

מתרגל חזרי שטיינר

מסגרת אלמנטים ב-2 תרכאל מס 1

ushapira@math.huji.ac.il

היום ששור שא לא כז קטור אקוס, אא סקוולטיונים

שטת קטלה: יום א' 17-18
התנהגה סליון

קוולטיונים

ניתן ל- \mathbb{R}^4 מסנה של חוז, לאטר נא-דר סולת כסל

(כסום כמיוסן סורטל מת הווקטור $(a,b,c,d) \in \mathbb{R}^4$

} כמיוסן הנה

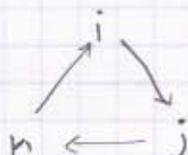
$$a+bi+cj+dk$$

הכפול (הכין חק) חכסל קוולטיונים (סדר $i^2 = j^2 = k^2 = -1$

$$ij = k$$

$$jk = i$$

$$ki = j$$



$$-i = ij^2 = kj$$

$$-j = ik$$

$$-k = ji$$

כמה כהנסק שכאטת \mathbb{R}^4 נוקטל מסנה של חוז וחת כסולת הנהל רכזת

אסטן מת רחוס הנה ה- H .

כסל אחסס טרו הנוכס של H .

הנוכס של $H = H$ אולל כל החסרים ה- H שמתחלסים (כסל) עם כל חסר H .

סענה: $\mathbb{R} = H$ (כד שאסור יהיה טטנוכ טסטין שהוא יתחלל עם שטל טטין i, j, k)

הווחה: מוכסרת הנהל טירו של \mathbb{R} טטרכ. לנה שטל חס:

$$h = a+bi+cj+dk \in H$$

$$hi = ai - b - ck + dj$$

חס h טטרכ, אכ טתקוים:

$$ih = ai - b + ck - dj$$

$$\Rightarrow c=0, d=0$$

\rightarrow ח טטוכ חזק
טתקוים טטיון

ומהמטעמה $hj = jh$

נקט שבא $b=0$ $h \in \mathbb{H}$ (קייטנו כי הוא מטעם)

$h \mapsto \bar{h}$ ^{הפונקציה} $h \mapsto \bar{h}$ •

$(a+bi+cj+dk) = a-bi-cj-dk$ $\bar{\cdot}$

$\overline{h_1 h_2} = \bar{h}_1 \cdot \bar{h}_2$ צריך לטובק שהפונקציה כזו מכפלת כל כמות של

(כמות הפונקציה ההפוכה היא הומומורפיזם של \mathbb{H} על עצמו (אוטומופיזם))

$h \cdot \bar{h} = (a+bi+cj+dk) \cdot (a-bi-cj-dk) =$
 $= a^2 + b^2 + c^2 + d^2 = |h|^2$
 (היחס המגדולי)

מסקנה: אכן אומר $h \neq 0$ \mathbb{H} יש הפכי, ומייד ניתן $\bar{\cdot}$ הפונקציה:

$h^{-1} = \frac{\bar{h}}{|h|^2}$

תכונות: הפונקציה $a+ib \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ $\mathbb{C} \ni$ $M_2(\mathbb{R})$ היא שכיח של \mathbb{C}
 כשזה לחיט $M_2(\mathbb{R})$ -?

את אותו הפונקציה (רבה אהבתי) $|\mathbb{H}|$:

נשים את שכל קוורטרניון $h = a+bi+cj+dk =$

$= (a+bi) + (c+di)j$

אין לנו רוחים של $\mathbb{H} = \{z_1 + z_2 j \mid z_i \in \mathbb{C}\}$

זו אהבתי הפונקציה הזו מראה וקטורי 19-ממדי של \mathbb{C} עם בסיס $1, j$

נשים את שהכל נכתם הפכה מטעם קודם: $jz = j(a+bi) = (a-bi)j =$

$= \bar{z}j$

$$z_1 - z_2 j \mapsto \begin{pmatrix} z_1 & \bar{z}_2 \\ -\bar{z}_1 & z_2 \end{pmatrix}$$

ההסתקה

②

$M_2(\mathbb{C})$ הנה פונקטורים של חזים.

הנחה: (בדוק רק מה שמוזכר)

$$(z_1 + z_2 j)(w_1 + w_2 j) = (z_1 w_1 - z_2 \bar{w}_2) + (z_1 w_2 + z_2 \bar{w}_1) j$$

המטרה היא לכתוב מחדש תוצאת ההסתקה של:

$$\begin{pmatrix} z_1 & z_2 \\ \bar{z}_2 & \bar{z}_1 \end{pmatrix} \begin{pmatrix} w_1 & w_2 \\ -\bar{w}_2 & \bar{w}_1 \end{pmatrix} = \begin{pmatrix} z_1 w_1 - z_2 \bar{w}_2 & z_1 w_2 + z_2 \bar{w}_1 \\ -\bar{z}_2 w_1 - \bar{z}_1 \bar{w}_2 & -\bar{z}_2 w_2 + \bar{z}_1 \bar{w}_1 \end{pmatrix}$$

נמצא מרחבים של \mathbb{C} בתוך H

$$\mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$$

$$\mathbb{R}(j) = \{ \quad \quad \quad | \quad \quad \quad \}$$

$$\mathbb{R}(h) = \{ \quad \quad \quad | \quad \quad \quad \}$$

הצגה מרחבים קוורטניונים h שטק"מים $h^2 \in \mathbb{R}$

$$h^2 = a + bh$$

כאשר h מתנו מרחבים קוורטניונים שטק"מים סולגניים מעלה שניה של \mathbb{R}

$$h = i + j$$

$$h^2 = (i + j)(i + j) = -2$$

$$\mathbb{R}[x] \ni x^2 + 2 = 0 \quad \leftarrow h \text{ מקיים את המשוואה}$$

$$\leftarrow \mathbb{R}(h) = \{a + bh \mid a, b \in \mathbb{R}\} \text{ (אחידה) ארכיב}$$

זה אומר שמרחב החזים \mathbb{R} -טק"מים (כמרחב ווקטורי של \mathbb{R})

זה גם שיהיה כי מהנוסחה ארבעה נוספים שברצוננו $h \in \mathbb{R}(h)$ או $h \in \mathbb{R}(h)$

כמוכן שהקומוטטיביות נכשלת מהמבנה שהוספתי רק חזרה \mathbb{R} - \mathbb{R} ,

מכך שטק"מים מהצורה $p(h), q(h)$ כאשר $p, q \in \mathbb{R}[x]$ סולגניים

של המרחב של H , מתחילים.

קראו אותם שבתנו הם מרחב של \mathbb{C}

מבנים אלגבריים 2 - תוכן מס' 2יהי חוג B .בהינתן אידיאלים $I, J \subset B$ נגזיר את היחסים שלהם:

① $I + J = \{i+j \mid i \in I, j \in J\}$

② $I \cap J$

③ $I \cdot J = \left\{ \sum_{k=1}^l i_k \cdot j_k \mid \begin{array}{l} j_k \in J \\ i_k \in I \\ l \in \mathbb{N} \end{array} \right\}$

ⓐ **הערות:** $I + J$ הוא האידיאל הנטורי הנטור מ- I ו- J ⓑ $I \cap J$ האידיאל הנטורי הנטור מ- I ו- J Ⓒ I, J אידיאל הנטור מ- $I \cap J$

נזכר בע"מ אם יבנתם.

הערה א': כה נכון בתנאי של $I + J \neq B$ (כי אזנו \exists אינו נחשב לאידיאל)

$$I = (f)$$

הערה ב': נחזיר את $F[x]$ של אידיאלים

(זה נובע מההאמרת של אוקלידס)

$$J = (g)$$

אם f, g זכים אז ייתכן לנו שקיימים $a, b \in F[x]$ שעומקם

$$\begin{array}{c} a f + b g = 1 \\ \uparrow \quad \quad \uparrow \\ I \quad \quad J \end{array}$$

$$1 \in I + J \Rightarrow I + J = F[x] \leftarrow$$

→ זה נובע
ש החוג

ב) נדיקה; (כזו טענה טריוויאלית)

ג) סכימות לחיבור ה- $I \cdot J$ נוספת מההכפלה ישירות:
סכימות לכל מהחולף

$$r\left(\sum_k i_j j_k\right) = \sum_k (r i_j) \cdot j_k$$

כמו-כן נקבע מההכפלה ש $I \cdot J \subset I \cap J$

~~∞~~

משפט (להתאמה) דיבר (המסנים ו) על טיוח תתי-חבורות (נורמליות של G/N)

שנמצאות בהתאמה חלף ואל עם חבורות נורמליות (המכלול את N

ואורולו ה- G . אותו משפט מתקיים אם נחזים

משפט (להתאמה) אחרים:

בהינתן חוט R ואידיאל $I \subset R$ ישנה להתאמה חלף ואל טין אידיאלים של חוט

הטנה R/I לטין אידיאלים של R (המכלים את I): $I \subset J \subset R$

(הוכחה): (תכונן הנומומורפיזם היטב):

$$\varphi: R \rightarrow R/I$$

$$\varphi(x) = \bar{x} = x + I \quad \text{:(המסדר ע')}$$

לכל אידיאל $L \subset R/I$ מתקיים ש: $\varphi^{-1}(L) = J$ אידיאל ה- R (המכל את I

(הערה): אם L אידיאל ממש ($L \neq R/I$) כלומר $1 + I \notin L$ אז ברור ש $1 \notin J$

כלומר J אידיאל ממש.

