מבנים אלגבריים 2

מבוסס על הרצאותיו של פרופ' שחר מוזס

סמסטר ב' תשס"ח

דינה זליגר

עודכן לאחרונה: 01/08/2008 22:57

תנאי שימוש

Please read the following important legal information before reading or using these notes. The use of these notes constitutes an agreement to abide by the terms and conditions below, just as if you had signed this agreement.

A. THE SERVICE.

The following notes ("The service") are provided by Dina Zil's Notes-Heaven ("Notes-Heaven").

B. DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY.

Notes-Heaven does not endorse content, nor warrant the accuracy, completeness, correctness, timeliness or usefulness of any opinions, advice, content, or services provided by the Service.

YOU AGREE THAT USE OF THE SERVICE IS ENTIRELY AT YOUR OWN RISK. THE SERVICE PROVIDED IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND. NOTES-HEAVEN EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION: ANY WARRANTIES CONCERNING THE ACCURACY OR CONTENT OF INFORMATION OR SERVICES. NOTES-HEAVEN MAKES NO WARRANTY THAT THE SERVICE WILL MEET YOUR REQUIREMENTS, OR THAT THE SERVICE WILL BE ERROR FREE; NOR DOES NOTES-HEAVEN MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE SERVICE OR AS TO THE ACCURACY OR RELIABILITY OF ANY INFORMATION OBTAINED THROUGH THE SERVICE. YOU UNDERSTAND AND AGREE THAT ANY DATA OBTAINED THROUGH THE USE OF THE SERVICE IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR GPA.

NEITHER NOTES-HEAVEN NOR ANY OF ITS PARTNERS, AGENTS, AFFILIATES OR CONTENT PROVIDERS SHALL BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF USE OF THE SERVICE OR INABILITY TO GAIN ACCESS TO OR USE THE SERVICE OR OUT OF ANY BREACH OF ANY WARRANTY.

C. INDEMNIFICATION.

You agree to indemnify and hold Notes-Heaven, its partners, agents, affiliates and content partners harmless from any dispute which may arise from a breach of terms of this Agreement. You agree to hold Notes-Heaven harmless from any claims and expenses, including reasonable attorney's fees and court costs, related to your violation of this Agreement.

D. OWNERSHIP RIGHTS.

The materials provided by the Service may be downloaded or reprinted for personal use only. You acknowledge that the Service contains information that is protected by copyrights, trademarks, trade secrets or other proprietary rights, and that these rights are valid and protected in all forms, media and technologies existing now or hereafter developed. You may not modify, publish, transmit, participate in the transfer or sale, create derivative works, or in any way exploit, any of the Content, in whole or in part. You may not upload, post, reproduce or distribute Content protected by copyright, or other proprietary right, without obtaining permission of the owner of the copyright or other proprietary right.

E. NO COPYING OR DISTRIBUTION.

You may not reproduce, copy or redistribute the design or layout of this service, individual elements of the design, Notes-Heaven logos or other logos appearing on this service, without the express written permission of Notes-Heaven, Inc. Reproduction, copying or redistribution for commercial purposes of the service is strictly prohibited without the express written permission of Notes-Heaven, Inc.

If you have any questions about this statement or the practices of this service you can contact

Dina Zeliger
dinazil @ notes-heaven.com

Draft

תוכן עניינים

תנאי שימוש 1
תוכן עניינים 2
תזכורות 4
חוגי פולינומים 7
הגדרות ותכונות בסיסיות 7
קריטריונים לאי-פריקות 9
תורת השדות 11
התורה הבסיסית של הרחבות של שדות 11
הרחבות אלגבריות 16
בניות בסרגל ובמחוגה 17
שדות פיצול וסגורים אלגבריים 17
הרחבות ספרביליות 17
פולינומים והרחבות ציקלוטומיים 17
תורת גלואה 18
פתרונים של מבחנים 19
תשס"ז – מועד א (פרופ' אהוד דה-שליט) 19
תשס"ז – מועד ב (פרופ' אהוד דה-שליט) 19
תשס"ו – מועד ב' (פרופ' צליל סלע) 19

מבוא

תזכורות

<u>הגדרה</u>: **חוג** הוא קבוצה R עם שתי פעולות דו-מקומיות $+,\cdot: R \times R \to R$ שנקראות חיבור $(+)$ וכפל $(\cdot)$ כך שמתקיימות התכונות הבאות:

- $(R,+)$ חבורה אבלית עם איבר יחידה 0. כלומר, לכל $a,b,c \in R$ מתקיימות התנאים הבאים:
  - אסוציאטיביות: $(a+b)+c = a+(b+c)$
  - איבר יחידה: $0+a = a+0 = a$
  - קומוטטיביות: $a+b = b+a$
  - איבר נגדי: קיים $-a \in R$ כך ש-$a+(-a) = (-a)+a = 0$
- אסוציאטיביות: לכל $a,b,c \in R$ מתקיים $a\cdot(b\cdot c) = (a\cdot b)\cdot c$
- דיסטריביוטיביות: לכל $a,b,c \in R$ מתקיים:
  - $a\cdot(b+c) = a\cdot b + a\cdot c$
  - $(a+b)\cdot c = a\cdot c + b\cdot c$

אם קיים $1 \in R$ כך שלכל $a \in R$ מתקיים $1\cdot a = a\cdot 1 = a$ נאמר ש-1 איבר יחידה ונאמר ש-R **חוג עם יחידה**. אם לכל $a,b \in R$ מתקיים $a\cdot b = b\cdot a$ נאמר ש-R **חוג קומוטטיבי**.

<u>הגדרה</u>: יהי R חוג. קבוצה $I \subseteq R$ נקראת **אידיאל** אם I תת חבורה של $(R,+)$ ואם לכל $r \in R$ ולכל $i \in I$ מתקיים $ri, ir \in I$. במקרה זה מסמנים $I \lhd R$. אם R קומוטטיבי, אידיאל I נקרא **ראשי** אם קיים $a \in R$ כך ש-$I = aR = Ra$. במקרה זה מסמנים $I = (a)$[1]. אם בחוג קומוטטיבי R כל אידיאל הוא ראשי R נקרא **חוג ראשי**. אידיאל נקרא **מקסימלי** אם לכל אידיאל $I \subseteq J \lhd R$ מתקיים $I = J$ או $J = R$.

<u>למה</u>: יהי $\varphi: R \to T$ הומומורפיזם של חוגים ונניח ש-$I \subseteq \ker\varphi$ אידיאל. אזי φ משרה הומומורפיזם של חוגים $\tilde{\varphi}: {}^{R}/_{I} \to T$, $\pi(a) \mapsto \varphi(a)$.

