על־ידי t שורש שיחידה). בקראת הרחבה ביקלוטומית): הרחבה L/K בקראת הרחבה ביקלוטומית אבו L/K

 $\xi^n=1$ , שכן, n מסדר מסדר מיטיביים פרימיטיביים שרשי הסדר מעל K הם מעל K המלדים של פרימיטיביים מסדר M שכן, אז כל הצמודים של M מעל M הסדר של M שורש פרימיטיביים מסדר M שורש פרימיטיביים מסדר M שכן, אז כל הצמודים של M הוגם M בינו מסדר M שכן, אז כל הצמודים של M הוגם M בינו מסדר M שכן, אז כל הצמודים של M המלדים מסדר M שכן, אז כל הצמודים מסדר M מעל M הסדר של M המלדים מסדר M שכן, אז כל הצמודים מסדר M מעל M המלדים מסדר M מעל M מעל M מעל M המלדים מסדר M מעל M מעל

יש אלידי על־ידי על־ידי  $\sigma\in\mathrm{Aut}_K(L)$  ממסקנה שראינו (3.2.11, ארטום, ראינו, ארטום, כל  $\sigma\in\mathrm{Aut}_K(L)$  ממסקנה שראינו שוב באמת האינו, על־ידי (3.2.11, ארטום, כל באמת האינו) מסקנה שראינו (על באמת האינו), על באמת ראינו (על באמת באמנום ארטום, כל באמת באמנום ארטום, ולכן (על באמת באמנום ארטום), ולכן על באמת האינו (על באמת באמנום ארטום), ולכן על באמת באמנום ארטום ארטום ולכן על באמת באמנום ולכן על באמת באמנום ארטום ולכן על באמת באמנום ולכן בא

# :(מיכאל) ברשומות של מיכאל):

- $\gcd(a,n)=1$  אם ורק אם הפיך הוא  $a\in\mathbb{Z}/n\mathbb{Z}$  .1
- (a,n)=1 אם ורק אם אל יוצר של הוא יוצר כי להראות עם יוצר עם מסדר מסדר מסדר עם איקלית מסדר מיוצר .2
- $h\in H$  עבור  $\sigma_a(h)=ah$  על־ידי הנתון איש הנתון כך כך ערכור אבור כך כל אנוני אנוני ( $Z/n\mathbb{Z})^ imes \hookrightarrow \mathrm{Aut}(H)$  עבור 3.

#### :הוכחה

- ההופכי , $ax\equiv 1 mod n$  ולכן ax+ny=1 שמתקיים x,y כך שקיימים מזהות בז'ו נובע מזהות בז'ו נובע אקיימים , $ax\equiv 1 mod n$  ולכן ax+ny=1 ולכן ax+ny=1 הכפלין של ax=1 ולכן ax=1 הפיך.
- בכיוון השני, נניח ש־ab=k הפיך ולכן קיים  $ab=1 \mod n$  המל  $ab=1 \mod a$  הפיך ולכן קיים משמע בכיוון השני, נניח ש־ $ab=1 \mod n$  הפיך ולכן קיים מab=a+k הפיך ולכן קיים מab=a+k ולכן בכיוון מחלק בב כל אירוף לינארי של ab=a+k ולכן עבור בפרט מחלק בב כל מחלק בב כל צירוף לינארי של ab=a+k ולכן עבור מובע כי aa=a+k וולכן בב כי מחלק בב כל מחלק בב כל מחלק בב כל אירוף לינארי של ab=a+k וולכן עבור מובע כי aa=a+k וולכן בב כי מחלק בב כי מחלק בב כל מחלק בב כי מחלק בב כי
- $k\in\mathbb{Z}$  עבור k(ag) עבור k(ag) עבור הראשון נניח ש־k(ag) עבור k(ag) ונסתכל על תת־החבורה הנוצרת על־ידי ag שכל איבריה הם מהצורה ag עבור ag עבור ag הסדר של ag הוא ה־ag הוא כפולה של ag המינימלי כך ש־ag הוא יוצר של ag המפשים ag המינימלי על־ידי ag הוא יולכן ag המינימלי שמקיים את ag הוא יוצר של ag ולכן ag המינימלי שמקיים את ag הוא יוצר של ag היולכן ag היולכן ag המינימלי שמקיים את ag המינימלי שמקיים את יובר על ag היולכן ag היולכן ag המינימלי שמקיים את יובר על־ידי ag היולכן ag היולכן ag המינימלי שמקיים את יובר של ag היולכן ag היונימלי שמקיים את יובר של ag היולכן ag היונית של־ידי ag היולכן ag היולכן ag היונימלי שמקיים את יובר על־ידי ag היונימלי שמקיים את יובר של יובר ש
  - 3. להשלים?

למה L/K כאשר  $\ell$  (כאשר ביקלוטומית מסדר נותמלית). הרחבה ביקלוטומית אזי ביקלוטומית מסדר וו $\ell$ 

- $\gcd(n,a)=1$  אם ורק אם מסדר מסדר פרימיטיבי אורש  $\xi^a$  .1
- $\eta \in \mu_n$  עבור אם  $\sigma(\eta) = \eta^a$  אם ורק אם  $\sigma \mapsto a$ יון) וי $\sigma \mapsto a$ יון) איכון איכון  $\operatorname{Aut}_K(L) \hookrightarrow \operatorname{Aut}(\mu_n) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}$  עבור .2

להשלים כמה טענות לא ברורות בהקשר להוכחה לעיל

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

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

. בזוגות היים אפשר לכל לכל נכונה לכל שהטענה להוכיח אפשר באינדוקציה באינדוקציה אפשר להוכיח א

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

$$\left(\mathbb{Z}_{n}\right)^{\times}\cong\left(\mathbb{Z}_{n_{i}}\right)^{\times}\times\ldots\times\left(\mathbb{Z}_{n_{r}}\right)^{\times}$$

ישר ישר מהגדרות לפתוח הסיני (R imes S) (פשוט מתקיים החורה שעבור R,S חוגים מהגדרות הסיני ויחד עם ההוכחה שעבור איזומורפיזם).

 $.1 < n \in \mathbb{N}$  יהי יבו :21.2

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

 $\lambda:G_{p^n} o G_P=\mathbb{F}_p^ imes$  ואז p ואז בתור התחלה במצום הוכחה: ניקח את שני המקרים בחשבון. נסתכל על הומומורפיזם הצמצום עם מודלו p ואז להשלים...

# 13/05 - 13 הרצאה 22

## 22.1 הרחבות ציקלוטומיות – המשך

#### תשלימי

:הוכחה

# 22.2 הרחבות רדיקליות

פרק 6.4 ברשומות של מיכאל.

 $L=K\left(a^{rac{1}{n}}
ight)$  אם הרחבה הרחבה בקראת הרחבה שדות L/K נקראת הרחבה הרחבה רדיקלית הרחבה בתור אגדרה לפעמים נראה אותה בתור K(lpha)/K עבור lpha המקיים המ

הזה: מהסוג הזה: כבר ראינו שתי בעיות שיכולות לקרות בהרחבות מהסוג הזה:

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

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

- נובע שאם  $\mu_n\subset K$  מההכלה  $t^n-a$  כאשר שדה פיצול אז בודר) אז L הוא שורש נובע על־ידי שורש (ההרחבה הנוצרת על־ידי שורש ל-2. ההרחבה הנוצרת על־ידי שורש בוד $\mu_n lpha = \{lpha, \xi_n lpha, ..., \xi_n^{n-1} lpha \}$  נובע שאם הוספתי שורש t. פיצלתי הכל ב $\mu_n lpha = \{lpha, \xi_n lpha, ..., \xi_n^{n-1} lpha \}$
- - $(C_{lpha/K=\mu_{nlpha}}$  אם ורק אם או קורה אי־פריק (זה אי־פריק אם אם  $\operatorname{Aut}_K(L)=\mu_n$  ובפרט ובפרט | $\operatorname{Aut}_K(L)|=[L:K]$  .3
    - . מכך ש־ $\kappa$  איברים. מכילה  $\mu_n$  ,  $n \in K^{\times}$  איברים. 1

a של ה־nי של השורש הוא  $\xi \alpha \in \mu_n \alpha$  כל

 $\mu_n \alpha$  שורשים, הפולינום הם הפולינום שורשים, שורשים שורשים ח לכל היותר לכל לינום לפולינום לפולינום איז לכל היותר שורשים, ולכן שורשים, ולכל היותר איז לכל היותר שורשים, ולכל היותר של ה