נכיון השט! בהיותן אידיאל $I \subset J \subset R$ מתקיים ש $L = \varphi(J) \subset R/I$ אם אידיאל

כי φ על.

$$L \rightarrow \varphi^{-1}(L)$$

$$J \rightarrow \varphi(J)$$

ין הוכחות כזו.

ברור כי $\varphi(\varphi^{-1}(L)) = L$ כי $\varphi \circ \varphi^{-1} = \text{id}$.

מכיוון השני:

$\varphi(J) = \{j+I \mid j \in J\}$

אכן $\varphi^{-1}(\varphi(J)) =$

$= \varphi^{-1}(\{j+I \mid j \in J\}) =$

$= \bigcup_{j \in J} \{j+I\} = J$

→ $J \rightarrow$ מחזיקים קבוצה, לא על אברים כפי שהשטנו קודם

בהוכחה "כ" ברורה וההוכחה "ע" נוספת מוכיח ש J מכיל את I .



סקרים: המציאותים R/I הם מהצורה:

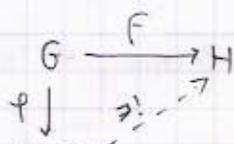
$J/I = \{j+I \mid j \in J\} \subset R/I$

(מקובל מנהל חבורה חבורה כי J מכיל את I)

עבור J אידאל שמת I

כאשר המציאותים R/I הם מהצורה J/I עבור אידאל J שמת I

את I

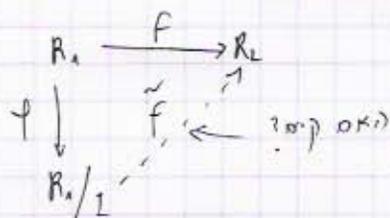


אם יש שתי חבורות

מכשלהם $N \subset \text{ker } f$ מתהייטם וקאם

עקרון שני: בהינתן חטים R_1, R_2 (אידאל) $I \subset R_1$ אם הומומורפיזם $F: R_1 \rightarrow R_2$

מתקין פירק הנה $I \subset \text{ker } f \iff R_1/I$



כאשר: מתבין צדק הטנה, סירוסו של ק"ם (הוטומופיני) \tilde{f}
 $\tilde{f}: R_1/I \rightarrow R_2$ רק שהזאתה (ה"ל) מתחברת לאוגר
 $f = \tilde{f} \circ \varphi$

הוכחה: הכחיות נרורה כי אם קיים \tilde{f} ירה אז הכרסין של f מכלי את הכרסין

של φ ששוה ל- I

מכאן שני, אם הכרסין של f מכלי את I אז נצייר

$$\tilde{f}(x+I) = f(x)$$

(אם שריבצים)

$$x_1 + I = x_2 + I$$

כה מוכר (ה"ט) כי אם

$$f(x_1 - x_2) = 0$$

אז $x_1 - x_2 \in I$ ולכן

Ker

$$\Downarrow$$

$$f(x_1) = f(x_2)$$

נותר לבדוק כי \tilde{f} אכן הוטומופיני.

באמצע: יהא f פולינום ב- $F[x]$

נסמן $I = (f)$ (מ"ן את האידיאלים בחום $F[x]/I$)

אידיאל בחום הטנה הוא מרובנה J/I כאשר $I \subset J \subset F[x]$

מאחר ו- $F[x]$ הוא **חוקרטי** (וקט"ל) $J = (g)$

הכילה $I \subset J$ אם ורק אם $f = g \cdot h$ \Leftarrow אם הכרוק של f ארמשיני

$$f = m_1 \cdot \dots \cdot m_\ell$$

הוא:

אז g ח"ם אלהות מכילה חלקית של m_i -

הערה: האידיאלים (הטקטואים) הם J/I סבוי $J = (m_i)$

מסנים מצטרפים 2- תואל מס 3

קריטריון מיינשטיין:

נתון סולנוס $p(x) = \sum_{i=0}^n a_i x^i$ על \mathbb{Z}

אם p סריק על \mathbb{Z} כלומר ישנס $f, g \in \mathbb{Z}[x]$ מפכה $1 \leq$ כן
ע: $p = f \cdot g$ אז הינו יכולים להטיל מוטו $|\mathbb{F}_p[x]|$ טחוקן הבא:

$\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ ובאל שיה חוס טנה על \mathbb{Z} יש לנו הוטרקה

(טמן את התמונה על \mathbb{Z} כ- $\bar{\cdot}$)

וההוטרופיה הינה מטרקה באופן טמטי (הוטרופיה בין הפולינומיל על החטים (אלי-)

$\mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x] = \mathbb{F}_p[x]$ כאשר ההוטרופיה היא:

$\sum a_i x^i \mapsto \sum \bar{a}_i x^i$

נחזור אפולנוס $\bar{p}(x) = a_i x^i \mapsto \mathbb{Z}[x]$

אם $p = f \cdot g$ אז $\bar{p} = \bar{f} \cdot \bar{g}$ כלומר תמונה p טול חמף מהחטים

$\mathbb{F}_p[x]$ סריקה

לראון נכנס קריטריון מיינשטיין שנתנה כיתה:

קריטריון מיינשטיין: אם $p(x) = \sum_{i=0}^n a_i x^i$ סולנוס על \mathbb{Z} ישנו ראשוני q

כך ש: $q | a_i$ $i=0, \dots, n-1$ $q \nmid a_n$ $q^2 \nmid a_0$

אז $p(x)$ מ-סריק על \mathbb{Z}

נוכיח את הו' כיתה

קריטריון ההפוכו: אם $p(x) = \sum_{i=0}^n a_i x^i$ ישנו ראשוני q הנקיים $q | a_i$

(טמן p מ-סריק על \mathbb{Z}): $p = (\sum_{i=0}^d b_i x^i) (\sum_{i=0}^{n-d} c_i x^i)$ $q^2 \nmid a_0$ $q \nmid a_n$

נשים אז אפטרופיה הכמותי $\text{deg } p = \text{deg } f + \text{deg } g$ ולכן $d + (n-d) = n$ (ההפוכו)

כהיכ $q \nmid b_d$ (אמנונו יוצים כ- הנקטרים החוכים b, c אז ממולקום כ- q

כי מפכאם שני a_0 לא ממולקום כ- q (קול שנספחה סמוק) $\bar{p} = \bar{f} \cdot \bar{g}$

כ- $\mathbb{Z}/q\mathbb{Z}[x]$ אז $\bar{p} = \bar{a}_0$ (יוצים לביאולמא סריק) כלומר סולנוס לביאולמא חוס

סולנו $\bar{f} \in \mathbb{F}_q$ לביאולמא $1 \leq d$ וכו' סריקה

הערה 1: טורם \mathbb{Z} ונתנה שדות והסניה ריבסיטר (הרי חסיה)

היא הכחה: מתחילים משה \mathbb{F} (כרגיל) אפוא שיה ניתן סגור סגור חותו)

כוחים סוגים אי-סדק $p(x) \in \mathbb{F}[x] \iff J = (p)$ (חיה) (ש)

הוא חיה מקסימלי $\mathbb{F}[x]/I \iff \mathbb{F}[x]$ שיה

(המקסימליות) $I \subseteq J \subseteq \mathbb{F}[x]: I \iff I \subseteq J = (q)$ $q \in \mathbb{F}[x]$ קים $q \in \mathbb{F}[x]$ כק s

(כי זה חס רחם, כל חיה) (נר"ע" חיה חיה) $\iff p = q \cdot g$ $p = q \cdot g$ ונתון ש- p סדק (ניצח) (החיה)