<u>למה</u>: יהי $\varphi: R \to R'$ איזומורפיזם של חוגים. ויהי $I \lhd R$ אידיאל. נסמן $I' = \varphi(I)$. אזי $I' \lhd R'$ ו-φ משרה איזומורפיזם $\tilde{\varphi}: {}^{R}/_{I} \to {}^{R'}/_{I'}$ המוגדר ע"י $\tilde{\varphi}(a+I) = \varphi(a) + I'$.

<u>משפטי האיזומורפיזם</u>:

1. יהיו R,T חוגים ויהי $f: R \to T$ הומומורפיזם. אזי ${}^{R}/_{\ker f} \cong \operatorname{im} f$.
2. יהי R חוג ונניח ש-$A \leq R$ ו-$B \lhd R$. אזי $A+B$ תת חוג של R, $A \cap B$ אידיאל ב-A ו-${}^{(A+B)}/_{B} \cong {}^{A}/_{A\cap B}$.

[1] לכאורה הסימון הזה יכול ליצור בלבול, אבל למעשה תמיד יהיה ברור מההקשר אם מדובר באידיאל או סתם סוגריים...

3. יהי R חוג ויהיו $I \subseteq J$ אידיאלים ב-R. אז $J/I \lhd R/I$ ו-$\left(R/I\right)/\left(J/I\right) \cong R/J$.

<u>הגדרה</u>: נאמר שחוג R הוא **תחום שלמות** אם R חוג קומוטטיבי עם יחידה ואם לכל $a,b \in R$ אם $a \cdot b = 0$ אז $a = 0$ או $b = 0$, כלומר אין ב-R מחלקי אפס.

<u>הגדרה</u>: יהי R תחום שלמות.

א. a נקרא **הפיך** (או **יחידה**) אם קיים $b \in R$ כך ש-$ab = 1$
ב. אם $a,b \in R$ נאמר ש-a **מחלק** את b ונסמן $a|b$ אם קיים $x \in R$ כך ש-$ax = b$.
ג. האיברים ב-R אשר מחלקים את 1 נקראים **יחידות** (אלה בדיוק האיברים ההפיכים ב-R)
ד. אם $a,b \in R$ כך ש-a מחלק את b ו-b מחלק את a נאמר ש-a,b **חברים**. קל לראות שתנאי זה שקול לכך שקיים איבר הפיך $u \in R$ כך ש-$au = b$.
ה. $a \in R$ לא הפיך נקרא **אי-פריק** אם לא ניתן לכתוב אותו כמכפלה של שני איברים לא הפיכים.
ו. $0 \neq a \in R$ לא הפיך נקרא **ראשוני** אם כאשר $a|bc$ בהכרח $a|b$ או $a|c$.

<u>הגדרה</u>: נאמר שחוג R הוא **חוג אוקלידי** אם קיימת פונקציה $d: R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ כך ש-

- לכל $a,b \in R \setminus \{0\}$, $d(a) \leq d(ab)$
- לכל $a,b \in R$ אם $a \neq 0$ אז קיימים $q,r \in R$ כך ש-$b = aq + r$ ואם $r \neq 0$ אז $d(r) < d(a)$ (הפירוק הזה נקרא **חילוק עם שארית**)

<u>טענה</u>: חוג אוקלידי הוא חוג ראשי.

<u>משפט</u>: בחוג אוקלידי איבר הוא אי-פריק אמ"מ הוא ראשוני.

<u>משפט הפריקות היחידה</u>: יהי R חוג אוקלידי ויהי $0 \neq a \in R$ איבר לא הפיך. אז ניתן לכתוב $a = r_1 \dots r_k$ כאשר $r_i \in R$ לכל $1 \leq i \leq k$ איברים אי-פריקים (כלומר ראשוניים). יתר על כן, הצגה זו יחידה עד כדי שינוי סדר ויחסי חברות. כלומר, אם גם $a = t_1 \dots t_m$ אז $k = m$ וקיימת תמורה $\pi \in S_k$ כך שלכל $1 \leq i \leq k$, $r_i = \varepsilon_i t_{\pi(i)}$ כאשר $\varepsilon_i \in R$ הפיך.

<u>הגדרה</u>: יהי R חוג ו-$I \lhd R$ אידיאל. נגדיר יחס שקילות על R באופן הבא: $a \sim b$ אמ"מ $b - a \in I$. אפשר להוכיח בקלות שזה יחס שקילות ושמחלקות השקילות שלו הן מהצורה $[a] = a + I = \{a + i : i \in I\}$. קבוצת כל מחלקות השקילות מסומנת ב-R/I. על קבוצה זו מגדירים חיבור וכפל ע"י

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = ab + I$$

אפשר לראות שפעולות אלה מגדירות על $R/_I$ מבנה של חוג. חוג זה נקרא **חוג המנה**. יחד עם חוג המנה מגיעה **ההטלה הטבעית** $\pi: R \to R/_I$, $a \mapsto \bar{a} = a + I$.

ההטלה הטבעית היא הומומורפיזם ולכן לכל $g(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ מתקיים

$$g(x+I) = g(\pi(x)) = \sum_{i=0}^{n} a_i \pi(x)^i = \sum_{i=0}^{n} a_i \pi(x^i) \overset{1}{=} \pi\left(\sum_{i=0}^{n} a_i x^i\right) = \pi(g(x)) = g(x) + I$$

כאשר (1) נכון בגלל תכונות ההומומורפיזם. נשים לב שיש כאן אי-דיוק קל. מבחינה טכנית, הביטויים $a_i \pi(x^i)$ כלל לא מוגדרים משום ש-$a_i \in R$ ואילו $\pi(x^i) \in R/_I$ ואנחנו לא יכולים לכפול אותם. בכתיב $a_i \pi(x^i)$ הכוונה היא למעשה $\pi(a_i)\pi(x^i)$. כלומר כאשר מציבים בפולינום איבר מחוג המנה מסתכלים גם על המקדמים כאיברים בחוג המנה. ואז מתכונות הומומורפיזם נקבל:

$$g(x+I) = g(\pi(x)) = \sum_{i=0}^{n} \pi(a_i)\pi(x)^i = \sum_{i=0}^{n} \pi(a_i x^i) = \pi\left(\sum_{i=0}^{n} a_i x^i\right) = \pi(g(x)) = g(x) + I$$

<u>משפט</u>: יהי R חוג קומוטטיבי עם יחידה ויהי $I \lhd R$. אזי I מקסימלי אמ"מ $R/_I$ שדה.

<u>משפט</u>: יהי $\varphi: F \to K$ הומומורפיזם של שדות. אזי $\varphi \equiv 0$ או φ חח"ע.