כעת, שדה שדה פיצול של פיצול שדה שדה שלו ולכן (כל השורשים ב־ב') בהיינו מתפצל לחלוטין דהיינו הפולינום  $\mu_n \in L = K(\alpha)$  ולכן (כל השורש שלו ולכן  $\mu_n \in K$  בפרט, הוא נוצר על-ידי שורש אחד)

 $.\xi_\sigma\in\mu_n$ עבור  $\sigma(\alpha)=\xi_\sigma\alpha$  ולכן  $t^n-a$  של שורש אלה, שגם שלו, לצמוד את לוקח לוקח הוא מוחרפיזם .2 מתקיים  $\xi\alpha\in\mu_n$  אחר אחר אחר שורש אחר לכל שורש אחר אחר מכך, לכל שורש אחר

$$\sigma(\xi\alpha) = \sigma(\xi)\sigma(\alpha) = \xi\xi_{\sigma}\alpha = \xi_{\sigma}\cdot(\xi\sigma)$$

 $a^{rac{1}{n}}$  שורש ב־מחירה של תלויה מכפילה ל ונקבל העתקה א השורש  $\lambda: {
m Aut}_K(L) o \mu_n$  משמע המפילה כל שורש ב־ $\xi\sigma$  ונקבל העתקה מכך, א מדעה מכך, פועלת לפי פועלת לפי לפי ג  $\xi_{ au}$  או מכך, ס פועלת לפי המכך,

$$(\sigma \tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\xi_{\tau}\alpha) = \xi_{\sigma}\xi_{\tau}\alpha$$

ולכן  $\lambda$  זה הומומורפיזם.

. שורש שורש lphaכך כך  $t^n-a$  שלים אי־פריק גורם גורם זהי f(t) יהי .3

אז לפי למה ב־ב והעוצמה ב־ב ולכן היש בידיוק (L:K] אז הפולינום הפריד של הפולינום של הפולינום ב־L:K] האז אז אז הפריד אז הפריד של הפולינום הפריד אז הפריד ( $\mathrm{Aut}_K(L)$ ) היא בידיוק (לקשר)

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

 $\mu_n \subseteq K$ ש־ ש־הכרח לא הכלי כאשר כללי במקרה לא הערה: במקרה כללי כאשר

42

14/05 – 6 תרגול 23

23.1 שדות קומפוזיטום

תשלימי

5 תרגיל 24

טריקים 24.1

תשלימי

24.2 מסקנות

תשלימי

#### 19/05 - 14 הרצאה 25

# 25.1 הרחבות רדיקליות – הרחבות ארטין־שרייר

פרק 6.4 ברשומות של מיכאל.

אין שורש (יש שורש לא ספרביליים החלוטין (יש שורש 1, אין הדרה 25.1 (הרחבות ארטין־שרייר): נניח שp>0 אין הרחבות ארטין־שרייר): נניח שרטיער נניח שרטיער אוטומורפיזמים, הרחבות אי־פרידות), אז במקרה זה יש לנו תחליף: פולינום מהצורה בא  $t^p-t-a\in K[t]$  נקרא ארטין־שרייר ועבור כל שורש בארטין־שרייר.  $L=K(\alpha)/K$  פולינום זה, ההרחבה ארטין־שרייר.

.(0 במציין מדרגה יותר מ־1 במציין לפרות לפולינומים מדרגה אזור לקרות לפולינומים ( $f(\alpha+\beta)-f(\alpha)+f(\beta)$  משמע היותר מ־1 במציין לפולינומים מדרגה אזור במציין לפולינומים בגלל שאנחנו במציין פתרון: נשים לב שמתקיים בגלל שאנחנו במציין לפולינומים בגלל שאנחנו במציין אזור פתרון: נשים לב

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

(בים אגפים כשנחסר יעלם בכל־מקרה כי a כי ממהקבוע אז (נתעלם ממהקבוע היא בכל־מקרה בל

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

. (במילים ארטין־שרייר). הוא שורש של פולינום ארטין־שרייר). המקיים lpha=a המקיים  $lpha=\overline{K}$  המקיים ארטין־שרייר). אזי  $a+\mathbb{F}_p=\{lpha, lpha+1, \cdots, lpha+p-1\}$  ויך וווחבור של של  $a+\mathbb{F}_p=\{a, a+1, \cdots, a+p-1\}$  שדה פיצול של  $a+\mathbb{F}_p=\{a, a+1, \cdots, a+p-1\}$ 

המקיים  $\mathrm{Aut}_K(L)\simeq \mathbb{F}_p(=\mathbb{Z}/p)$  חבורות של איזומורפיזם אזי אזומורפיזם אזי  $\alpha\notin K$  אזי ולכן אם אזי לא מעניין כי הוא מעניין כי הוא מתפצל לחלוטין, ולכן אם  $\alpha\notin K$  אזי  $\alpha\in K$  המקיים  $\sigma\mapsto\sigma(\alpha)-\alpha$ 

 $a+\mathbb{F}_p\subseteq K(lpha)=$ ולכן זה שדה פיצול של מורשים אדה מיצול  $a+\mathbb{F}_p\subseteq K(lpha)=$ ורים איז  $a+\mathbb{F}_p\subseteq K(lpha)=$ ולכן זה שורשים איז מורשים איז מ

 $\sigma(lpha)=lpha+$  נניח  $\sigma(lpha)=lpha'$  שדרגתו גדולה מ־1 ולכן יש לו עוד שורש lpha', ולכן יש כך שמתקיים  $\sigma\in {
m Aut}_K(L)$  עניח lpha'=lpha+ שדרגתו גדולה מ־1 ולכן כל lpha'=lpha+ צמוד של lpha'=lpha+ כלומר lpha'=lpha+ שורש lpha'=lpha+ ולכן כל lpha'=lpha ולכן כל lpha'=lpha'=lpha ולכן כל lpha'=lpha'=lpha ורכן כל lpha'=lpha'=lpha ורכן כל lpha'=

נקבל אם כך שמתקיים  $\sigma' \mapsto i'$  האוטומורפיזמים  $p = [L:K] = \deg f_{\alpha/K}$  עם כך אם נקבל אם נקבל אם האוטומורפיזמים והאוטומורפיזמים או

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

25.2 הרחבות פרידות (ספרביליות)

פרק 7.1 ברשומות של מיכאל.

על־ידי (ספרבילית) ברידה פרידה על־ידי ברתבה על־ידי: עבור אי־פרידה) על־ידי ברגה על־ידי עבור אי־פרידה) על־ידי על־ידי ברגה אי־פרידה אי־פרידה על־ידי על־

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

. (בתור התחלה הב- $\mathbb{Q}^-$  אבל בהמשך נראה אי־פרידה בעצם (בתור התחלה הב- $[L:K]_i=rac{[L:K]_s}{[L:K]_s}$  ברידה בישר מספר ה־K

 $[L:K]_i=\deg_{K,i}(lpha)$ ו ר' $[L:K]_s=\deg_{K,s}(lpha)$  אזי פרמיטיבית, אזי הרחבה L=K(lpha)/K: נניח ש־L:K[i] הרחבה פרמיטיבית, אזי וניח שL:K[i] הרחבה למה בפרט, L:K[i] הרחבה בפרט, L:K[i] הרחבה בפרט, וויי בפרט, וויי בפרט, וויי בארט הרחבה פרט, וויי בארט הרחבה פרט הרחבה

 $\deg_{K,s}(lpha)=|C_lpha|$ י הא lpha' את שיכון יחיד שלוקח שכן לכל צמוד שכן  $[L:K]_S=\left|\operatorname{Hom}_K\left(K(lpha),\overline{K}
ight)
ight|=|C_lpha|$  השיוויון השני נובע מכך שמתקיים  $[L:K]_i=\frac{[L:K]_i}{[L:K]_s}=\frac{\deg_K(lpha)}{\deg_{K,s}(lpha)}=\deg_{K,i}(lpha)$  ולכן ולכן  $[L:K]_i=\frac{[L:K]_i}{[L:K]_s}$ 

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

45

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

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

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

הוכחה: נשים לב שמספיק להוכיח את הראשון כי מכפליות הדרגה אוטומטית נקבל את השני.