הערה נוספת: \mathbb{F} מר/משוק סוגים סבסי נתון $\mathbb{F}[x]/I$ δ העתקה

$$a \rightarrow \bar{a} = a + I$$

3 אם נטון $\mathbb{F}[x]/I = \mathbb{L}$ אז נתון סגור $p(x)$ טיב I

\mathbb{L} $= \mathbb{L}[t]$ חס (סגור) יונים סטניה t \mathbb{L}

אם $p(x) = \sum a_i x^i \in \mathbb{F}[x]$ אז $p(t) = \sum \bar{a}_i t^i$

כנתון $\mathbb{L} = \mathbb{F}[x]/I$ יש את החסר (הטיק) $\bar{x} = x + I$ (זים את החיה $\bar{x} \in \mathbb{L}$)

כ- $p(t)$ וקטל

$$p(\bar{x}) = \sum \bar{a}_i \bar{x}^i = \overline{\sum a_i x^i} = \overline{p(x)} = 0 \in \mathbb{L}$$

תרגיל: נתון סגור $p(x) = x^3 + 2x^2 - 4x + 2$ \mathbb{Q} הוא אי-סדק \mathbb{Q} סגור

אי קרטרן אי-נטטין $2|2, 2|4, 2|2, 2|2$ $2^2|2$ (אכן)

הסוגים הנה אינו סדק \mathbb{Q} (נלם הכחה סטניה)

נתון: $p(x)$ אי-סדק \mathbb{Q} $\mathbb{F}[x]$ אינו קרטרן אי-נטטין

ואכן $\mathbb{F}[x]/(p)$ שיה וכן אז מתקנה ניתן אפוא את הרבה $(p) = I$

נסמן $g(x) = x^2 + x + 1$ ונרבה אפוא את העתקה $\bar{h} = h + I$

ככ $\bar{g}\bar{h} = 1 \in \mathbb{L}$ כוא את $(\bar{g}) \in \mathbb{L}$

$\bar{g}\bar{h} = 1 \iff gh - 1 = p \cdot f$ $gh - 1 = p \cdot f$

אז אחרונים $gh + pf = 1$ (זכור) אפוא f, h סגור p, g $gh + pf = 1$ $gh - 1 = p \cdot f$ $gh + pf = 1$ $gh - 1 = p \cdot f$ $gh + pf = 1$ $gh - 1 = p \cdot f$

הרחבות של שדות.

בהינתן שדות $F \subset K$ אומרים ש K שדה הרחבה של F ומסמנים "K/F" או "K:F" (K על F)

K מהווה הרחבה וקטורי של F.
היטעם של K כמרחב וקטורי (קרא פרק הרחבה).

בהינתן הרחבה K/F, עבור זיכר $\theta \in K$ (מטן) $F(\theta)$ את השדה התיניתי (בתוך K) שטכיל את F ואת θ .

$$F(\theta) = \bigcap_{L \text{ שדה}} L \text{ שטכיל } F \text{ ו-} \theta \in L$$

(צבר היום θ) היטוואציה היי בשיטה שלה הרחבות מפרטת 2

הרחבות מפרטת 2

תהי K/F הרחבה מפרטת 2.

מסקולי טיפ נוסע שמיין שדות כינים $f \notin L \subset K$

מסקנה: אז $F \cup \theta \in \theta$ מתקיים
(צעה סב-א/א-ס-F)
עבור $\theta \in K \setminus F$ מתקיים:

ש $\theta, 1$ בלתי תלויים אינאריה של F

(כי אם $a+b\theta=0$ אז $\exists a,b \in F$ אז $a=b-\theta$ או $\theta \in F$ ומה זה איתנו יוצאים שזה לא מתקיים)

כאל שהפרטה היא 2, נקטל ש $\theta, 1$ בסיס F -K מל F

$$K = F(\theta) = \{a+b\theta \mid a,b \in F\}$$

(ההרצה הנל היא יחידה)

אזמת כמות, $\theta^2, \theta, 1$ כפר תלויים אינאריה של F (כי מה 3 אינאריים)

ולכן קיימים $a, b, c \in F$ כך ש $a\theta^2 + b\theta + c = 0$, $a \neq 0$ כי אחרת θ הוא תלוי.

ולכן θ מקיים פולינום מפרטת 2, נאמר θ הוא שורש של פולינום מפרטת

2 מל F (והפולינום הזה הוא: $P(x) = ax^2 + bx + c$ (פולינום ריבועי))

$$P(\theta) = 0$$

א. התקף טענה זו: הוכח $\exists \theta \in F$! θ הוא שורש של פולינום ריבועי מעל F

(שים לב, $P(x)$ הוא פולינום מ- F מעל F)

כי אם היה שורש θ של $P(x)$ אז שני השורשים של P היו θ ו- θ

היינו מקבלים של $P(x)$ יש 3 שורשים ב- K

סיכום: כל הרחבה מובנת K/F היא מהצורה $F(\theta)$ כאשר θ הוא שורש

של מטריצה ריבועית מעל F (שמיין לה שורשים ב- F)

משקלה "טבעית" של הרחבות כזו, היא משקלה הרחבות K/F כאשר

$$K = F(\theta) \quad \theta^2 = \alpha \in F \quad (\text{מסומן } \sqrt{\alpha} = \theta)$$

במקרה שכזה נקראת הרחבה K/F שונה מ- F אך כל הרחבה מובנת K/F ,

היא מהצורה הזו, כלומר הרחבה הרחוקה θ הוכחה שורש של פולינום $P(x)$ מעל F

שורש ב- F .

בדקה: נהיה K/F מובנת K , נבחר $\theta \in K \setminus F$. נהפיק שמיין יודעים כי קיים

$$P(x) = ax^2 + bx + c \quad (\alpha \neq 0) \quad \text{פולינום מובנת } K$$

$$P(\theta) = 0 \quad \text{כק ש:}$$

$$P(x) = 0$$



$$x = \left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a^2} - \frac{c}{a}$$

יודעים כי θ בחר את המשוואה הזו ולכן אכן נסמן $\omega = \theta + \frac{b}{2a}$, $\omega \notin F$

$$h = F(\theta) = F(\omega) \quad \leftarrow \quad \omega^2 = \frac{b^2}{4a^2} - \frac{c}{a} \in F \quad \text{ומקיים}$$



בעזרת: מין נורמלות K/C מוצגת סוסית.

הוכחה: נהיית $C \setminus K$ מצבוי $\deg(K/C) > n$ מתקיים ש:

$\theta^0, \theta^1, \dots, \theta^{n-1}$ תווים זינאית מל C ולכן ישנם $a_0, \dots, a_{n-1} \in C$

$$\sum a_i \theta^i = 0 \quad \text{כך ש}$$

או לחלופין θ שורש של פולנום מל C (זה נסתרה אלמט ריסוד)

של המצבה.

דוגמא נכית עבור שדה מופין 2: $\text{char } F = 2$:

נבחר $\mathbb{Z}/2\mathbb{Z} = F_2$ (האיברים הם $(0, 1)$) ולפי ניתן להוציא שורש

וקנינו בעבר בהצגה K/F_2 מוצגת 2 (א שדה בן מוצגת אינדיס)

ולכן א זיענו מתקבל מ F_2 ע"י הוספת שורש של אינדיס F מל

לאור מה שרצינו בתחילת השיעור א בן מתקבל ע"י הוספת שורש של פולנום ריסודי

מל F .

$$K = F_2[x]/(x^2 + x + 1)$$

מבנים אלגבריים 2 - תוצאות מס' 5

נפרד היום שום על קריטריון מייננסטיין והלמה של אציוס.

קריטריון מייננסטיין (ננסח במשק)

יהי R תחום פריקות חד-ערכית ! $I < R$ אידיאל ראשוני.

אם $f(x) = \sum_{i=0}^n a_i x^i$ שסגורו $a_i \in I$ $i=0, \dots, n-1$ $a_n \notin I$

אז $f(x)$ אי-סריק בחוט $R[x]$. (צריך הנהגה נכסרת והיא שהמחוק הנישטול (המקסימלי) של מקדמי הפולינום הוא 1).

ההוכחה: נניח בסלילה של f היה סריק אז היו $g(x), h(x) \in R[x]$

$f(x) = g(x)h(x)$ שסגורים

(הנחתנו אסבי ה \gcd של מקדמי f מוגדרת שהסיווק הכה הוא למכסלת סוליטעמים ממעלה ≤ 1).