<u>הגדרה</u>: **הפולינומים הסימטריים האלמנטריים** ב-n משתנים $X_1, \dots, X_n$ הם הפולינומים:

$$\begin{aligned}
s_0(X_1, \dots, X_n) &= 1 \\
s_1(X_1, \dots, X_n) &= \sum_{1 \le j \le n} X_j \\
s_2(X_1, \dots, X_n) &= \sum_{1 \le j < k \le n} X_j X_k \\
&\vdots \\
s_n(X_1, \dots, X_n) &= X_1 \cdot \dots \cdot X_n
\end{aligned}$$

חישוב פשוט מראה ש-

$$\prod_{j=1}^{n} (\lambda - X$$

חוגי פולינומים

הגדרות ותכונות בסיסיות

<u>הגדרה</u>: יהי R חוג. **חוג הפולינומים** מעל R, שיסומן ב-$R[X]$, הוא קבוצת איברים מהצורה $p(X) = p_m X^m + \cdots + p_1 X + p_0 = \sum_{i=1}^{m} p_i X^i$. חיבור וכפל מוגדרים באופן הבא:

$$\sum_{i=0}^{m} p_i X^i + \sum_{i=0}^{m} q_i X^i = \sum_{i=1}^{m} (p_i + q_i) X^i$$

$$\left(\sum_{i=0}^{n} p_i X^i\right) \cdot \left(\sum_{i=0}^{m} q_i X^i\right) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} p_i q_j\right) X^k$$

קל לראות שהפעולות האלה אכן מקיימות את אקסיומות החוג. אם $p_m \neq 0$ נאמר שה**דרגה** (או **מעלה**) של p היא m ונסמן $\deg p = m$. נאמר ש-p הוא פולינום **מתוקן** (**monic**) אם $p_n = 1$.

אנחנו תמיד נדברים על חוגים קומוטטיביים ולכן חוג הפולינומים יהיה קומוטטיבי.

<u>משפט</u>: יהי R תחום שלמות. אזי

1. $\deg(pq) = \deg p + \deg q$ עבור פולינומים $p, q \in R[x]$ שאינם אפס.
2. היחידות של $R[x]$ הן בדיוק היחידות של R.
3. $R[x]$ הוא תחום שלמות.

<u>משפט</u>: יהי F שדה. אזי חוג הפולינומים $F[x]$ הוא חוג אוקלידי. בפרט, אם $a, b \in F[x]$ כך ש-$b \neq 0$, אז קיימים $q, r \in F[x]$ יחידים כך ש-$a = qb + r$ ו-$r = 0$ או $\deg r < \deg b$.

<u>מסקנה</u>: בהינתן פולינום $p(X) \in F[X]$ כך ש-$\deg p \geq 1$ (כלומר הוא לא הפיך) ניתן להציגו כמכפלת פולינומים אי-פריקים. אם p פולינום מתוקן אזי ניתן להציגו כמכפלת פולינומים אי-פריקים מתוקנים באופן יחיד עד כדי סדר.

<u>הגדרה</u>: יהי $q(X) = \sum_{i=0}^{m} d_i X^i \in \mathbb{Z}[X]$ ויהי p ראשוני. נסמן $\overline{q[X]} = \sum_{i=0}^{m} \overline{d_i} X^i \in \mathbb{Z}_p[X]$ כאשר $\overline{d_i} \in \mathbb{Z}/p\mathbb{Z}$ תמונת d_i מודולו p. קל להשתכנע שההעתקה $\underset{q(X) \mapsto \overline{q(X)}}{\mathbb{Z}[X] \to \mathbb{Z}_p[X]}$ היא הומומורפיזם של חוגים.

<u>הלמה של גאוס</u>: יהי $f \in \mathbb{Z}[X]$ כך ש-$\deg f \geq 1$. אם f פריק ב-$\mathbb{Q}[X]$ אז הוא פריק ב-$\mathbb{Z}[X]$.

<u>הוכחה</u>: נניח ש-$f = gh$ כאשר $g, h \in \mathbb{Q}[X]$. קיימים $r, s \in \mathbb{N}$ כך ש-$h_1 = sh, g_1 = rg \in \mathbb{Z}[X]$. לכן $rsf = g_1 h_1$. אם $rs = 1$ סיימנו. אחרת, יהי p ראשוני כך ש-$p|rs$. נתבונן בשוויון $rsf = g_1 h_1$

מודולו p ונקבל את השוויון $\overline{rsf} = \overline{g_1}\overline{h_1} = \overline{g_1}\overline{h_1}$. אבל $p|rs$ ולכן $0 = \overline{rsf} = \overline{g_1}\overline{h_1}$. אבל החוג $\mathbb{Z}_p[X]$ הוא תחום שלמות ובפרט אין בו מחלקי אפס. לכן, $\overline{g_1} = 0$ או $\overline{h_1} = 0$ (בשוויונים בחוג הפולינומים מודולו p). נניח בה"כ ש-$\overline{g_1} = 0$. פירוש הדבר שכל המקדמים של g_1 מתחלקים ב-p. כלומר, קיים פולינום $g_2 \in \mathbb{Z}[X]$ כך ש-$g_1 = pg_2$. לכן $\frac{rs}{p} f = g_2 h_1$. אם $\frac{rs}{p} = 1$ סיימנו כי מצאנו פירוק של f ב-$\mathbb{Z}[X]$. אחרת, יש ראשוני שמחלק את $\frac{rs}{p}$. כך ניתן לחזור על התהליך עד שנקבל פירוק $f = g_k h_k$. התהליך בהכרח ייגמר משום שהפירוק של rs לראשוניים הוא סופי ובכל שלב המקדם של f במשוואה $af = g_j h_j$ קטן ממש.

☺

<u>טענה</u>: קיים אלגוריתם אשר בהינתן פולינום $f \in \mathbb{Q}[x]$ מוצא פירוק שלו לגורמים אי-פריקים.

<u>הוכחה</u>: נטען שאפשר להניח ש-f פולינום מתוקן במקדמים שלמים. אחרת, אפשר בוודאי לכפול את f במספר רציונלי ולקבל פולינום מתוקן. כעת, יהי D המכנה המשותף המינימלי של כל המכנים של המקדמים של f. אז $D^{\deg f} f\left(\frac{x}{D}\right)$ הוא פולינום מתוקן במקדמים שלמים ופירוק שלו נותן פירוק של הפולינום המקורי.