היות לנו העתקה וזה נותן לנו  $\sigma|_F:F\hookrightarrow \overline{K}$  נגדיר צמצום  $\sigma:L\hookrightarrow \overline{K}$  לכל , $\left|\operatorname{Hom}_K\left(L,\overline{K}\right)\right|=[L:K]_s$ היות ו

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

ניקח של כל הרחבה) או סגור אלגברי (כי זה סגור אלגברי הסיב את  $\overline{K}=\overline{K}$  ואז הסיב עם עם F עם לחבר: נזהה את הסיב את גודל הסיב את גודל הסיב ל $\overline{K}=\overline{K}$  הסיב נהיה איזומורפי ל $\overline{K}=\overline{K}$  הסיב נהיה איזומורפי ל

מכאן, בכל סיב של א יש בידיוק  $[L:F]_s = \left| \operatorname{Hom}_F \left( L, \overline{K} \right) \right|$ איברים איברים מכאן, מכאן

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

 $\operatorname{char}(K)=p>0$  אם  $[L:K]_i\in p^{\mathbb{N}}$ י ר-רחבה באה וור $[L:K]_i=1$  אם הופית לכל הרחבה מסקנה :25.1 מסקנה ווריש.

אז  $L=K(lpha_1, \cdots, lpha_n)$  אם פרימטיביות: אז הרחבות היא מגדל הרחבה חופית שכל הרחבה מכך שכל הרחבה הוכחה: זה נובע ישירות מכך הרחבה הופית היא מגדל של הרחבה הופית היא מגדל של הרחבה החופית היא אז

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

ואז מהלמה לעיל

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

. בהם או המכפלה או  $p^n$  או או מהם המכפלה שלהם.

A בחינו פריד מעל (ספרבילית) אם פרידה ברחבה אלגברית נקראת ברחבה אלגברית ברחבה אלגברית ברחבה אלגברית ברחבה אלגברית נקראת ברחבה פרידה אם ורק אם כל תת־הרחבה סופית היא הרחבה פרידה.

משפט באים שקולים: עבור הרחבה טופית L/K הבאים עבור יעבור יבור יעבור י

הרחבה פרידה L/K .1

K מעל פרידים  $\alpha_1, \cdots, \alpha_n$ ער כך בר $L = K(\alpha_1, \cdots \alpha_n)$ .2

$$[L:K]_s = [L:K]$$
 .3

$$[L:K]_i = 1.4$$

הדרגה. מהגדרת מהגדרה אשית, בבירור בירות מהגדרת שירות ל $3\Longleftrightarrow 4$ מהגדרת הדרגה. הוכחה:

ואנחלינום המינימלי הפולינום המינימלי ב $K_j=K$  כך ש־ $K_j=K$  כך ש־ $K_j=K$  כך שר $K_j=K$  כך שרכינום המינימלי בעצמו ודעים שהפולינום המינימלי בא הפולינום המינימלי בא כי מי שמחלק פריד (כי מי שמחלק פריד הוא פריד בעצמו) ולכן בו הראשון פריד (כי מי שמחלק פריד הוא פריד בעצמו) ולכן בו הראשון פריד (בי מי שמחלק פריד הוא פריד בעצמו) ולכן בו הראשון פריד (בי מי שמחלק פריד הוא פריד בעצמו) ולכן בו בא הראינו על דרגות ולכן בו בו בא בו בא בי ב

כך שמתקיים לא גדל שניה ולכן שL/K(eta)/K כך שמתקיים לבית בשלילה בעלילה פרידה ולכן של פרידה ולכן על פרידה בשלילה בעלילה בעלילה בעלילה איז א ברחבה פרידה ולכן לביש פרידה ולכן בעלילה ב

$$[L:K]_i = \underbrace{[L:K(\beta)]_i}_{=1} \cdot \underbrace{[K(\beta):K]_i}_{>1} > 1$$

וזאת סתירה.

מסקנה הסגור  $K\subseteq L_S\subseteq L$  הרחבה אלגברית שך K שך מעל מעל הספרביליים להאיברים קבוצת כל האיברית קבוצת להתרשה העצם, הרחבה אלגברית המקסימלית).

את כל מוכיח מעל מעל מעל ספרביליים את הרחבה ספרבילית ולכן כל הרחבה ספרביליים מעל או אז מוכיח מעל או הרחבה מפרבילית ולכן אז אז או הרחבה מפרביליים מעל או הרחבה מפרביליים מעל אז אז או הרחבה מפרבילית העדה. מכונות השדה.

K הספרבילי של  $K^S\subseteq\overline{K}$  ווהוא נקרא הסגור הספרבילי של האיברים הספרביליים האלגבריים מעל K ווהוא נקרא הסגור הספרבילי של הגדרה 25.4 הוא גם נורמלי: למשל, שדה פיצול של כל הפולינומים הספרביליים.

F/Kו בא ורק אם ורק אם הרחבה ספרביליות אזי אלגבריות אלגבריות מגדל הרחבות הספרביליות): אם אם ברביליות אוי ברחבות אלגבריות אזי ברחבות הספרביליות): אם L/F/K אם אם ברחבות הספרביליות.

במילים אחרות, הרחבות ספרביליות זו מחלקה שלמה.

K מעל מעל ספרבילי ש־ $\alpha$  ספרביליות, ניקח מפרביליות, ספרבילי ספרבילי מעל הראות הרחבות מעל מעל מעל מעל

 $\beta_i \in F$  כאשר  $f_{\alpha/F} = t^n + \sum_{i=0}^{n-1} \beta_i t^i$  הוא ספרבילי המינימלי הפולינום ולכן הפולינום מער ספרבילי מעל מער כי נתון כי מ

 $f_{lpha/F}$  אז G מקיים פולינום ספרבילית (כי היוצר G מקיים פולינום ספרבילית (כי היוצר G ולכן G ולכן והיא ספרבילית אז G ולכן G והיא ספרביליות ספרביליות ספרביליות סופיות, ולכן מעל G ולכן והיא מגדל הרחבות ספרביליות סופיות, ולכן

$$\left[L':K\right]=\left[L':F'\right]_i\cdot [F:K]_i=1\cdot 1=1$$

K מעל ספרבילי ספרבילית ו־ספרבילי מעל

.15 הערה: את המסקנה לעיל התחלנו להוכיח בהרצאה 14 וסיימנו בהרצאה

## 20/05 - 15 הרצאה 26

## (Perfect Fields) שדות פרפקטים 26.1

הוא אוטומורפיזם הר $\operatorname{Fr}_p$  שקול לכך ש $K = K^p$ ו הוא רביזם הגדרה ברפקט): שדה K נקרא פרפקט אם הגדרה ברה ברות האוטומורפיזם וי $K = K^p$  אוטומורפיזם וי $K = K^p$  אוטומורפיזם וי $K = K^p$ .