נסמן את ההומומורפיזם הטבעי $R \rightarrow R/I$ $\alpha \rightarrow \bar{\alpha}$; הומומורפיזם זה מתרחם בצורה

$R[x] \rightarrow R/I[x]$ $\sum b_i x^i \rightarrow \sum \bar{b}_i x^i$; $\bar{\alpha}$

ונקטל את הישויון הנא ב- $R/I[x]$: $\bar{\alpha}_n \cdot x^n = \bar{f} = \bar{g} \cdot \bar{h}$

ממחר (הסיווק של x^n למכסלת סוליטעמים אי סריקים הוא $x^n = x \cdot x \cdot \dots \cdot x$ נקטל של :

$\bar{g} = \bar{r} \cdot x^m$, $\bar{h} = \bar{s} x^{n-m}$

$\bar{\alpha}_n = \bar{r} \cdot \bar{s}$ כמשק

נסמן שם $m \neq 0$ אם $n-m \neq 0$

ממחר נחמר (הומומורפיזם שלני $R/I[x]$; $R[x]$) צרכות יכולות רק לצבנה,

נקטל שממחר אצבנת \bar{f} (שמה n אז צרכותיהם של \bar{g}, \bar{h} אם בן שמורות כמו של g, h

כפרט אצלות שנות 1.

\Leftarrow : \bar{g}, \bar{h} מין מקדמים תוכסטיים \Leftarrow (המקדמים התוכסטיים של g, h היו ב- I).

\Leftarrow (המקדמים התוכסטיים של $f \in I^2$ וכו' סתירה!)

הערה: מכאן נקרא שמום $\sum_{i=0}^n a_i x^i$ פולינום טרנקהטיים שלמים

שסמורו: ① $\gcd(a_1, \dots, a_n) = 1$

② קיים ראשוני p (נחלק את a_i $i=0, \dots, n-1$)

$\sum a_i x^i$ אי-פריק $\mathbb{Z}[x]$ אם $p^2 \nmid a_n$ או $p^2 \nmid a_0$

מה הקשר בין פריקות של פולינום ב- $\mathbb{Z}[x]$ לבין אי-פריקות שלו ב- $\mathbb{Q}[x]$?

אז כיתה כלליות אם \mathbb{Z} רחום פריקות קב-עתי F ! שדה. (הנחת של F אז מה הקשר בין

אי-פריקות ב- $\mathbb{R}[x]$ לבין אי-פריקות ב- $\mathbb{F}[x]$.

ברור שם $\mathbb{R}[x] \in \mathbb{R}[x]$ מקיים שג- \gcd של מקטנו $1 =$ אז אי-פריקות ב- $\mathbb{F}[x]$

אנחה אי-פריקות ב- $\mathbb{R}[x]$.

הערה של מאס: (נמצא הכיוון הישני של מה שזה נהיה רחום).

אם $\mathbb{R}[x] \in \mathbb{R}[x]$ אי-פריק ב- $\mathbb{R}[x]$ אז הוא אי-פריק ב- $\mathbb{F}[x]$. (אם נכניח דמות כרס)

קריטריון מיינרסטיין (הניסוח המקורי):

אם \mathbb{Z} , \mathbb{R} , \mathbb{F} הם כניסוח הקופסא אז לא רוק של f אי-פריק ב- $\mathbb{R}[x]$

הוא אם אי-פריק בחום הפולינומים מעל שדה רחום $\mathbb{F}[x]$.

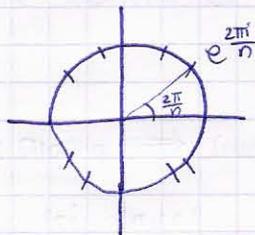
דוגמה: מהינתן שדה F מוסף האיברים ב- F המקיימים את המשוואה $x^n - 1 = 0$

נקראים שורשי יחידה. n ב- F .

מסקנות: - 1 שורש יחידה n

- שירות לכל n נהכני

- כלומר מוסף שורשי היחידה n מהווה תת-חבורה של F^* שסדרה $n \geq$



טמקרה $F = \mathbb{C}$

יש n שורשי

$e^{\frac{2\pi i k}{n}}$ יחידה

$k = 0, 1, \dots, n-1$

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \dots + 1) \quad \text{נשים לב ש:}$$

$$\text{Q} \quad \sum_{i=0}^{n-1} x^i \quad \text{הי-כריק מסל} \quad \text{נסה להכין עבור זילן n-1 (הכולנים)}$$

נתבונן במיזמוניסם מ $\mathbb{Z}[x]$ אצטנו העוסר ע"י $p(x) \mapsto p(x+1)$

(תשתמשו בשיש שימור של הכסולות, כלומר \cong שההסתקה היא הומומורפיסם (העוקבה שצה

מיזמוניסם נבער עכב שההכב: נמן ע"י $p(x) \mapsto p(x-1)$

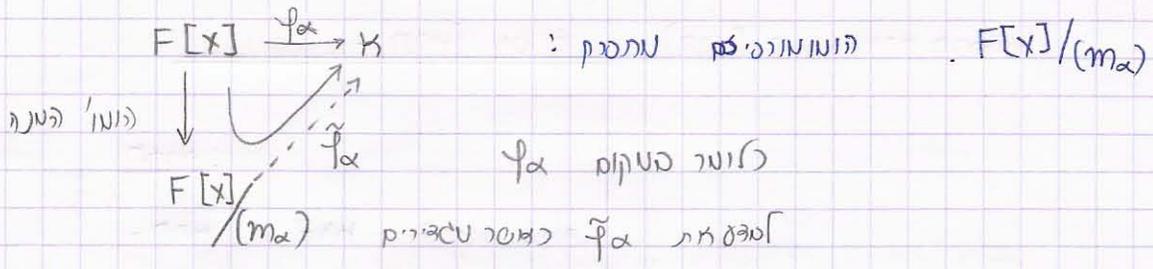
$$x^n - 1 = (x-1) \left(\sum_{i=0}^{n-1} x^i \right) \quad \text{(כע) חת המיזמוניסם}$$

$$\implies (x+1)^n - 1 = x \left(\sum_{i=0}^{n-1} (x+1)^i \right) \xrightarrow{\text{לבי}} \sum_{i=1}^n \binom{n}{i} x^{i-1} = \sum_{i=0}^{n-1} \binom{n}{i+1} x^i$$

בינעם נוסק
(ונצטב x)

למ $n=p$ מס' נמשני אב (הכולנים במאל שמה עונה על תנאי קריטריון מיזמוניסם עבור

נמשני p



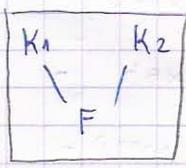
אותה $\tilde{\phi}_\alpha$ (ביים) $\tilde{\phi}_\alpha$ הוא שיכון כי מתוקים

מס' (המנוס'ים) $\tilde{\phi}_\alpha$ (הנה שפה כי m_α מ-ז-פיק) $F[x]/(m_\alpha)$

אין $\tilde{\phi}_\alpha$ היא מינוס'ים של השפה $F[x]/(m_\alpha)$ עם תמונת $(K \neq)$
 (תמונת שפה תחת (המנוס'ים היא שפה) תמונת היא) $\{ \sum_{i=1}^n a_i \alpha^i \mid a_i \in F \}$

$K \supseteq F(\alpha) = \{ \}$ מסקנה:

הערה: המינוס'ים $\tilde{\phi}_\alpha$ שזהו מה $\bar{\alpha} = \alpha + (m_\alpha)$



מסקנה: אם נתונה 2 הרחבות $K_1, K_2 \setminus F$

ניתן אם $K_1 = F(\alpha)$, $K_2 = F(\beta)$ וכן $m_\alpha = m_\beta$

$\alpha: K_1 \cong K_2 \iff K_1 \cong F[x]/(m_\alpha) = F[x]/(m_\beta) \cong K_2$

שעבורו: ① $\alpha(\alpha) = \beta$

② $\sigma|_F = id$

הערה: כאן הוכחנו קיום אברור ש α כפי הוא יחיד כי אם τ

הוא סוג מינוס'ים בעל התמונת הנל

$$\tau(\sum a_i \alpha^i) = \sum \tau(a_i) \tau(\alpha)^i = \sum a_i \alpha^i = \alpha(\sum a_i \alpha^i)$$

\downarrow
② + ①

$\sigma = \tau \iff$

הערה: אם מתקנה $K_1 = K_2$, כושר (תורה) הרחבה $K = F(\alpha)$ אפוא

(הינא'י) של α , מ יש סוג שנים β כ K

אז ישנו מינוס'ים מהשפה א' צפנו (מינוס'ים) σ , שעבורו

$\sigma|_F = id_F ! \quad \alpha(\alpha) = \beta$

$$K = \mathbb{C} = \mathbb{R}(i)$$

$$F = \mathbb{R}$$

$$m = x^2 + 1$$

$$\beta = (-i) \quad \text{אם} \quad \alpha = i$$

$$\alpha(z) = \bar{z}$$

הערה: אם α אוטומופיזם σ של K הנקיים $\sigma|_F = \text{id}_F$ אם σ אם σ

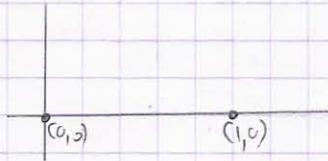
α שורש של הפולינום $\sum a_i x^i = f(x) \in F[x]$ אם $\alpha(\alpha) = f(\alpha)$ שורש של f

$$\sum a_i \alpha(\alpha)^i = \sum \alpha(a_i) \alpha(\alpha^i) = \alpha(\sum a_i \alpha^i) = \alpha(f(\alpha)) = \alpha(c) = c = 0 \quad \text{הוכחה:}$$