<u>לדוגמה</u>:

נניח שרוצים לפרק את $\frac{2}{3}x^4 - \frac{2}{3}x^3 + \frac{19}{24}x^2 - \frac{2}{3}x + \frac{1}{8}$. נכפול אותו ב-$\frac{3}{2}$ כדי לקבל את הפולינום המתוקן $x^4 - x^3 + \frac{19}{16}x^2 - x - \frac{3}{16}$. המכנה המשותף המינימלי של המכנים הוא 16 ודרגת הפולינום היא 4. אז נסתכל ב-

$$16^4\left(\left(\frac{x}{16}\right)^4 - \left(\frac{x}{16}\right)^3 + \frac{19}{16}\cdot\left(\frac{x}{16}\right)^2 - \frac{x}{16} - \frac{3}{16}\right) =$$
$$= x^4 - 16x + 16\cdot 19x^2 - 16^3x - 3\cdot 16^3$$

זהו פולינום מתוקן בשלמים והפירוק שלו הוא $(x^2+256)(x-4)(x-12)$. ע"י חלוקה ב-16^4, הצבת $16x$ במקום x וחלוקה ב-$\frac{3}{2}$ נקבל פירוק של הפולינום המקורי:

$$\frac{2}{3}\cdot\frac{1}{16^4}((16x)^2+256)(16x-4)(16x-12) =$$
$$= \left(\frac{x^2}{384} + \frac{1}{384}\right)\left(\frac{x}{6144} - \frac{1}{8192}\right)\left(\frac{x}{6144} - \frac{3}{8192}\right) =$$
$$= \frac{2}{3}x^4 - \frac{2}{3}x^3 + \frac{19}{24}x^2 - \frac{2}{3}x + \frac{1}{8}$$

אז נניח כעת ש-f פולינום במקדמים שלמים. בוודאי אפשר גם להניח ש-$\deg f \geq 1$. אחרת, הטענה טריוויאלית. מספיק להראות שקיים חסם M שניתן לחישוב בזמן סופי כך שאם $g(x) = \sum_{i=0}^{n} h_i x^i \in \mathbb{Z}[x]$ מחלק את f אז $|h_i| < M$ לכל $0 \leq i \leq n$. אם כך, אפשר פשוט לחפש באופן שיטתי את כל המחלקים של f.

נסמן את המקדמים של f ב-$a_0, \dots, a_{m-1}$. מהמשפט היסודי של האלגברה אפשר לכתוב את f כמכפלת גורמים לינאריים מרוכבים: $f(x) = \prod_{i=1}^{m}(x - \alpha_i)$ כאשר $\alpha_i \in \mathbb{C}$. ראשית, נטען שכל

שורש של f מקיים $|\alpha_i| \le \max(1, mB)$ כאשר $B = \max_{0\le i\le m-1}|a_i|$. ואכן, אם $|\alpha| > \max(1, mB)$ נראה ש-$f(\alpha) \ne 0$ ובפרט אינו שורש:

$$\left|\frac{f(\alpha)}{\alpha^{m-1}}\right| = \left|\frac{\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0}{\alpha^{m-1}}\right| = \left|\alpha + a_{m-1} + \frac{a_{m-2}}{\alpha} + \cdots + \frac{a_1}{\alpha^m} + \frac{a_0}{\alpha^{m-1}}\right|$$
$$\overset{1}{\ge} \left||\alpha| - \left|a_{m-1} + \frac{a_{m-2}}{\alpha} + \cdots + \frac{a_1}{\alpha^m} + \frac{a_0}{\alpha^{m-1}}\right|\right| \overset{2}{\ge} |\alpha| - \left|a_{m-1} + \frac{a_{m-2}}{\alpha} + \cdots + \frac{a_1}{\alpha^m} + \frac{a_0}{\alpha^{m-1}}\right|$$
$$\overset{3}{\ge} |\alpha| - \sum_{i=0}^{m-1}\left|\frac{a_i}{\alpha^{m-i-1}}\right| \overset{4}{\ge} |\alpha| - \sum_{i=0}^{m-1}|a_i| \overset{5}{\ge} |\alpha| - mB \overset{6}{>} 0$$

כאשר:

- (1) נכון מאי שוויון המשולש $\big||x| - |y|\big| \le |x + y|$
- (2) נכון כי תמיד $x \le |x|$
- (3) נכון מאי שוויון המשולש $|x + y| \le |x| + |y|$
- (4) נכון כי $|\alpha| > \max(1, mB) \ge 1$
- (5) נכון $B = \max_{1\le j\le m-1}|a_j| \ge a_i$
- (6) נכון כי $|\alpha| > \max(1, mB) \ge mB$

לכן $|f(\alpha)| > |\alpha^{m-1}| > 1$. בפרט, $f(\alpha) \ne 0$ ולכן לא יכול להיות שורש. מכאן שבהינתן פולינום $f \in \mathbb{Z}[x]$ אפשר למצוא בזמן סופי חסם על גדלי השורשים המרוכבים שלו.

נניח כעת שיש פירוק $f = gh$ כאשר $g(x) = \prod_{i\in I}(x - \alpha_i)$ ו-$h(x) = \prod_{i\notin I}(x - \alpha_i)$ עבור $I \subsetneq \{1, \dots, m\}$. מאחר שאפשר לשנות את סדר השורשים אפשר להניח בה"כ ש-$g(x) = \prod_{i=0}^{r}(x - \alpha_i) = x^r + c_{r-1}x^{r-1} + \cdots + c_1x + c_0$. אז מתקיים $c_k = s_k(\alpha_1, \dots, \alpha_r)$ הפולינום הסימטרי האלמנטרי ה-k ב-r משתנים. אבל הפולינומים הסימטרי האלמנטרי הם פונקציות קבועות וידועות ולכן בהינתן חסם על הגדלים של $\{\alpha_i\}_{i=0}^{r}$ אפשר לחשב חסם על c_k לכל $0 \le k \le r$. ומאחר שאנחנו מעוניינים רק במקדמים שלמים, פירוש הדבר שיש רק מספר סופי של מועמדים לבדוק וסיימנו.

☺

קריטריונים לאי-פריקות

<u>קריטריון איזנשטיין</u>: יהי $f(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{Z}[x]$ ונניח שקיים ראשוני p כך ש-

1. $p \nmid a_m$
2. $p|a_i$ לכל $0 \le i < m$
3. $p^2 \nmid a_0$

אזי f אי-פריק.

<u>הוכחה</u>: נניח בשלילה $f = gh$ כאשר $g, h \in \mathbb{Z}[X]$. נתבונן בשוויון זה מודולו p, $\bar{f} = \bar{g}\bar{h}$. אבל $p|a_i$ לכל $0 \le i < m$ ולכן $\overline{f(x)} = \overline{a_m}x^m$ ומאחר ש-$p \nmid a_m$ נובע ש-$\overline{a_m} \ne 0$. לכן בהכרח $\overline{g(x)} = \overline{c_k}x^k$ ו-$\overline{h(x)} = \overline{d_{m-k}}x^{m-k}$ כאשר $\overline{a_m} = \overline{c_k}\,\overline{d_{m-k}}$. לכן,

$$g(x) = c_kx^k + c_{k-1}x^{k-1} + \cdots + c_1x + c_0$$
$$h(x) = d_{m-k}x^{m-k} + d_{m-k-1}x^{m-k-1} + \cdots + d_1x + d_0$$

כאשר $p|c_i$ ל-$0 \le i \le k-1$ ו-$p|d_i$ ל-$0 \le i \le m-k-1$. בפרט, $p|c_0$ ו-$p|d_0$. אבל $f = gh$ ולכן $a_0 = c_0 d_0$. אבל אז $p^2|a_0$ בסתירה להנחה.