 $\ldots \supseteq K^{rac{1}{p}} \supseteq K \supseteq K^{p^2} \ldots$ ולכן ולכן א יש סדרה  $K^{rac{1}{p}} \simeq K \stackrel{\mathrm{Fr}}{\simeq} K^p \simeq K^{p^2}$  יש סדרה עש יש

דוגמה שבת השבת  $K \supseteq \mathbb{F}_{p^n} = \{x \mid x^{p^n} = x\}$  בת על וגם מתקיים על השבת ומשיקולי סדר נקבל ומשיקולי סדר נקבל שהוא השבת אנדומורפיזם ומשיקולי סדר נקבל השבת השבת אנדומורפיזם ומשיקולי סדר נקבל שהוא השבת של השבת השבת השבת השבת השבת השבת של השבת השבת של השבת של השבת השבת של השבת של השבת של השבת של השבת של השבת של השבת השבת של השבת ה

 $t \notin K^p$  כי בפקטי אדה אבל הוא אבל אבל על נסתכל א, נסתכל במציין אלדוגמה K:26.1

#### משפט 26.1 יהי אדה אזי משפט

- היא ספרבילית ברית אלגברית אם ורק אם ורק אם פרפקטי אם פרפקטי אלגברית ל.1
  - פרפקטי אזי לכל הרחבה אלגברית פרפקטי אזי לכל פרפקטי .2

#### :הוכחה

- .. אפשר להניח ש־ $0 \neq 0$  כי בשדה ממציין 0 כל הרחבה היא ספרבילית.  $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  ולכן  $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  ואבילו  $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  וואפילו  $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  אי־פריד הוא אי־פריד מעל  $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  וניח שקיימת הרחבה  $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  אי־פריד הוא אי־פריד הוא  $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  אי־פריק ב־ $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  אבל א אי־פריק ב־ $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  אבל א אי־פריק ב־ $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  אבל א אי־פריק ב־ $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  אבל א אי־פריק ב־ $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  אבל א אי־פריק ב־ $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$  אבל א אבל א אבל א אבל א אי־פריק ב־ $f_{\alpha/K} = f_{\alpha/K} = f_{\alpha/K}$
- שכל זה אומר אבל הריח. אבל לפי ((1) ולכן ((1) פרידה פרידה (פרפקטי אלגברית. אלגברית. אז לכל F/L אלגברית. אלגברית פרידה לפי (1) ולכן אלגברית. אלגברית פרידה אומר שכל בפרידה ולפי (1) נקבל ש־L פרפקטי.

 $.K^{rac{1}{p^{\infty}}} = igcup_{n \in \mathbb{N}} K^{rac{1}{p^n}}$  פרפקטיזציה) במציין על במציין פרפקטיזציה: לכל שדה לכל (פרפקטיזציה) במציין ו

 $(\infty$  אולי  $0 [K:K^p] = p^n$  ידי על־ידי (במציין פער מציין במציין מבה K במציין לכל (אולי -p) (אולי הגדרה 26.3 הגדרה

#### :26.1 תרגיל

- K את שר המכיל המינימלי פרפקט פרפקט הוא הוא הוא המכיל את .1
- . (רמז: פרובניוס) ו $l\in\mathbb{Z}$  לכל  $[K:K^p]=\left[K^{rac{1}{p}}:K
  ight]=\left[K^{p^l}:K^{p^{l+1}}
  ight]$  לכל 2.
  - ני. בי ו ולכן  $\left[K:K^p\right]_s=1$  אז סופי אות שאם הראות שאם .3

 $r_p(K)=1=p^0$ ואז פרפקטי $K)\Longleftrightarrow r_p(K)=0$  ואז וואז  $r_p(K)=1=p^0$ פרפקטי: נסמן מלהיות פרפקטי: נסמן הערה:  $r_p(K)=1$ 

22/05 – 7 תרגול 27

27.1 משהו

תשלימי

6 תרגיל 28

28.1 טריקים

תשלימי

28.2 מסקנות

תשלימי

# 26/05 - 16 הרצאה 29

# (purely inseparable) בטהרה בטהרות אי־פרידות אי־פרידות 29.1

פרק 7.2 בסיכום של מיכאל.

 $\operatorname{char}(K) = p > 0$ כל הפרק הוא תחת ההנחה כל

(זאת־אומרת,  $\deg_{K,s}(lpha)=1$  מתקיים  $lpha\in L$  מתקיים בטהרה אי־פרידה בקראית אי־פרידה אלגברית בטהרה): הרחבה אלגברית בטהרה בעל מקרידה בטהרה אי־פרידה בטהרה ( $\mu$  של ממוד יחיד, כמו למשל כל החזקות עד פאר.

# 29.2 תורת גלואה

# 29.3 התאמת גלואה

27/05 - 17 הרצאה 30

30.1 התאמת גלואה – המשך

28/05 – 8 תרגול 31

31.1 משהו

7 תרגיל 32

32.1 טריקים

32.2 מסקנות

# 03/06 - 18 הרצאה 33

33.1 המשפט היסודי של תורת גלואה

# 04/06 - 9 תרגול 34

# 34.1 פולינומים סימטריים

 $\sigma \cdot t_i = t_{\sigma(i)}, \ \sigma \cdot$  על־ידי  $S_n$  לינומים פעולה אלמנטריים: יהי  $T_n$  שדה ו־ $T_n$  שדה פעולה שלמנטריים אלמנטריים: יהי אלמנטריים שדה ו־ $T_n$  $.P(t_1, \dots, t_n) = P(t_{\sigma(1), \dots \sigma(n)})$ 

. $\operatorname{Gal}(L/K) \simeq S_n$  את שמתקיים שמתקיים של הפעולה, ובהרצאה של את שדה נקודות שדה את  $K = L^{S_n}$ נסמן ב

נגדיר  $f(x)=x^n-s_1$ , כאשר  $f(x)=x^n-s_1x^{n-1}+s_2x^{n-2}+\cdots+(-1)^ns_n$  נגדיר  $f(x)=\prod_{i=1}^n(x-t_i)\in L[x]$  נגדיר נגדיר אם מקדמי

$$-s_1 = -t_1 - t_2 - \dots - t_n \Rightarrow s_1 = \sum_{i=1}^n t_i$$
 
$$s_2 = \sum_{1 \le i \le n} t_i t_j, \ s_k = \sum_{1 \le i \le n \le n} t_i \cdots t_k$$

אבל זה אבל את סדר הגורמים את הפולינומים שייכים ל- $L^{S_n}$  והם שייכים ל-nל-משתנים הסימטריים האלמנטריים האלמנטריים ל- $s_1, \dots s_n$  נקראים הפולינומים הסימטריים האלמנטריים ל-(f משנה את

 $L=F(s_1,\cdots,s_n)$  מקיים (עיל) מההגדרה של הפעולה של תחת על עדה השבת (שדה השבת לעיל) מענה 34.1 מענה אות על ישרה השבת אות מענה ו

ומצד  $[L:F(s_1,\cdots,s_n)]\leq \deg(f)!=n!$  אז  $F(s_1,\cdots,s_n)$  מעל של שדה פיצול הכיוון השני:  $L:F(s_1,\cdots,s_n)$  אז ההכלה בכר ראינו, עבור הכיוון השני:  $L:F(s_1,\cdots,s_n)$ מתקיים מהכרח ולכן בהכרח  $[K:F(s_1,\cdots,s_n)] \leq 1$  נקבל ב־י!ת נחבר לאחר לאחר וביחד וביחד ולכן בהכרח ולכן ולכן הכרח ולכן ולכן הכרח מתקיים  $[L:F(s_1,\cdots,s_n)] = [L:K]$ 

=n! ממשפט ארטין  $S_n$  וסדר החבורה  $[K:F(s_1,\cdots,s_n)]=1$  מהגדרת הדרגה מ

П

כך  $F[x_1,\cdots x_n] \hookrightarrow F[s_1,\cdots,s_n]$  ביזומורפיזם (המשפט היסודי של הפולינומים הסימטריים) בי $F[t_1,\cdots t_n]^{S_n} = F[s_1,\cdots,s_n]$  כך משפט 34.1 המשפט היסודי של הפולינומים הסימטריים)  $P(x_1, \dots, x_n) \mapsto P(s_1, \dots s_n)$ 

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: אותו של מונום סימטריים. בול הוא אותו א הוא אחד המונומים אותו ל $t^{a_1}_{\sigma(1)}\cdots t^{a_n}_{\sigma(n)}$  אז גד $t^{a_1}_1\cdots t^{a_n}_n$  אותו אחד המונומים סימטריים. בפולינומים סימטריים איברי איברי דים פולינומים סימטריים. בפולינומים סימטריים אחד המונומים אותו אותו אותו של הוא אותו של הוא אותו של אותו אותו של אותו אותו של אותו אותו של אות  $f(t_1,t_2)=t_1+t_1t_2^2+\cdots$  פולינום (זאת אומרת, אם ניקח את  $t_2$  את  $t_2=t_1+t_1$  נמצאים בי

 $t_1^{a_1} \cdot t_2^{a_2} \cdot \cdots \cdot t_n^{a_n} > t_1^{b_1} \cdot t_2^{b_2} \cdot \cdots \cdot t_n^{b_n}$  אם: נתון על־ידי (הסדר הלקסיגורפי על המונומים): נתון אם:

- $a_1 + \dots + a_n > b_1 + \dots + b_n$  .1
- $a_i>b_i$ מקיים  $a_i\neq b_i$ שר כך הראשון וגם ה־<br/> i הגם וגם  $a_1+\cdots+a_n=b_1+\cdots b_n$ . 2

טענה 34.2 (תכונות הסדר הלקסיגורפי על המונומים):

- $m_1 m_{1'} > m_2 m_{2'}$  אז  $m_{1'} > m_{2'}$  גום הוגם  $m_1 > m_2$  מונומים כך שינומים הוגם  $m_{1'}, m_{2'}$  מונומים וגם הוגם מונומים וגם אם .1
  - 2. לכל מונום יש מספר סופי של מונומים שקטנים ממנו

, בפרט, המונומים המונומים מכפלת המונומים או המונומים אז המונום המונומים אז המונומים אז המונומים אז אם אז המונומים מסקנה 34.1 אז המונומים אז המונומים פרט, אם אם מסקנה או מכפלת מסקנה אז המונומים מסקנה המונומים המונומים מסקנה אז המונומים המונומים המונומים המונומים המונומים המונומים מסקנה מחובילים. בפרט,  $t_1^{a_1} \cdot (t_1t_2)^{a_2} \cdot (t_1t_2t_3)^{a_3} \cdot \dots = t_1^{a_1+a_2+\dots+a_n} \cdot t_2^{a_2+\dots a_n} \cdot \dots \cdot t_n^{a_n}$  המונום המוביל של  $s_1^{a_1} \cdot \dots \cdot s_n^{a_n}$  המונום המוביל של לכן למונומים שונים ב- $s_i$ -ים, במונחי ה- $t_i$ -ים, במונחי שונים שונים לכן למונומים שונים ב-

, מונומים ב־ $x_i$ ים, שונומים לא טריוויאלי לא צירוף לינארי לא פרי $P(s_1,\cdots,s_n) \neq 0$  אז אז דו אונומים לא מונומים לא פריב, אורה מסקנה שירה לא מונומים בי $x_i$ כשנציב את ה־ $t_i$ ים נקבל צירוף לינארי של מונומים ב־ $s_i$ ים, מתוך אלו, כשנשכתב למונחי של טריוויאלי של טריוויאלי של מונומים ב־ $s_i$ ים, מתוך אלו, כשנציב את ה־ $s_i$ ים נקבל צירוף לינארי לא טריוויאלי של מונומים ב־ $s_i$ ים, מתוך אלו, כשנשכתב למונחי של הישר לאחד יש דרגה מקסימלית בת. שום עם שמטמצם לא יכול איכול דבר. במונחי $t_i$ ידם במונחי

זה מביא לנו את "היש איזומורפיזם" מהמשפט היסודי.

 $.f_2$  של של מונום מוביל של  $t_1t_2$ י הוא מונום מוביל של הסדר הסדר הסדר הסדר. מהגדרת הסדר הוא מונום מוביל של הוא מונום מוביל יהיה  $.t_1t_2^3$  הוא מונום המונום המונום המוביל יהיה  $.t_1t_2^3$  הוא מונום מוביל יהיה מונום מוביל של מונום מונו

 $f=P(s_1,\cdots,s_n)$ עך כך כך  $p\in F[x_1,\cdots x_n]$ שקיים להראות רוצים סימטרי, אחנו פולינום פולינום כעת, בהינתן

 $t_i$  בין החליף אז ניתן להחליף אז ניתן להחליף בין מימטרי אז  $a_i < a_{i+1}$  את המונום המוביל של  $c \cdot t_1^{a_1} \cdot \cdots \cdot t_n^{a_n} : f$  ומכיוון ש־ $c \cdot t_1^{a_1} \cdot \cdots \cdot t_n^{a_n} : f$  אז ניתן להחליף בין ניקח את המונום המוביל של  $c \cdot s_1^{a_1-a_2} \cdot s_2^{a_2-a_3} \cdot \cdots \cdot s_n^{a_n} : f$  וזה פולינום סימטרי. נשים לב שזה בידיוק המונום המוביל של  $c \cdot s_1^{a_1-a_2} \cdot s_2^{a_2-a_3} \cdot \cdots \cdot s_n^{a_n} : f$  קטן יותר. המונום המוביל של  $c \cdot s_1^{a_1-a_2} \cdot s_2^{a_2-a_3} \cdot \cdots \cdot s_n^{a_n} : f$ 

וכל פעם אנחנו  $c\cdot s_1^{a_1-a_2}\cdot s_2^{a_2-a_3}\cdot \dots \cdot s_n^{a_n}$  חותר מספר מונומים שקטנים של מונומים לכי יש רק מספר סופי של (כי יש רק מספר סופי של מונומים בי  $c\cdot s_1^{a_1-a_2}\cdot s_2^{a_2-a_3}\cdot \dots \cdot s_n^{a_n}$  מקטינים ממש את המונום המוביל), ולכן כשנגיע ל־ $c\cdot s_1^{a_1-a_2}\cdot s_2^{a_2-a_3}\cdot \dots \cdot s_n^{a_1-a_2}$ 

. דוגמה 1.34.2 ניקח  $f=t_1^2+t_2^2$  ומהגדרת הסדר הלקסיגורפי נקבל  $t_1^2$  הוא מונום מוביל, ונכתוב את  $f=t_1^2+t_2^2$  ומהגדרת הסדר הלקסיגורפי נקבל  $t_1^2+t_2^2-t_1^2-2t_1t_2-t_2^2=-2t_1t_2=P_1$  אוז  $s_1^2=(t_1+t_2)^2=t_1^2+2t_1t_2+t_2^2+t_1^2$  בצעד הראשון, ניקח את את  $P_1-2s_2=2t_1t_2-2s_2=0$  נאז  $P_1-2s_2=2t_1t_2-2s_2=0$  נאז  $P_1-2s_2=2t_1t_2-2s_2=0$  ואל השני ניקח אז את  $P_1-2s_2=2t_1t_2-2s_2=0$  האל השני ניקח אוז את  $P_1-2s_2=2t_1t_2-2s_2=0$  האל השני ניקח אוז את באריים השני מוניקה השני ניקח אוז את באריים השני מוניקה השני מוניקה

#### Norm, Trace 34.2

ההרחבה אופרטור  $M_{lpha}:L o L$  ונגדיר העתקה ונגדיר הרכחבה סופית): תהיי תהיי תהיי אופרטור הרכחבה ונגדיר אופרטור אופרטור אופרטור אופרטור האופרת (עקבה ונורמה של הרחבה הופית).  $M_{lpha}(x)=lpha\cdot x$  סופית) על־ידי

ביחס לבסיס מ־ $M_{lpha}$  ביחס לבסיס מ־ $M_{lpha}$  ביחס ל $\alpha=x+y\sqrt{7}$  ועבור  $\mathcal{B}=\left(b_1=1,b_2=\sqrt{7}\right)$  הוא למשל ל $\Delta L/K$ הוא ביחס ל- $\Delta L/K$ ביחס לבסיס מ־ $\Delta L/K$ ביחס מ־ $\Delta L/K$ 

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

טענה lpha אזי הם הצמודים של  $lpha_1, \cdots lpha_n$  אזי מענה 34.3 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.