יש $\alpha \in K$ שורש של m_α של K ו- K

סכמ' ומחוכה

בניית הרציונלים:

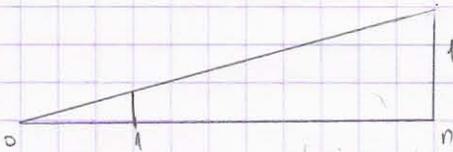


ניתן לחבר, עם המחוכה ונכח נכונים

מ. השאלה איך מביעים $\frac{1}{n}$

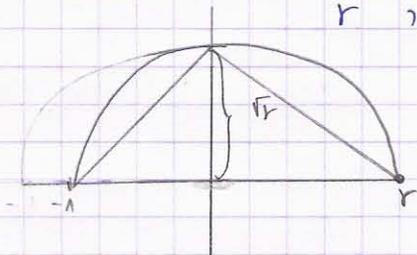
דימיון משולשים מאפשר לנו לבנות מכאן את הנט' מחזקה $\frac{1}{n}$

אנחנו ס' חיבור (קבל את כל הרציונלים).



הוצאת שורש: נניח שבינו את הנסכר r

משכך נבחרים $\sqrt[n]{r}$



נרצה לנתח את שדה הריבוי של $p(x) = x^5 - 3$ על \mathbb{Q}
 מסתבר כי $\alpha = \sqrt[5]{3}$ הוא שורש של $p(x)$ וכן $\theta = e^{\frac{2\pi i}{5}}$ הוא שורש של $x^5 - 1$.

חשבת שורשי $p(x)$ הם $\alpha, \alpha\theta, \dots, \alpha\theta^4$

אם כן שדה הריבוי הוא:

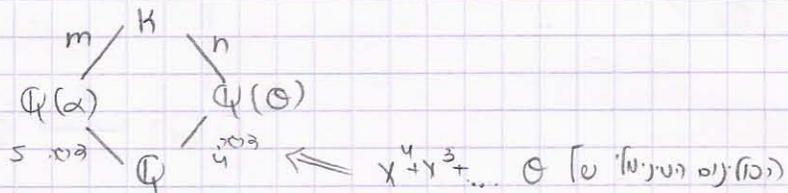
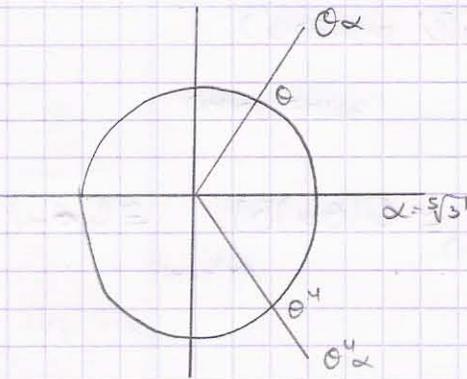
$$K = \mathbb{Q}(\alpha, \alpha\theta, \dots, \alpha\theta^4) = \mathbb{Q}(\alpha, \theta)$$

כי $\theta, \theta^2, \theta^3, \theta^4 \in \mathbb{Q}(\alpha, \theta)$

נרצה להבין את תכונת גלואה $G = \text{Gal}(K/\mathbb{Q})$

תכונה חשובה

$$(\theta^j \alpha)^5 = \theta^{5j} \alpha^5 = 3$$



$$[\mathbb{Q}(\alpha, \theta) : \mathbb{Q}(\alpha)] = n$$

α מקיים פולינום טייטלי ממונה $n \leq 5$ על \mathbb{Q} ולכן $n \leq 5$

$$[K : \mathbb{Q}] = 4 \cdot n = 5 \cdot m$$

$$m \leq 4, n \leq 5$$

ולכן ממחרת! - 4, 5 מסתדרים כפנים

$$n=5 \iff 5|m \iff 4|m$$

$m=4$

מסקנות:

① הריבויים הטייטלי של θ על $\mathbb{Q}(\alpha)$ (שמו $x^4 + x^3 + x^2 + x + 1$)

② הריבויים הטייטלי של α על $\mathbb{Q}(\theta)$ (שמו $x^5 - 3$)

(ניתן $x^5 - 3$ לא הריבויים הטייטלי של α על $\mathbb{Q}(\theta)$)

$$x^5 - 3 = m_\alpha \cdot (h) \quad \text{אם } m_\alpha \text{ איננו}$$

מחשבת גלואה נכונה $|G| = 20$ (כי K/\mathbb{Q} נורמלית וסכומית \iff גלואה)

נבנה את המיטמונורפיזמים (המרכיבים) את G

איך נונים מיטמונורפיזם? מיינרצוקיה

מסתבר שיש מיטמונורפיזם σ הפיכים את α ל $\theta^j \alpha$

מק"ם $\alpha \in G$ אוטומופיזם

$$i=0, \dots, 4 \quad \sigma(\alpha) = \theta^i \alpha$$

$$j=1, \dots, 4 \quad \sigma(\theta) = \theta^j$$

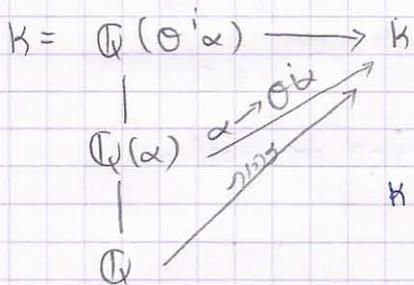
נקט i, j כגוף ונסנה α כגוף. (כגוף α נוסף θ^i בוס i, j)

$$G = \{ \sigma_{ij} \mid i \in \{0, \dots, 4\}, j \in \{1, \dots, 4\} \}$$

$$\mathbb{Q} \xrightarrow{\text{מיון}} \mathbb{Q} \quad \mathbb{Q}(\alpha) \cong \frac{\mathbb{Q}[x]}{(x^5-3)} \cong \mathbb{Q}(\theta^i \alpha)$$

$$\mathbb{Q} \rightarrow \mathbb{Q}(\theta^i \alpha) \quad \mathbb{Q}(\theta^i \alpha) \uparrow \mathbb{Q}(\alpha) \quad \text{קיימו אוטומופיזם מ $\mathbb{Q}(\alpha)$ ל $\mathbb{Q}(\theta^i \alpha)$ }$$

(שהצטפוס שלו \mathbb{Q} - (נוא הפחות)



מאיתו המיון

$$K = \mathbb{Q}(\alpha)(\theta) \cong \frac{\mathbb{Q}(\alpha)[x]}{(x^4+x^3+x^2+x+1)} \cong \frac{\mathbb{Q}(\theta^i \alpha)[x]}{(x^4+\dots+1)} \cong \mathbb{Q}(\theta^i \alpha)$$

ולכן $K = \mathbb{Q}(\theta^i \alpha)$

$$\mathbb{Q}(\alpha) \xrightarrow{\varphi} \mathbb{Q}(\theta^i \alpha)$$

(קנה) אוטומופיזם (מרחים את φ)

$$\mathbb{Q}(\alpha, \theta) \text{ מ } \mathbb{Q}(\alpha, \theta^i)$$

מרחיב לנו שטני השדות הללו הם α ולכן מסה"כ מנינו אוטומופיזם של \mathbb{Q}

(שהוא הפחות \mathbb{Q}) (נשוק את α ל $\theta^i \alpha$ ואת θ ל θ^j)

נסמן אוטומופיזם $\sigma_{ij} : \alpha \rightarrow \theta^i \alpha$ ו $\theta \rightarrow \theta^j$ (חשב את אוח הכסל)

$$\theta \rightarrow \theta^j$$

$$\sigma_{ij} \sigma_{kl}(\theta) = \sigma_{ij}(\theta^k) = \theta^{kj}$$

$$\sigma_{ij} \sigma_{kl}(\alpha) = \sigma_{ij}(\theta^k \alpha) = \sigma_{ij}(\theta^k) \sigma_{ij}(\alpha) = \theta^{kj} \theta^i \alpha = \theta^{i+kj} \alpha$$

$$\sigma_{ij} \sigma_{kl} = \sigma_{(i+kj)j} \quad (\text{החיסור הוא mod 5})$$

הצטפוס \mathbb{C} ממוצעת Γ א מכוון אתר מספר 2 ב- \mathbb{C} ולכן שבו

השבת שלה שהוא $\mathbb{R} \cap K$ צפן להיות הרכבה מפוסה 10 מ \mathbb{Q} .