☺

טיוטה

תורת השדות

התורה הבסיסית של הרחבות של שדות

<u>למה</u>: יהי F שדה. אזי $I \lhd F[x]$ הוא אידיאל מקסימלי אמ"מ $I = (f)$ עבור פולינום אי-פריק $f \in F[x]$.

<u>הוכחה</u>:

($\Leftarrow$) נניח ש-I מקסימלי. $F[x]$ חוג וקלידי ולכן תחום ראשי. לכן קיים פולינום $f \in F[x]$ כך ש-$I = (f)$. נראה שהוא אי-פריק. נניח בשלילה ש-$f = gh$ פירוק של f. אזי נטען ש-$(f) \subsetneq (g) \subsetneq F[x]$. ראשית, אם $qf \in (f)$ אז $qf = q(gh) = (qh)g \in (g)$. לכן $(f) \subseteq (g) \subseteq F[x]$. נראה שאין שוויונים. אילו היה מתקיים $(f) = (g)$ אז $g \in (f)$, כלומר קיים $q \in F[x]$ כך ש-$g = qf = q(gh) = g(qh)$. מאחר ש-$F[x]$ תחום שלמות נובע ש-$qh = 1$. אבל זה בהכרח גורר ש-$q = h = \pm 1$ וזה בסתירה לכך שהנחנו ש-$f = gh$ פירוק של f. ברור גם ש-$1 \notin (g)$ ולכן $(g) \neq F[x]$. לכן $(f) \subsetneq (g) \subsetneq F[x]$. אבל זו סתירה למקסימליות של $I = (f)$. לכן f אי-פריק.

($\Rightarrow$) נניח ש-f אי-פריק ונניח בשלילה ש-$(f) \subsetneq J \subsetneq F[x]$. קיים $g \in F[x]$ כך ש-$J = (g)$. אבל אז $f \in (g)$, כלומר קיים $h \in F[x]$ כך ש-$f = gh$. אבל בהכרח $\deg g \geq 1$ ובגלל ש-f אי פריק נובע ש-$h \in F$. אבל אז $(f) = (g)$ בסתירה.

☺

<u>מסקנה</u>: יהי F שדה ויהי $f \in F[x]$ פולינום אי-פריק. אזי $F[x]/(f)$ שדה שמכיל את F ומכיל שורש של f.

<u>הוכחה</u>: מהלמה נובע באופן ישיר ש-$F[x]/(f)$ שדה. שדה זה מכיל את F במובן של שיכון.

נגדיר $\varphi: F \to F[x]/(f)$ ע"י $\varphi(a) = a + (f)$. זהו למעשה צמצום של ההטלה הטבעית $\pi: F[x] \to F[x]/(f)$ ל-F. מאחר שמדובר בהומומורפיזם של שדות שהוא כמובן אינו טריוויאלי (למשל $\varphi(1) = 1 + I = 1_{F[x]/(f)} \neq 0_{F[x]/(f)}$) נובע שההטלה היא חח"ע ולכן $F \hookrightarrow F[x]/(f)$ שיכון.

נראה שיש ל-f שורש. נטען ש-$\bar{x}$ הוא שורש של f. נניח ש-$f(x) = \sum_{i=0}^{n} a_i x^i$. אז $f(\bar{x}) = f(x) + I = I = 0_{F[x]/(f)}$ וזה מה שרצינו.

☺

<u>מסקנה</u>: יהי F שדה ויהי $p \in F[x]$ פולינום ממעלה לכל הפחות 1. אזי קיים שדה $F \subseteq E$ וקיים $\alpha \in E$ כך ש-$p(\alpha) = 0$.

הוכחה: יהי $f \in F[x]$ גורם אי-פריק של p. לפי המשפט הקודם קיים שדה שמכיל את E ובו שורש של f. אבל שורש של f הוא בוודאי שורש של p ולכן סיימנו.

☺

נניח שבמשפט כבר היה שורש של p ב-F, כלומר $p(x) = (x-\alpha)q(x)$ עבור $\alpha \in F$ ו-$q \in F[x]$. אז הגורם האי-פריק שאנחנו מסתכלים עליו הוא $x-\alpha$. במקרה זה נטען ש-$F \cong {F[x]}/{(x-\alpha)}$

(אז למעשה לא הגדלנו את השדה שלא לצורך). אכן, נתבונן בצמצום של הטלה הטבעית:

$$\varphi: F \to {F[x]}/{(x-\alpha)}$$

$$a \mapsto a+(x-\alpha)$$

כבר ראינו בהוכחה שזה הומומורפיזם חח"ע. אם נראה שהוא על נקבל על הדרוש. נניח ש-$h(x)+(x-\alpha) \in {F[x]}/{(x-\alpha)}$. אפשר לחלק עם שארית ולקבל $h(x) = q(x)(x-\alpha)+r(x)$.

אם $r(x)=0$ אז $h \in (x-\alpha)$ ולכן $\varphi(0) = 0+(x-\alpha) = h(x)+(x-\alpha)$. אם $r(x) \neq 0$ אז $\deg r < \deg(x-\alpha) = 1$ ולכן $r \in F$. לכן $\varphi(r) = r+(x-\alpha) = h(x)+(x-\alpha)$. בכל מקרה מצאנו מקור ל-$h(x)$ ולכן ההעתקה היא גם על ולכן $F \cong {F[x]}/{(x-\alpha)}$ ואכן לא הגדלנו את

השדה שלא לצורך.

טענה: יהי F שדה ויהי $p \in F[x]$. אזי $\alpha \in F$ שורש של p אמ"מ $(x-\alpha)|p(x)$.

הוכחה:

($\Leftarrow$) נחלק את $p(x)$ עם שארית ב-$x-\alpha$. נניח ש-$p(x) = (x-\alpha)q(x)+r(x)$. נציב $x=\alpha$ ונקבל $0 = p(\alpha) = (\alpha-\alpha)q(\alpha)+r(\alpha) = r(\alpha)$. אבל או ש-$r(x)=0$ או ש-$\deg r < \deg(x-\alpha) = 1$. בכל מקרה $r(x) \in F$ ולכן $r(x) = r(\alpha) = 0$. לכן $p(x) = (x-\alpha)q(x)$. כלומר, $(x-\alpha)|p(x)$.