8 תרגיל 35

35.1 טריקים

35.2 מסקנות

05/06 – שעת קבלה של גבע 36

36.1 מסקנות

- 09/06 19 הרצאה 37
- 37.1 עוד עובדות על התאמת גלואה
  - 37.2 שימושים של תורת גלואה

# 10/06 - 20 הרצאה 38

38.1 בניות של מצולעים משוכללים

# 11/06 – 10 תרגול 39

#### 39.1 הדיסקרמיננטה

f שדה פיצול של רבר  $\operatorname{char}(F) \neq 2, f \in F[x]$  שדה פיצול של לאורך התרגול,

. שורשים  $\alpha_i$ ור המקדם המקדם האו<br/>ה $\alpha$  כאשר  $f(x) = \alpha \prod_{i=1}^n (x - \alpha_i)$ ב־בLב-ב

. השורשים. G של משתכנת ב-G השורשים, נסמן אי־פריק של אי־פריק לבנתיים וראינו  $G=\mathrm{Gal}(L/F)$ נניח למתוקן, אי־פריק של אי־פריק לבנתיים וראינו

$$.L\ni R=\prod_{1\leq i< j\leq n}\bigl(\alpha_i-\alpha_j\bigr)$$
 ונגדיר  $\sigma(\alpha_i)=\alpha_{\sigma(i)}$ את  $\sigma\in G$ נסמן נסמן

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

הוכחה: מתקיים

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

. שכן מכבד מכבד ולכן אוטומורפיזם שכן  $\sigma$ 

כאשר הסימן הוא הסימן אותם הגורמים כמו ב-R בפרט אולי לסימן ולכן בפרט את אותם הגורמים כמו ב-R בפרט אולי לסימן ולכן

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

 $\operatorname{sgn}(\sigma) = (-1)^{\ell}$ יידוע ש

 $D_f\in L^G=F$  ולכן  $\sigma\in G$  לכל  $\sigma(D_f)=D_f$  עב לב שים ונשים של את הדיסקרמיננטה את מאר ב-2 אינווריאנטי (נסמן ב-2 אינווריאנטי תחת כל אוטומורפיז מילים אחרות, אינווריאנטי תחת כל אוטומורפיז

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

.(F-ם שורש ה' (כלומר, ש כ־כלומר, היא ריבוע ה'  $D_f$  אם ורק אם  $G\subseteq A_n$ 

. ההרחבה אותה אותה מתוקן ו- $F \neq 0$  באורם מתוקן היה אפשר לחלק בגורם מתוקן ו- $f \neq 0$  אותה ההרחבה. הארחבה מתוקן היה אפשר לחלק בגורם מתוקן ו- $f \neq 0$  אותה ההרחבה.

## :39.1 דוגמה

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

ולכן

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

אז נוכל לכתוב

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

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 לפולינום אי־פריקות אי־פריקות קריטריון וקיבלנו התפצל כבר ב-F מתפצל אבל אבל  $A_2=\{e\}$  אבל אבל אבל הייבוע כך עוקר או אי־פריקות אבל אבל אבל האבל אבל הייבוע ב- $G\subseteq A_2$  אבל אבל אבל אבל אבל הייבוע מתפצל כבר ב-G

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

*הוכחה*: ישירות מ התאמת גלואה.

f במקדמי כפולינום כפולינום  $D_f$  את שלנו זה המטרה שלנו יפה עבורו, אז אבל אין לנו ביטוי של $D_f$  אבל תכונות של $D_f$  אבל אין לנו ביטוי יפה עבורו, אז המטרה שלנו זה להביע את

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

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

. חיובית מדרגה משותף מדרגה על הf,gיש אם ורק אם  $\mathrm{Res}(f,g)=0$ : 39.2 למה

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

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

אם ורק אם יש תלות אם ורק השורות השורות בין השורות לינארית בין הפולינומים  $\mathrm{Res}(f,g)=0$ 

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

כלומר

$$0 = \sum_{i=0}^{m-1} c_i x^i f + \sum_{i=0}^{n-1} d_i x^i g = \left(\sum_{i=0}^{m-1} c_i x^i\right) f + \left(\sum_{i=0}^{n-1} d_i x^i\right) g \Rightarrow \left(\sum_{i=0}^{m-1} c_i x^i\right) f = \left(-\sum_{i=0}^{n-1} d_i x^i\right) g \Rightarrow \left(\sum_{i=0}^{m-1} c_i x^i\right) f = \left(-\sum_{i=0}^{m-1} c_i x^i\right) g \Rightarrow \left(\sum_{i=0}^{m-1} c_i x^i\right) f = \left(-\sum_{i=0}^{m-1} c_i x^i\right) g \Rightarrow \left(\sum_{i=0}^{m-1} c_i x^i\right) f = \left(-\sum_{i=0}^{m-1} c_i x^i\right) g \Rightarrow \left(\sum_{i=0}^{m-1} c_i x^i\right) f = \left(-\sum_{i=0}^{m-1} c_i x^i\right) g \Rightarrow \left(\sum_{i=0}^{m-1} c_i x^i\right) f = \left(-\sum_{i=0}^{m-1} c_i x^i\right) g \Rightarrow \left(\sum_{i=0}^{m-1} c_i x^i\right) g \Rightarrow \left($$

. איוויאלית. משש התלות לא ורק אם ורק שונה מ-m+n והיא משש מדרגה לא מדרגה של מדרגה לא מדרגה משותפת של מי

יש כפולה משותפת חייבת להיות מכפלה של כל הגורמים: אחרת, הם זרים, וכפולה משותפת להיות מכפלה של כל הגורמים יש כפולה מדרגה של לפחות m+n.

$$\mathrm{Res}ig(x+8,x^2+1ig)=0, \ \ \mathrm{Res}(x+1,2x+2)=\detegin{bmatrix} 1 & 1 \ 2 & 2 \end{bmatrix}=0$$
 :39.2 דוגמה

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

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

*הוכחה*: טכני מאוד.

הערה (תזכורת – נגזרת פורמלית וכלל לופיטל לנגזרת פורמלית):

עבור אומר לנגזרת פורמלית לנגזרת פורמלית לנגזרת  $f'=na_0x^{n(n-1)}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}$  מתקיים מתקיים לנגזרת פורמלית לנגזרת פורמלית שמתקיים ביים  $f'(\alpha_i)=\prod_{j\neq i}(\alpha_i-\alpha_j)$ 

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

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

. $\mathrm{Gal}(L/F)\subseteq A_n$  אם ורק אם Fים אוא ריבוע היבוע לעיל וי $D_f$  הוא ביחס להגדרה לעיל ובפרט, גם ביחס להגדרה ובפרט, אם ורק אם ורק אם ורק אם ורק אם הורק אם הורק אם הורק למה ובפרט. ובפרט הורק אם ובפרט הורק ובפר

- 9 תרגיל 40
- טריקים 40.1
- **40.**2 מסקנות

# 16/06 - 21 הרצאה 41

#### 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.

 $G=\mathrm{Gal}(L/\mathbb{Q})\simeq (\mathbb{Z}/p\mathbb{Z})^{ imes}\simeq \mathbb{Z}/(p-1)\mathbb{Z}:=G^{ad}$  היי שמתקיים , $L=\mathbb{Q}ig(\xi_pig)$  את ראשוני ונבחן את יהי Gמאינדקס בים מאינדקס של ההרחבה וזו  $H=G^2$  אותה מאינדקס Hמאינדקס מאינדקס של הריבועים שב-G

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

 $p \neq 2$  עבור  $G^2 < G$  איז מסקנה (41.2 תת־חבורה מאינדקס מסקנה  $G^2 < G$ 

 $G = \{1,2,3,4\}, G^2 = \{1,4\}$  נקבל p=5 נקבל :41.1 דוגמה 1.1 אבור

הגדרה ( $p \neq 2$ ) ויהי ( $p \neq a$ ) וי

ובסימונים של מיכאל

$$\begin{pmatrix} \frac{a}{p} \end{pmatrix} = \begin{cases} 1 & a \in G^2 \\ -1 & a \in G \smallsetminus G^2 \\ 0 & (p \nmid a) \end{cases}$$
 אחרת

 $G^2$  הוא בידיוק הוא והגרעין והגרעין מובן בעצם הוא בעצם ל $G\mapsto G/H=\{\pm 1\}$  הוא בידיוק זה כמובן כמובן הומ

p=5 מתקיים: **41.2** מתקיים

$$\begin{array}{cccc}
 a & \left(\frac{a}{p}\right) \\
 0 & 0 \\
 1 & 1 \\
 2 & -1 \\
 3 & -1 \\
 4 & 1 \\
 5 & 0
\end{array}$$

תרגיל 1.11 ב־
$$F_p$$
 להראות שמתקיים: 41.1  $\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}$  . 1  $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$  . 2

1. זה מבחן אויילר.