$$\mathbb{Q}(\sqrt[5]{3}, \frac{\theta + \theta^4}{2}) = \mathbb{R} \cap K \quad \text{ולכן}$$

מטרים אלאגרים - תכאל מט' 8

מטרת השיעור היא לתת את שדה הפיצול של הפולינום $x^4 - 2$.
נסמן K

K/\mathbb{Q} היא הרחבת אלווזה כלומר נרמלית וספרטלית כי זה ממזין 0.
(שדה פיצול של פולינום ספרטלי הוא הרחבת אלווזה)
נבדוק את שורשי הפולינום: $a = \sqrt[4]{2}$

$$\mathbb{Q}(a) = \mathbb{Q}[x] / f_a(x)$$

אכן $[\mathbb{Q}(a) : \mathbb{Q}] = 4$

אם נוסיף את i ל $\mathbb{Q}(a)$ קיבלנו את כל השורשים.

הפולינום $x^2 + 1$ מעל \mathbb{Q} , מתמסס ע"י i

$i \notin \mathbb{Q}(a)$ ואכן $[\mathbb{Q}(a, i) : \mathbb{Q}(a)] = 2$

ואכן ממסלת ההרחבות $[\mathbb{Q}(a, i) : \mathbb{Q}] = 4 \cdot 2 = 8$

שדה הסדרים: $[\mathbb{Q}(a) : \mathbb{Q}] \cdot [\mathbb{Q}(a, i) : \mathbb{Q}(a)]$

נרצה לתאר את $Gal(K/\mathbb{Q})$

בו הרחבת אלווזה $\Leftrightarrow |Gal(K/\mathbb{Q})| = 8$

אוטומופיזם עושה פרמוטציה לשורשים

השורשים הם - $a = \sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$
" " " "
 $a, ia, i^2a, -i^3a$

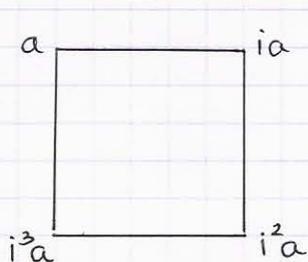
$a \mapsto a, ia, i^2a, -i^3a$ \Leftrightarrow (4 תמשרויות)

$i \mapsto i, -i$ (2 תמשרויות)

\Leftrightarrow אכל היוונו יש 8 תמשרויות

\Leftrightarrow אלו הם כל האוטומופיזמים כי יש אכל היותר 8 אוטומופיזמים G -

מענה: $Gal(K/\mathbb{Q})$ היא הרחבה הפינהצית D_4



מספר אסוכב את הריבוע אשקלי

אונת סטיק מצשטו צ"י

נסמן α - סימול

τ - שיקוף

$$D_4 = \{id, \alpha, \alpha^2, \alpha^3, \tau, \tau\alpha, \tau\alpha^2, \tau\alpha^3\} \Leftarrow$$

כל תמונה שתתקבל (ויהא מסימוליים ושיקוליים).

הוכחת היסודות: (נסמן α מה α ומה i מה α - τ שיקוף שמיין מה α ל i)

$$\sigma(\alpha) = i\alpha \quad \sigma(i) = -\alpha$$

$$\tau(\alpha) = \alpha \quad \tau(i) = -i$$

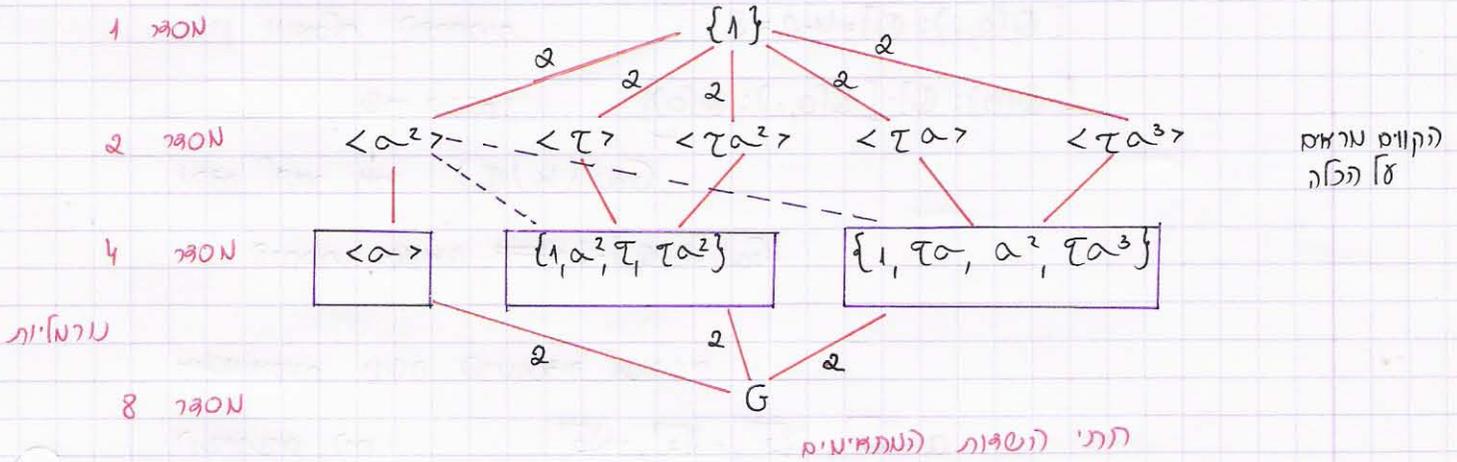
ספיר מה D_4 נוצר מהזרת: $D_4 = \{\sigma, \tau\}$

$$\alpha^4 = \tau^2 = id$$

$$\alpha\tau = \tau\alpha^3$$

הכנסות: חבורת גלואה הוכחה (הכנות):

תתי חבורות של $Gal(L/K)$



תתי (השפיות) (המתחמים)

א מתחמים Γ כי Gal הוכחת ספר

דברת הוויחקה של (השפיה) (המתחמים) Γ יהיה מופחת (הוכחה) 4 עם א

נחשב מה שיהי (השפיה) של α - הוא מושיב טקוק מה i

$$\mathbb{F}(i) \subset \mathbb{F}(\langle \alpha \rangle)$$

$$\mathbb{F}(\alpha) \subset \mathbb{F}(\langle \tau \rangle)$$

$$[\mathcal{F}\langle\tau\rangle:\mathbb{Q}] = [G:\langle\tau\rangle] = 4$$

$$[\mathcal{F}\langle\sigma\rangle:\mathbb{Q}] = [G:\langle\sigma\rangle] = 2$$

$[\mathbb{Q}(a):\mathbb{Q}] = 4$ כי הרכבה מספר 4 של \mathbb{Q} וכך גם $K^{\langle\tau\rangle}$

$$\mathcal{F}\langle\sigma\rangle = \mathbb{Q}(i) \quad \text{ועל כן } \mathbb{Q}(a) = \mathcal{F}\langle\tau\rangle \leftarrow$$

$$\mathbb{Q}(a^2) = \mathbb{Q}(\sqrt{2}) \quad \text{כי כן תת הרכבה מספר 2}$$

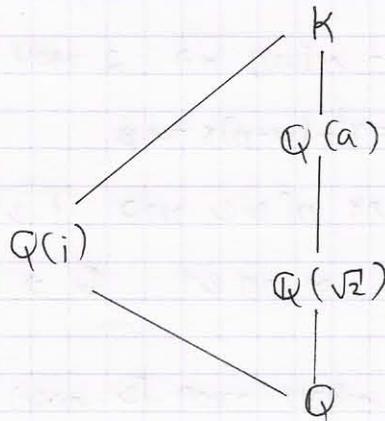
$$\sigma^2(\sqrt{2}) = \sqrt{2} \quad \text{ועל } \tau(\sqrt{2}) = \sqrt{2} \quad \text{ועל}$$

$$\sigma(\sigma(a^2)) = \sigma(i^2 a^2) = i^4 a^2 = a^2$$

$$\mathbb{Q}(\sqrt{2}) \subset \mathcal{F}\langle\sigma^2, \tau\rangle \quad \leftarrow$$

אם תת הרכבה שנוצרת ע"י σ^2, τ היא $\{1, \sigma^2, \tau, \tau\sigma^2\}$

ואין נקטא:



היסטורי ארתי חבורה של $Gal(L/K)$

אברים מספר 2: τ, σ^2

$$k=1,2,3 \quad \tau\sigma^k$$

$$\tau\sigma^k\tau\sigma^k = \tau\tau\sigma^{2k}\sigma^k = \tau^2\sigma^{4k} = 1$$

נמשך היסטורי ארתי היחסות מתאימות:

$$\mathcal{F}\langle\sigma^2, \tau\rangle = \mathbb{Q}(ia^2)$$

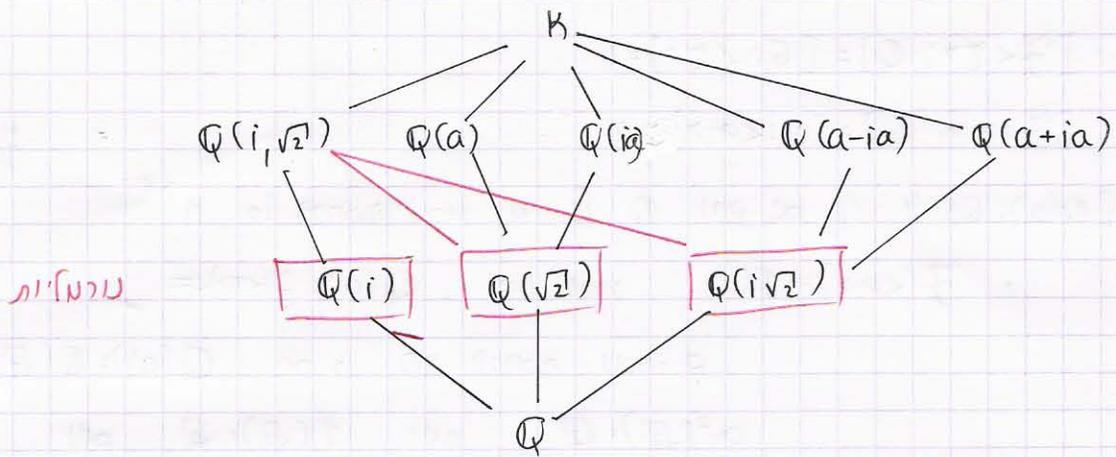
$\mathbb{Q}(ia^2)$ (ההרכבה האחרונה) (החבורה אחרי משפט א' אהה)

היקומפוזיטום של $\mathbb{Q}(\sqrt{2})$! $\mathbb{Q}(i)$ מתאים לחיתוק של היחסות-

$$\langle\sigma\rangle \quad ! \quad \{1, \sigma^2, \tau, \tau\sigma^2\}$$

שתי $\langle\sigma^2\rangle$.

$\mathbb{Q}(i, \sqrt{2})$ (הוא אמור להיות מתאים) $\langle\sigma^2\rangle$ גאומטרי מקום (היקומפוזיטום) הוא



מה החיתוך של $\{1, \alpha^2, \tau, \tau\alpha^2\}$, $\{1, \tau\alpha, \alpha^2, \tau\alpha^3\}$ הוא α^2
 ולכן הקומפוזיטום של $Q(\sqrt{2}), Q(i\sqrt{2})$ היא $Q(i, \sqrt{2})$

נתת חבורה מונומיאלית 2 היא נורמלית. (מח' הכרות אותה מחלקיה)
 כל הכחקה מסוג 2 היא נורמלית - אם יש שורש 1 יש אם אחר השני.

$$Q[x] \ni (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$$

יש כבר שורש 1 ברור שיש לנו את השורש השני,
 כי $\alpha + \beta \in Q$ ויש את α אז אם β יהיה באותו השדה.

סעיף: שפה היסטת של חבורה נורמלית היא רוחסה נורמלית.

המסקנה היא שחבורה נורמלית יוצרים שני נורמלי בהכחקה.

מי עוד נורמלי השפות המתחייבים?

$$\langle \alpha^2 \rangle \text{ הוא שפה סיבול של } (x^2-2)(x^2+1)$$

מבנים אלגוריתם 2 - תוכן מט 9

רמטרה: תוכן זה:

אנחנו פוזיטום $f \in \mathbb{Z}[x]$ מי-סדרן כך שכל ההוקציות שלו מופאו ראשוני- p הם סריקות:

$$\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$$

$$x^2 + px + 2 \longrightarrow x^2 + \bar{p}x + \bar{2} = x^2 + 2$$

~~✗~~

טענה: כל הרחבה סופית של \mathbb{Q} היא טטוסה.

הוכחה: לה נכון לכל הרחבה סטטולית.

הוכחה: תהי $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ הרחבה סופית.

נתבונן ב- $K_q = \mathbb{Q}(\alpha_1, \dots, \alpha_{n-1}, \alpha_n + q\alpha_n)$ $\forall q \in \mathbb{Q}$

נטען כי K יש מט סופי של שדות ביניים.

(מנהלתמנה ארתת חבורות - יש מט סופי).

אכן קיימים $q_1 \neq q_2$ כך ש: $K_{q_1} = K_{q_2}$

$$\alpha_1, \dots, \alpha_{n-1} \in M$$

$$M = K_{q_1} = K_{q_2}$$

$$M \ni (\alpha_{n-1} + q_1 \alpha_n) - (\alpha_{n-1} + q_2 \alpha_n) = (q_1 - q_2) \alpha_n$$

$$\alpha_n \in M \implies \alpha_{n-1} \in M$$

טטת קיטלני של $M = K$ (נתתנו $n-1$ מטרים והראנו שיש נופוסי: $n-1$ מטרים כך נמשיך עד שיש n מטרים)

~~✗~~

$\mathbb{Z} \longrightarrow M$ הוכחה:

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \longrightarrow M$

(הישא הפרימל' שמתאים ל- M)

שדות סופיים

טענה: כל שני שדות סופיים נחווט אצלם הם איזומורפיים

הוכחה: יהיו שני שדות $|H| = |L| = p^n$

L ! H הרחבה סופית של \mathbb{F}_p

הוכחנו סריקה ששדה בינו של כולתם סטטול' הוא יחיד.

נראה ש L ו- H הם שמת בינו של אותו כולתום מטל \mathbb{F}_p

$$|K^*| = p^n - 1$$

אכן מטעם ברור הקטן $a \in K^*$

$$a^{p^n-1} = 1 \implies a^{p^n} - a = 0$$

אזי נכון $b \in L$

$$0^{p^n} - 0 = 0$$

אם מינה האם מקיים ש:

$$X^{p^n} - X = 0 \quad \text{על } \mathbb{F}_p$$

אכן האיברים של L הם שורשים של

משיקולי עממי, L הם שדה הביטוי של הפולינום הסכמי

$$()' = p^n x^{p^n-1} - 1 = -1 \quad (\text{סכמי})$$



מסקנה: אם $a \in \mathbb{F}_p$ שמינו ריבוע אז ההכמה הריבועית $\mathbb{F}(\sqrt{a})$

מכילה את כל השורשים הריבועיים של \mathbb{F}_p

$$\mathbb{F}(\sqrt{a}) = \mathbb{F}_p[x] / x^2 - a$$

הוכחה: יהי $b \in \mathbb{F}_p$ אם b ריבוע ב \mathbb{F}_p אז $\sqrt{b} \in \mathbb{F}_p \subseteq \mathbb{F}_p(\sqrt{a})$

אם $b \in \mathbb{F}_p$ מינו ריבוע אז ההכמה $\mathbb{F}_p(\sqrt{b})$ מטעם 2

אכן $|\mathbb{F}_p(\sqrt{a})| = |\mathbb{F}_p(\sqrt{b})|$ אכן הם מצטמצמים. אכן מכיון ש b יש שורש

ב $\mathbb{F}_p(\sqrt{b})$ אזי יש לו שורש ב $\mathbb{F}_p(\sqrt{a})$

$$\mathbb{F}_p(\sqrt{a}) \leftarrow \mathbb{F}_p(\sqrt{b}) \quad \text{הכמה}$$

$$\phi(\beta^2) = \phi(b) = b \quad \beta^2 = b$$

נניח $d_1, d_2 \in \mathbb{Z}$ כך ש: $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) / \mathbb{Q}$ מופנה 4

קיים θ כך ש: $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$

בסיס K - $1, \sqrt{d_1}, \sqrt{d_2}, \sqrt{d_1 d_2}$

$$\theta = m + n\sqrt{d_1} + k\sqrt{d_2} + l\sqrt{d_1 d_2} \quad \text{נכתוב}$$

כאשר $(m, n, k, l) \in \mathbb{Z}$

טענה: הפולינום הטינטי של Θ מ $Z[x]$

(2)