($\Rightarrow$) אם $(x-\alpha)|p(x)$ אז $p(x) = (x-\alpha)q(x)$ וכמובן $p(\alpha) = (\alpha-\alpha)q(\alpha) = 0$.

☺

מסקנה: יהי F שדה ויהי $p \in F[x]$ פולינום ממעלה n. אזי יש ל-p לכל היותר n שורשים ב-F.

הוכחה: באינדוקציה על מעלת הפולינום. אם $n=1$ אז $p(x) = x-\alpha$ וכמובן יש בדיוק שורש אחד. נניח ל-n ונוכיח ל-$n+1$. יהי $p \in F[x]$ מדרגה $n+1$. אם אין לו שורשים אז סיימנו. אחרת, יהי $\alpha \in F$ שורש של p. אזי לפי הטענה הקודמת $p(x) = (x-\alpha)q(x)$ עבור $q \in F[x]$ בוודאי $\deg q = n$. לפי הנחת האינדוקציה ל-q יש לכל היותר n שורשים ב-F. ויחד עם α יש ל-p לכל היותר $n+1$ שורשים ב-F.

☺

<u>מסקנה</u>: יהי F שדה ויהי $p \in F[x]$ כך ש-$\deg p \geq 1$. נסמן $p(x) = \sum_{i=0}^{n} a_i x^i$. אזי קיים שדה $F \subseteq L$ כך שב-$L[x]$ מתקיים $p(x) = c\prod_{i=1}^{n}(x - \alpha_i)$.

<u>הוכחה</u>[2]: באינדוקציה שלמה על הדרגה של הפולינום. אם $n = 1$ הטענה טריוויאלית. נניח שלכל שדה K ולכל פולינום מעל השדה הזה מדרגה לכל היותר n יש שדה שמכיל את K ובו הפולינום מתפרק לגורמים לינאריים. נוכיח שהטענה נכונה ל-$n + 1$.

נניח ש-f פולינום מדרגה $n + 1$. נכתוב את f כמכפלה של גורמים אי-פריקים: $f = \prod_{i=1}^{m} f_i$. בה"כ יש לפחות שני גורמים. אחרת, לפי הטענה הקודמת אפשר להסתכל בשדה גדול יותר שמכיל שורש של f ושם כמובן יש פירוק לשני גורמים לפחות. מתקיים $\deg f_i \geq 1$. אם כולם לינאריים אז סיימנו. אחרת, נניח בה"כ ש-f_1 אינו לינארי. אז כמובן $\deg f_1 \leq n$. לכן אפשר להשתמש בהנחת האינדוקציה על f_1. יש שדה $F \subseteq E_1$ שבו f_1 מתפרק לגורמים לינאריים. אבל מאחר ש-$F \subseteq E_1$ מתקיים $\prod_{i=2}^{m} f_i \in E_1[x]$ וגם עבורו אפשר להשתמש בהנחת האינדוקציה, שהרי $\deg(\prod_{i=2}^{m} f_i) \leq n$: יש שדה $E_1 \subseteq L$ שבו הפולינום מתפרק לגורמים לינאריים. עכשיו $F \subseteq E_1 \subseteq L$ ו-f_1 מתפרק לגורמים לינאריים ב-E_1 ולכן בוודאי מתפרק לגורמים לינאריים ב-L ו-$\prod_{i=2}^{m} f_i$ מתפרק לגורמם לינאריים ב-L. לכן המכפלה $f = \prod_{i=1}^{m} f_i$ מתפרקת לגורמים לינאריים ב-L וסיימנו.

☺

<u>הגדרה</u>: יהי F שדה. שדה E שמכיל את F נקרא **שדה הרחבה** של F. בהרבה מקרים נסמן את ההרחבה ב-E/F. עבור פולינום $f \in F[x]$ מדרגה לכל הפחות 1, נאמר ש-f **מתפצל** ב-E אם אפשר לכתוב $f(x) = c\prod_{i=1}^{n}(x - a_i)$ ב-$E[x]$. במקרה זה, נאמר ש-E **שדה פיצול** של f. E נקרא **שדה הפיצול** של f אם הוא שדה מינימלי (מבחינת הכלה) שבו f מתפצל.

תחת הגדרות אלה, המסקנה למעשה אומרת שבהינתן פולינום $f \in F[x]$ קיים לו שדה פיצול.

<u>הגדרה</u>: יהי F שדה ותהיינה שתי הרחבות $F \subseteq E, E'$. F-הומומורפיזם הוא הומומורפיזם $\varphi: E \to E'$ כך ש-$\varphi|_F = id|_F$. כלומר $\varphi(a) = a$ לכל $a \in F$.

<u>הגדרה</u>: יהי F שדה ותהי K הרחבה שלו. יהיו $\alpha_1, \dots, \alpha_n \in K$. התת שדה המינימלי של K שמכיל את F ואת $\alpha_1, \dots, \alpha_n$ נקרא **תת השדה הנוצר** (**סופית**) ע"י $\alpha_1, \dots, \alpha_n$ מעל F ומסומן ב-$F(\alpha_1, \dots, \alpha_n)$. למעשה, מתקיים:

$$F(\alpha_1, \dots, \alpha_n) = \bigcap_{\substack{F \subseteq E \subseteq K \\ \alpha_1, \dots, \alpha_n \in E}} E$$

<u>למה</u>: יהי F שדה ויהי $g \in F[x]$ פולינום אי-פריק. נניח ש-$F \subseteq L$ שדה כך שקיים $\alpha \in L$ כך ש-$g(\alpha) = 0$ וכך ש-$L = F(\alpha)$. אזי קיים F-איזומורפיזם בין L ל-$F[x]/(g)$ שמעביר את α ל-$\bar{x} = x + (g)$.

---

[2] זאת לא בדיוק ההוכחה שניתנה בכיתה.