2. נובע ישירות מסעיף א' וחוקי חזקות

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

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

 $S = S_p$ יהי באשוני ו־2 < p יהי יהי יהי

 $\mathbb{Q}(\xi_p)$  אם היחידה הריבועיות היחיבה עת־ההרחבה איז  $\mathbb{Q}(\sqrt{p})$ ו $S^2=p$  אז p=4n+1 אם

. $\mathbb{Q}ig(\xi_pig)$  אם היחידה היחיבה הרחבה איא  $\mathbb{Q}ig(\sqrt{-p}ig)$ ו וי $S^2=-p$  או איז p=4n+3

את שנחשב מספיק מספיק שנחשב את מהגדרה מהוכחה: מההגדרה את

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

 $S^2\in\mathbb{Q}$ הסדר סכימה עבר להיות מ־0 כי (0,0)=0 לכל לכל שנבחר ונשים לב ש־(0,0)=0 כי להיות מ־0 כי הסדר הסדר לבנמק למה בגל להיות מ'(0,0)=0 בגלל התאמת גלואה) ונסתכל על האוטומורפיזם לב(0,0)=0 בגלל התאמת גלואה) ונסתכל על האוטומורפיזם לב מ'(0,0)=0 בגלל התאמת גלואה ונסתכל על האוטומורפיזם לב מ'(0,0)=0

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

ולכן

$$\sigma_k\big(S_p^2\big) = \left(\sigma_{k(S_p)}\right)^2 = \left(\left(\frac{k}{p}\right)S_k\right)^2 = \left(\frac{k}{p}\right)^2 S_p^2 \underset{\left(\frac{k}{p}\right) \in \{\pm 1\}}{=} S_p^2$$

 $S_p^2\in\mathbb{Q}$  ולכן כל  $S_p^2$  השמרת את את השמרת הלואה בחבורת כל כל כל  $S_p^2$  ולכן את את את משמרת את בחבורת השלנו: ב־ $S_p^{p-1}$  פעמים את 1 ו־ $S_a^{p-1}$  פעמים את להוכחה שלנו: ב־ $S_a^{p-1}$  יש לנו  $S_a^{p-1}$  פעמים את 1 ו־ $S_a^{p-1}$  פעמים את להוכחה שלנו: ב־ $S_a^{p-1}$  יש לנו להוכחה שלנו: ב- $S_a^{p-1}$  פעמים את 1 ו־ $S_$ (פשוט סוגריים, שהוא נתון על־ידי (פשוט מהגדרה/פתיחת הוא נתון נתון על־ידי על שהוא לחשב את נתון על

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

במילים אחרות,

$$a+b\equiv 0(\operatorname{mod} p) \Longleftrightarrow b\equiv -a(\operatorname{mod} p)$$

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

$$\begin{split} c_0 &= \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \left(-\frac{a}{p}\right) \lim_{\text{deceding approximation}} \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{a}{p}\right) \left(-\frac{1}{p}\right) \\ &= \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^2 \left(-\frac{1}{p}\right) \lim_{\left(\frac{a}{p}\right)^2 = 1 \forall x \not\equiv 0 (\text{mod } p)} \sum_{a=1}^{p-1} \left(-\frac{1}{p}\right) \\ &= (p-1) \left(\frac{-1}{p}\right) \lim_{\text{defends}} (p-1) (-1)^{\frac{p-1}{2}} \end{split}$$

 $.\left(-rac{1}{p}
ight)=-1$  אז  $p\equiv 3 \mod 4$  ואם  $\left(-rac{1}{p}
ight)=1$  אז  $p\equiv 1 \mod 4$  ולכן אם למה  $p\equiv 1 \mod 4$  כי זו פשוט דרך מהירה לקבל האם החזקה תניב  $p\mod 4$  או  $p\equiv 1 \mod 4$ 

 $(-1)^{2n}=1$  אם או הוקה הוגית ונקבל  $rac{p-1}{2}=2n$  ואז ווא או או הוקבל ווא אם 1 אם 1 אם 1.

 $(-1)^{2n+1}=(-1)$  אם אי־זוגית ונקבל ( $-1)^{2n+1}=2n+1$  ואז וא p=4n+3 אם  $p\equiv 3 \, \mathrm{mod} \, 4$  אם .2

עכשיו בחזרה ל־ $(c_1=\cdots c_{p-1})$  (כי  $c_0+(p-1)c_1=0$  ולכן אונ בחזרה ל- $c_0\in\mathbb{Q}$  (כי כי געינו כי אינו כי כי בחזרה ל-

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

ובסד־הכל

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

. ההקדמה שראינו שראינו ער ההרחבות  $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{-p})\subseteq\mathbb{Q}(\xi_p),\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{p})\subseteq\mathbb{Q}(\xi_p)$ הן תתי-ההרחבות שראינו בהקדמה.

$$p=4n+3$$
 כאשר הוכיח שאם  $S_p=\sqrt{p}i=\sqrt{-p}$ ור ור אם אם אם אזי אזי  $\xi=e^{rac{2\pi i}{p}}$  הערה: גאוס הוכיח שאם אזי

$$.\left(rac{2}{p}
ight)=(-1)^{rac{p^2-1}{8}}$$
 נוכיח כי יובמה 31.3 נוכיח כי

הטריק בי $\mathbb{Q}(\xi_8/\mathbb{Q})$ : מתקיים בימה ריבועיות הטריק הוא לבטא את ביל נחשב כמה מחשב כמה לבטא את לבטא את לבטא הטריק הוא

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

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

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

 $\mathbb{Q}\!\left(\sqrt{2}
ight)\!,\mathbb{Q}\!\left(\sqrt{-2}
ight)\!,\mathbb{Q}\!\left(i
ight)$  המדוברות המדוברות ולכן

וגם  $\mathbb{F}_{p^2}(\xi_8)\subseteq\mathbb{F}_{p^2}$  אז  $p\equiv\pm 1\,\mathrm{mod}\,8$  וגם  $\mathbb{F}_{p^2}$  איז  $p\equiv\pm 1\,\mathrm{mod}\,8$  וגם לכן אם

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

# 41.2 הרחבות ציקליות ופתירות ברדיקלים

פרק 8.4 ברשומות של מיכאל.

 $\sqrt[p]{m}$  בעזרת שניתן ארטין־שרייר במציין: עושורשים על ארטין־שרייר במציין:

. כלשהו.  $\sqrt[\infty]{V}$  כלשהו וסגור לשורש כשדה הקטן ביותר כשדה כשדה  $\sqrt[\infty]{K}$  כלשהו נגדיר נגדיר במציין  $\sqrt[\infty]{V}$ 

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

. היא ציקלית. הרחבת שדות  $G=\operatorname{Gal}(L/K)^{\perp}$  סופית הרחבת אם זו הרחבת נקראת נקראת נקראת שדות שדות L/K הרחבת שדות איקלית.

 $n \in K^ imes$ ו בי ונניח כי אוות מדרגה שדות הרחבת הרחבת באר: 41.2 משפט בי

 $a\in K$ עבור עבור  $\alpha=a^{\frac{1}{n}}$ עבור עבור אם ורק אם אם אם אם מדרגה ציקלית הרחבה אזי L/Kאזי אזי אוי

הם  $a^{rac{1}{n}}$  שכן צמודים של L/K, שכן צמודים של משוכן לתוך שכן ניח כי נניח כי L/K, מלמה שראינו,  $L=K\left(a^{rac{1}{n}}\right)$  הם הוכחה: . (כי  $K(a^{rac{1}{n}}/L$  פרידה ונורמלית ומשיוויון דרגות נקבל את השיוויון). מהצורה  $G=\mu_n$  ולכן ולכן  $G=\mu_n$ 

L/K של  $lpha=a^{rac{1}{n}}$  יוצר של ההרחבה, עלינו למצוא יוצר  $\sigma$  יוצר של  $Gal(L/K)\simeq \mathbb{Z}/n\mathbb{Z}$  של של שלינו למצוא יוצר שדות ציקלית ולכן  $lpha=a^{rac{1}{n}}$ 

. $(t^n-1=\prod_{\xi_i\in\mu_n}(t-\xi_i)$  מתקיים (מתקיים K

 $\sigma(lpha_i) =$ בך ש־ $lpha_1, \cdots lpha_n$  כך פיים מעל K, ולכן מעל ש־ $\sigma$  לכסין מעל אנחנו יודעים שונים) אנחנו לינאריים שונים אנחנו לינאריים שונים אנחנו אנחנו מאנים אנחנו מעל איז מתפרק לגורמים לינאריים שונים אנחנו אנחנים אות אנחנים א  $\xi_i \in \mu_n$  עבור  $\xi_i \alpha_i$ 