הוכחה: נגדיר הומומורפיזם של חוגים $\varphi: F[x] \to F(\alpha)$ ע"י $\varphi(x) = \alpha$ ו-$\varphi(c) = c$ לכל $c \in F$. ברור שהגדרה זו מגדירה הומומורפיזם יחיד. למעשה $\varphi\left(\sum_{i=0}^{n} c_i x^i\right) = \sum_{i=0}^{n} c_i \alpha^i$ ומעצם ההגדרה רואים שזה הומומורפיזם. נטען ש-$(g) \subseteq \ker\varphi$. ואכן, נניח ש-$gh \in (g)$. אז $\varphi(gh) = \varphi(g)\varphi(h) = g(\alpha)h(\alpha) = 0$, שהרי $g(\alpha) = 0$. לכן φ משרה הומומורפיזם של חוגים $\tilde{\varphi}: {F[x]}/{(g)} \to F(\alpha)$. אבל

g אי-פריק ולכן ${F[x]}/{(g)}$ שדה. אז $\tilde{\varphi}$ הומומורפיזם של שדות. ברור שהוא אינו טריוויאלי משום

שלכל $a \in F$ מתקיים $\tilde{\varphi}(a + (g)) = \varphi(a) = a$ (אז $\tilde{\varphi}$ למעשה F-הומומורפיזם). לכן בהכרח $\tilde{\varphi}$ חח"ע ולכן הוא על תמונתו. אבל התמונה היא שדה והיא כמובן מכילה את α כי $\tilde{\varphi}(x + (g)) = \varphi(x) = \alpha$ ואת F. לכן לפי הגדרת $F(\alpha)$ נובע שהתמונה מכילה את $F(\alpha)$ ולכן שווה לו. לכן קיבלנו F-איזומורפיזם $\tilde{\varphi}: {F[x]}/{(g)} \to F(\alpha)$. כך ש-$\tilde{\varphi}(x + (g)) = \alpha$ וזה מה שרצינו.

☺

מסקנה: יהי F שדה ויהי $g \in F[x]$ אי פריק כך ש-$\deg g \geq 1$. נניח ש-$L = F(\alpha)$ ו-$L' = F(\beta)$ כך ש-$g(\alpha) = 0 = g(\beta)$. אזי יש F-איזומורפיזם $\psi: L \to L'$ כך ש-$\psi(\alpha) = \beta$.

הוכחה: לפי המשפט הקודם יש F-איזומורפיזם $\varphi_1: L \to {F[x]}/{(g)}$ כך ש-$\varphi_1(\alpha) = \bar{x}$ ויש F-

איזומורפיזם $\varphi_2: {F[x]}/{(g)} \to L'$ כך ש-$\varphi(\bar{x}) = \beta$. ההרכבה $\psi = \varphi_2 \circ \varphi_1: L \to L'$ נותנת את

הדרוש.

☺

משפט: יהיו L, L' שדות ו-$\sigma: L \to L'$ איזומורפיזם. σ משרה איזומורפיזם $\sigma: L[x] \to L'[x]$, $f \mapsto f'$. יהי $f \in L[x]$. נניח ש-$L \subseteq E$ שדה פיצול מינימלי עבור f ו-$L' \subseteq E'$ שדה פיצול מינימלי עבור f'. אזי קיים איזומורפיזם $\varphi: E \to E'$ כך ש-$\varphi|_L = \sigma$.

הוכחה: נוכיח באינדוקציה על הדרגה של f. אם $\deg f = 1$ אז $E = L, E' = L'$ ואם ניקח $\varphi = \sigma$ נקבל את הדרוש. נניח כעת שהטענה מתקיימת עבור פולינומים ממעלה קטנה מזו של f. נכתוב את f כמכפלה של גורמים אי-פריקים: $f = f_1 \dots f_m$. יהי $\alpha_1 \in E$ שורש של f_1 (קיים כזה כי E הוא שדה פיצול של f). נתבונן ב-$f_1' = \sigma(f_1) \in L'[x]$. יהי $\beta_1 \in E'$ שורש של f_1'. קיים איזומורפיזם $\psi: L(\alpha_1) \to L'(\beta_1)$, שהרי לפי המשפט הקודם יש איזומורפיזמים $L(\alpha_1) \cong {L[x]}/{(f_1)}$

ו-$L'(\beta_1) \cong {L'[x]}/{(f_1')}$. אבל $\sigma: L \to L'$ איזומורפיזם ו-$f_1' = f_1$ ולכן $(f_1) = (f_1')$ ומכאן שלפי טענה

מהתזכורת יש איזומורפיזם $L'(\beta_1) \to L'[x]/(f_1') \to L[x]/(f_1) \to L(\alpha_1)$ ψ[3] כך שמתקיים $\psi: a \mapsto a + (f_1) \mapsto \sigma(a) + (f_1') \mapsto \sigma(a)$ לכל $a \in L$, ז"א $\psi|_L = \sigma$. נסמן $M = L(\alpha_1)$ ו-$M' = L'(\beta_1)$. יהיו $g \in M[x]$ ו-$g' \in M'[x]$ כך ש-$f(x) = (x - \alpha_1)g(x)$ ו-$f'(x) = (x - \beta_1)g'(x)$. נשים לב שמתקיים $g' = \psi(g)$. כמו כן, $M \subseteq E$ הוא שדה פיצול מינימלי של g ו-$M' \subseteq E'$ הוא שדה פיצול מינימלי של g': למשל, ברור ש-E שדה פיצול של g, שהרי הוא שדה פיצול של $f(x) = (x - \alpha_1)g(x)$. נניח שהוא לא המינימלי וששדה הפיצול המינימלי הוא $K \subsetneq E$. אבל $M = L(\alpha_1)$ שדה פיצול של $x - \alpha_1$ ולכן $M \cap K \subsetneq E$ שדה פיצול של f, בסתירה למינימליות של E. אבל עכשיו אפשר להשתמש בהנחת האינדוקציה, שהרי $\deg g = \deg f - 1 < \deg f$, M, M' שדות ויש איזומורפיזם $\psi: M \to M'$ ו-E, E' הם שדות פיצול מינימליים של g, g' בהתאמה. לכן יש איזומורפיזם $\varphi: E \to E'$ כך ש-$\varphi|_M = \psi$. אבל $L \subseteq M$ ולכן $\varphi|_L = (\varphi|_m)|_L = \psi|_L = \sigma$.

☺

<u>מסקנה</u>: יהי F שדה ויהי $f \in F[x]$. יהיו $F \subseteq E, E'$ שדות פיצול מינימליים של f. אזי E ו-E' F-איזומורפיים. בפרט, שדה הפיצול של פולינום יחיד עד כדי איזומורפיזם ולכן המונח שדה הפיצול מוגדר היטב.

<u>הוכחה</u>: בסימונים של ההוכחה הקודמת, נתבונן ב-$L = L' = F$ ו- $\sigma = \mathrm{id}$. אזי $f = f'$ ו-E שדה פיצול מינימלי של f ו-E' שדה פיצול מינימלי של f'. לכן קיים איזומורפיזם $\varphi: E \to E'$ כך ש-$\varphi|_F = \mathrm{id}$. אבל זה בדיוק אומר ש-φ הוא F-איזומורפיזם.