.m=nולכן ה $\sigma^m=1$ ער כך ביח תת־חבורה יוצרים ווצרים הם יוצרים את מייצרים ל $\xi_i$  מייצרים בטח

$$.\sigma(lpha)=\underbrace{(\xi_1\cdot\cdots\cdot\xi_n)}_{\text{COL}}lpha$$
 אז  $lpha=lpha_1\cdot\cdots\cdotlpha_i$  לכן אם

 $lpha^n \in L^{\operatorname{Gal}(L/K)} \stackrel{=}{\underset{\mathsf{K} \cap \mathcal{K}}{=}} K$ 

## 17/06 - 22 הרצאה 42

# 42.1 הרחבות ציקליות ופתירות ברדיקלים – המשך

שורש שורש (זה מעניינות מדרגה lpha=p , $lpha^p-lpha=a$  אט בעצם בעצם ארטין־שרייר ארטין המעניינות מדרגה אז ההרחבות המעניינות מדרגה  $p=\mathrm{char}(K)$  אם p ארטין־שרייר, שורש מסדר p שהוא פריד וברגע שמצאנו אחד מצאנו את כולם) ונוכיח שאלו כל ההרחבות הציקליות מדרגה ארטין

 $a^{rac{1}{n}}=\mu_n\cdot lpha$  בודה  $a^{rac{1}{n}}=\mu_n\cdot lpha$  בודה בודה לואה היא היא היא היא בודה לואה היא

 $\mathbb{F}_n$  איא הגלואה הובורת lpha=lpha עבור  $lpha+\mathrm{Fr}_n$  זה L=K(lpha)ב־

משפט  $a\in K$  אם  $a\in K$  איז לכל  $a^p-\alpha-a=0$  כאשר באם  $a\in K$  אם אם ורק אם  $a\in K$  איז איז אוז אוז אוז ביקלית (גלואה) אם ורק אם  $a\in K$  איז אוז ביקלית (גלואה) איז אוז ביקלית (גלואה) אם ורק אם ביקלית (גלואה) אוז אוז ביקלית (גלואה) אוז ביקלית (גלו . ארטין־שרייר) היא הרחבת ארטין־שרייר). L=K(a) אומרת

 $\Leftarrow$  ארטין־שרייר). אוטומורפיזמים (ראינו כשדיברנו ארטין־שרייר). גלואה כי יש שם אוטומורפיזמים אוטן ארטין־שרייר ארטין־שרייר). או L=K(lpha) אם בוכחה: . יוצר. שהוא כמובן שהוא  $0 
eq \sigma \in \operatorname{Aut}(L/K) = \mathbb{Z}/p\mathbb{Z}$  שהוא כמובן יוצר. נניח כי

 $f_{\sigma}\mid\underbrace{t^p-1}_{-(t-1)^n}t^p-1$  את מחלק את מהופייני של הפולינום ולכן מתקיים ולכן מתקיים מתקיים מכך שהוא יוצר מתקיים  $\sigma^p=\mathrm{Id}$  ולכן הפולינום האופייני של ה $\sigma:L o L$  פועל

 $.\sigma(\beta) \neq \beta$ כך ש־ $\beta \in L$ וקיים ולא 0ולא נילפוטנטי $\sigma - \operatorname{Id}$ לכן לכן

 $(\sigma(eta)
eq eta$  כי eta
eq K כי  $b\in K$  נסמן  $b\in C$  בממן  $b\in C$  אבל  $b\in C$  ולכן  $b\in C$  ולכן הלכן  $b\in C$  גומר אבל ולכן א

 $\sigma(\alpha)-\alpha=\frac{\sigma(\beta)-\beta}{b}=1$  ואז  $\sigma(\alpha)=\alpha+1$  ניקח  $\sigma(\alpha)=\alpha+1$  ואז  $\sigma(\alpha)=\alpha+1$  איז פעולה של  $\sigma(\alpha)=\alpha+1$  לסיכום, הפעולה של  $\sigma(\alpha)=\alpha+1$  על  $\sigma(\alpha)=\alpha+1$  לסיכום, הפעולה של  $\sigma(\alpha)=\alpha+1$  איז קבוצת הצמודים של  $\sigma(\alpha)=\alpha+1$  לסיכום, הפעולה של  $\sigma(\alpha)=\alpha+1$  איז קבוצת הצמודים של  $\sigma(\alpha)=\alpha+1$ ארטין־שרייר).

ואז הפולינום המינימלי

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

 $f(lpha+i)=(lpha+i)^p-(lpha+i)-a=0$  מתקיים  $i\in\mathbb{F}_p$  נראה לשכל: בראה ניסמן ונטען ש" ונטען מ"  $a=lpha^p-p$  נראה לשכל מחלים: בראה לשכל מתקיים

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

ולכן נקבל

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

 $.t^p-t-a$ שרש של ( $\alpha+i)$  ,  $i\in\mathbb{F}_p$ לכל לכל ולכן ולכן

השונים שונים  $\{lpha, lpha+1, \cdots, lpha+i-1\}$  השורשים שונים,  $lpha_i^p-lpha=a^p$  כך ש $lpha_i^p-lpha=a^p$  זה כל די זה כל מדי זה כל מדיים שונים שונים שונים וובים אונים שונים שונים שונים שונים אונים שונים שונים וובים אונים אונים שונים שונים וובים אונים שונים שו  $f_{\alpha}=t^{p}-t-a$  ואז

 $:a\in K$  נסיק

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

ובזאת סיימנו כי זו הרחבת ארטין־שרייר.

. או באוכחה לעיל גלואה ולא ציקלית כי מהתאמת גלואה בכל־מקרה חבורת גלואה היא מסדר p ראשוני וזה יהיה ציקלית כך או כך

. יותר הרבה יותר אבל אבל  $p^n$  אבל מסדר ציקליות הרחבות שמתאר הרבה יותר כבד.

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

 $L=K_n/K_{n-1}/\cdots/K_0=K$  מגדל מגדל מתפצלת מגדל רדיקלי) נקראת מגדל נקראת מגדל (מגדל רדיקלי) אם היא מגדל נקראת מגדל (מגדל רדיקלי) מגדל נקראת מגדל הדיקלי . עבור ארטין־שרייר שורש  $lpha=\mathscr{P}(a)$  או או $n\in K^{ imes}$  עבור עבור ( $\omega_n=lpha$ ) שורש יחידה שורש עבור  $K_{i+1}=K_i(lpha)$ כך ש

$$\sqrt[\infty]{K} = igcup_{L_i/K}$$
 מגדל הדיקלי מגדל (סגור הדיקלי) אנדרה 42.2 מגדל הדיקלי

 $\sqrt[n]{N}$  וסגור להוצאת שורש והוצאת שורש ארטין־שרייר ממכיל את א ביותר שמכיל את  $\sqrt[n]{N}$  וסגור להוצאת שורש הוא השדה הקטן ביותר הקטן ביותר האכיל

 $L \subseteq \sqrt[\infty]{K}$  אם אביקלית נקראת נקראת נקראת אלגברית אלגברית: הרחבה רדיקלית הרחבה 42.3 הגדרה אלגברית הדיקלית): הרחבה אלגברית

כמובן, אם של כל המגדלים זה הסגור הרדיקלי כך של E/K כך בר על בר הרדיקלי אם הסגור המגדלים זה הסגור הרדיקלי כמובן, אם בר כמובן אם הסגור הרדיקלית אם בר אם הסגור הרדיקלי או הסגור הרדיקלי

.(p וחבורת (גלואה ריבועי אז אגדל ריבועי מגדל מגדל מגדל מגדל אז א $K\subseteq L\subseteq F$  אם אביל יערגיל תרגיל או

חבורת p אז שאם יש לי G בטענה משדות לחבורות) בתרגום להשתמש (בתרגום מגדל ריבועי ובסגור מגדל ריבועי מגדל חבורת אז אז אז איינדקס  $H \leq G$  מאינדקס  $H_1 \subset H_2 \subset \cdots \subset G$  אז שרשרת

18/06 – 11 תרגול 43

43.1 משהו

10 תרגיל 44

טריקים 44.1

44.2 מסקנות