☺

<u>הגדרה</u>: תהי E/F הרחבת שות. אזי אפשר לחשוב על E כמרחב וקטורי מעל F. ההרחבה נקראת **הרחבה סופית** אם E מרחב וקטורי מממד סופי מעל F. במקרה זה נקרא לממד **דרגת ההרחבה** ונסמן $[E:F] = \dim_F E$.

<u>משפט</u>: יהיו $F \subseteq L \subseteq E$ שדות כך שההרחבות E/L ו-L/F סופיות. אזי $[E:F] = [E:L][L:F]$.

<u>הוכחה</u>: נניח ש-$[E:L] = n$ ו-$[L:F] = m$. יהיו $\{\alpha_1, \dots, \alpha_n\}$ ו-$\{\beta_1, \dots, \beta_m\}$ בסיסים של E/L ושל L/F בהתאמה. כדי להוכיח את הטענה מספיק להראות שהאוסף $\Omega = \{\alpha_i \beta_j\}_{\substack{1 \le i \le n \\ 1 \le j \le m}}$ הוא בסיס של E/F ושהוא מכיל nm איברים.

ברור ש-$E = \mathrm{span}_F\, \Omega$. בהינתן $\varepsilon \in E$ קיימים $a_1, \dots, a_n \in L$ כך ש-$\varepsilon = \sum_{i=1}^n a_i \alpha_i$, שהרי $\{\alpha_1, \dots, \alpha_n\}$ בסיס של E מעל L. אבל $\{\beta_1, \dots, \beta_m\}$ בסיס של L מעל F ולכן לכל $1 \le i \le n$ קיימם $b_{i,1}, \dots, b_{i,m} \in F$ כך ש-$a_i = \sum_{j=1}^m b_{i,j} \beta_j$. סה"כ נקבל ש-$\varepsilon = \sum_{i=1}^n a_i \alpha_i = \sum_{i=1}^n \left(\sum_{j=1}^m b_{i,j} \beta_j\right) \alpha_i = \sum_{i=1}^n \left(\sum_{j=1}^m b_{i,j} \beta_j\, \alpha_i\right)$, כלומר $\varepsilon \in \mathrm{span}_E\, \Omega$.

כעת, נניח שיש צירוף לינארי $\sum_{i=1}^n \left(\sum_{j=1}^m b_{i,j} \beta_j\, \alpha_i\right) = 0$. אבל אז $\sum_{i=1}^n \left(\sum_{j=1}^m b_{i,j} \beta_j\right) \alpha_i = \sum_{i=1}^n \left(\sum_{j=1}^m b_{i,j} \beta_j\, \alpha_i\right)$. כלומר קיבלנו צירוף לינארי של $\{\alpha_1, \dots, \alpha_n\}$ שמתאפס. אבל זה בסיס ולכן

---

[3] יהי $\varphi: R \to R'$ איזומורפיזם של חוגים. ויהי $I \lhd R$ אידיאל. נסמן $I' = \varphi(I)$. אזי $I' \lhd R'$ ו-φ משרה איזומורפיזם $\tilde{\varphi}: R/I \to R'/I'$ המוגדר ע"י $\tilde{\varphi}(a + I) = \varphi(a) + I'$.

$\sum_{j=1}^{m} b_{i,j}\beta_j = 0$ לכל $1 \le i \le n$. אבל אלה צירופים לינאריים של איברי הבסיס $\{\beta_1, \dots, \beta_m\}$ ולכן $b_{i,j} = 0$ לכל $1 \le j \le m$ ולכל $1 \le i \le n$. מכן שבהכרח האוסף Ω הוא בת"ל, בפרט כל האיברים בהכרח שונים. לכן $|\Omega| = nm$ וסיימנו.

☺

הרחבות אלגבריות

<u>הגדרה</u>: תהי $F \subseteq E$ הרחבת שדות. איבר $\alpha \in E$ ייקרא **אלגברי** מעל F אם קיים פולינום $0 \neq f \in F[x]$ כך ש-$f(\alpha) = 0$. אם $\alpha \in E$ אינו אלגברי הוא ייקרא **טרנסצנדנטי**. ההרחבה E/F תיקרא **הרחבה אלגברית** אם כל $\alpha \in E$ הוא אלגברי מעל F.

<u>למה</u>: תהי E/F הרחבת שדות ונניח ש-$\alpha \in E$ אלגברי מעל F. אזי $F(\alpha) = F[\alpha]$.

<u>משפט</u>: הרחבה E/F היא סופית אמ"מ היא אלגברית ונוצרת סופית.

<u>הוכחה</u>:

($\Leftarrow$) נניח שההרחבה E/F סופית ו-$[E:F] = n$. יהי $\alpha \in E$. נתבונן בקבוצה $\{1, \alpha, \alpha^2, \dots, \alpha^n\} \subseteq E$. אלה $n+1$ וקטורים במרחב n-ממדי. לכן קיימת ביניהם תלות לינארית לא טריוויאלית מעל F:

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$$

נסמן $f(x) = \sum_{i=0}^{n} a_i x^i$. זה לא פולינום האפס משום שהתלות אינה טריוויאלית ו-$f \in F[x]$ משום שהתלות היא מעל F. מתקיים $f(\alpha) = 0$ ולכן α אלגברי מעל F. נותר להוכיח שההרחבה היא נוצרת סופית, אבל זה ברור. מאחר שההרחבה סופית יש בסיס $\{\beta_1, \dots, \beta_n\}$ ל-E מעל F. ברור שמתקיים $E = F(\beta_1, \dots, \beta_n)$ וזוהי הרחבה נוצרת סופית.

($\Rightarrow$) נניח כעת שההרחבה אלגברית ונוצרת סופית. אז קיימים $\alpha_1, \dots, \alpha_k \in E$ כך ש-$E = F(\alpha_1, \dots, \alpha_k)$.

בניות בסרגל ובמחוגה

שדות פיצול וסגורים אלגבריים

הרחבות ספרביליות

פולינומים והרחבות ציקלוטומיים

טיוטה

תורת גלואה

טיוטה

פתרונים של מבחנים

תשס"ז – מועד א (פרופ' אהוד דה-שליט)

חלק א

חלק ב

חלק ג

תשס"ז – מועד ב (פרופ' אהוד דה-שליט)

חלק א

<u>שאלה 1</u>

א. הגדירו: שדה פיצול של $f(x)$.

יהי F שדה. עבור פולינום $f \in F[x]$ מדרגה לכל הפחות 1, נאמר ש-f **מתפצל** ב-E אם אפשר לכתוב $f(x) = c\prod_{i=1}^{n}(x - a_i)$ ב-$E[x]$. במקרה זה, נאמר ש-E **שדה פיצול** של f.

ב. יהי

חלק ב

חלק ג

תשס"ו – מועד ב' (פרופ' צליל סלע)

חלק I

חלק II