הוכחה: ראינו שיהיה (שלבטים עובדי) אנוח את הפולינום הטינטי של איבר

ההסונות הטריצט העתקי (יכל) טאיט

$$\begin{pmatrix} m & md_1 & kd_2 & ldd_2 \\ n & m & lda & kd_2 \\ k & ld_1 & m & nd_1 \\ l & k & n & m \end{pmatrix}$$

טריצט העתקי (יכל) ה- Θ

ל-ה רכסיס שטפאנו

העמודות לרה התנוות של רכסיס לבי רכסיס

Θ מקיים את אוננו יודעים שלפולינום הוטינטי של הטריצט

(יכל) ינום הוטינטי הוא מתקן מטולה μ

m_Θ מטולה μ לכן הפולינום הוטינטי = m_Θ

$$m_\Theta \in Z[x]$$

מה אוננו יודעים על $|F_p(\sqrt{d_1}, \sqrt{d_2})| / F_p$?

$$2 \geq |F_p(\sqrt{d_1}, \sqrt{d_2}) : F_p| \quad (1)$$

$$\text{לכן } |F_p(\sqrt{d_1}, \sqrt{d_2}) : F_p| \leq 2 \Rightarrow \bar{\Theta} = \bar{m} + n\sqrt{d_1} + k\sqrt{d_2} + l\sqrt{d_1d_2} \in F_p \quad (2)$$

$$\bar{m}_\Theta(\bar{\Theta}) = 0 \quad \text{אנו יודעים כי } \bar{\Theta} \text{ מקיים את } \bar{m}_\Theta \text{ לוננו}$$

$$m_\Theta(\Theta) = 0 \quad \text{כי}$$

לכן אם \bar{m}_Θ היה אי-סריק אז כל שרש שלו היה יופי רכחנה מספר μ ,

אבל $\bar{\Theta}$ יופי רכחנה מספר לכל היותר 2, לכן \bar{m}_Θ סריק מטל F_p .

שתי הערות לידע כללי:

* תכיל (קלטה): רכחנה $\beta_1, \beta_2, \beta_3, \dots, \beta_n$ עבור \mathbb{C} רכחנה $\beta_1, \beta_2, \dots, \beta_n$ של $Q(\sqrt{p_1}, \dots, \sqrt{p_n})$

* הערת מסב: (אנוני העם)

jmilne.org
 יו טריצט העתקי
 כחמו

היום מתחיל מרחיב (יונתן)

לפתור היום בעיקר תחילת מסמך: 8:

(3)

נתון: יהי $K = \mathbb{Q}(\sqrt[8]{2})$ שדה הפולינום \mathbb{Q}

$$G = \text{Gal}(K/\mathbb{Q})$$

צריך למצוא את כל הרכיבות הביניים $\mathbb{Q} \subseteq M \subseteq K$ כך ש M/\mathbb{Q} הרכיבה (נונתה).

פתרון: מתורת אדמה אנו יודעים כי M/\mathbb{Q} הרכיבה (נונתה) אם ורק אם

$$G = \text{Gal}(K/\mathbb{Q}) \triangleright \text{Gal}(K/M)$$

לכן נרצה למצוא את תתי החבורות העונות של G .

השנוטים: $\epsilon_8 = e^{\frac{2\pi i}{8}}$ $\epsilon_8^k \sqrt[8]{2}$ $\chi^2 - 2$ $k=0,1,\dots,7$

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

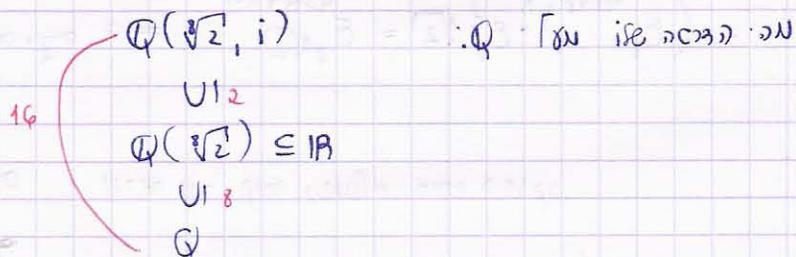
$$2x^2 = 1 \implies x = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$$

$$\implies \epsilon_8 = \sqrt{2} \left(\frac{1}{2} + i \frac{1}{2} \right)$$

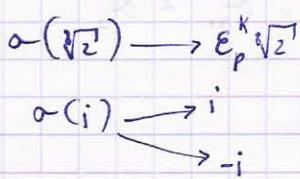
לכן יש לנו 8 שנוטים, ושדה הפולינום הוא:

$$K = \mathbb{Q}(\sqrt[8]{2}, \epsilon_8^7 \sqrt[8]{2}) = \mathbb{Q}(\sqrt[8]{2}, \epsilon_8) =$$

$$= \mathbb{Q}(\sqrt[8]{2}, i)$$



$$|\text{Gal}(K/\mathbb{Q})| = 16$$



אם $\sigma \in G$ אז

יש לך קבוצת 16 אוטומופיזמים וחסר לך אחד מהאפשרויות האלו

ת"ק של קבוצת אוטומופיזמים.

$$\sigma_k(\sqrt{2}) = \epsilon_8^k \sqrt{2}$$

(סטן ב')

$$\sigma_k(i) = i$$

(סטן ג) - את ההצגה הנמוכטת:

$$\gamma(\sqrt{2}) = \sqrt{2}$$

$$\gamma(i) = -i$$

$$G = \{ \sigma_k, \sigma_k \tau \mid k=0,1,\dots,7 \}$$

מהו σ_k מהו τ מהו ϵ_8 מהו $\sqrt{2}$

$$\sigma_k(\epsilon_8) = ?$$

$$\sigma_k(\epsilon_8) = \sigma_k(\sqrt{2}) \cdot \left(\frac{1}{2} + i\frac{1}{2}\right) \leftarrow =$$

$$\left(\sigma_k(\sqrt{2})\right)^4 = \left(\epsilon_8^k \sqrt{2}\right)^4 = \epsilon_8^{4k} \cdot \sqrt{2}$$

המשך

$$= \sigma_k(\epsilon_8) = \epsilon_8^{4k} \underbrace{\sqrt{2} \left(\frac{1}{2} + i\frac{1}{2}\right)}_{\epsilon_8} = \epsilon_8^{4k+1}$$

$$\sigma_k \cdot \sigma_k(i) = i$$

$$\sigma_l \cdot \sigma_k(\sqrt{2}) = \sigma_l(\epsilon_8^k \sqrt{2})$$

מהו σ_l מהו σ_k מהו ϵ_8 מהו $\sqrt{2}$

$$\left(\sigma_l(\epsilon_8)\right)^k \cdot \epsilon_8^k \cdot \sqrt{2} =$$

$$= \left(\epsilon_8^{4l+1}\right)^k \cdot \epsilon_8^k \sqrt{2} = \epsilon_8^{4lk+k+l} \Rightarrow \sigma_l \cdot \sigma_k = \sigma_{(4lk+l+k) \bmod 8}$$

ונראי מה קורה בטבלים אחת בתוספת:

$$\sigma_1 = \alpha$$

$$\alpha^2 = \sigma_1 \cdot \sigma_1 = \sigma_{4+1+1} = \sigma_6$$

$$\alpha_6 = \alpha^2$$

$$\alpha_7 = \alpha^3$$

$$\alpha^3 = \alpha^2 \cdot \alpha = \sigma_6 \cdot \alpha = \sigma_{24+6+1} = \sigma_{31} = \alpha_7$$

$$\alpha_4 = \alpha^4$$

$$\alpha_5 = \alpha^5$$

$$\alpha_2 = \alpha^6$$

$$\alpha_3 = \alpha^7$$

$$1 = \alpha^8$$

$$\langle \alpha \rangle \cong \mathbb{Z}/8\mathbb{Z}$$

$$\langle \alpha_1, \alpha_2, \dots, \alpha_{r-1}, 1 \rangle$$

כמוכן כל אקטוריה ציקלית יש תת-רכיב יחידה של σ (מחלק חזקה):

ה $\langle \alpha \rangle$ יש שתי תתי-רכיבות לא סכימאיות

$$\langle \alpha^2 \rangle \cong \mathbb{Z}/4\mathbb{Z} \quad \langle \alpha^4 \rangle \cong \mathbb{Z}/2\mathbb{Z} !$$

מכאן, כל רכיבה של $G = \text{Gal}(K/\mathbb{Q})$ היא חזקה ב-2

קודם כל משערה אותה טקוס כי היא נרמלת לפני שהיא חזקה

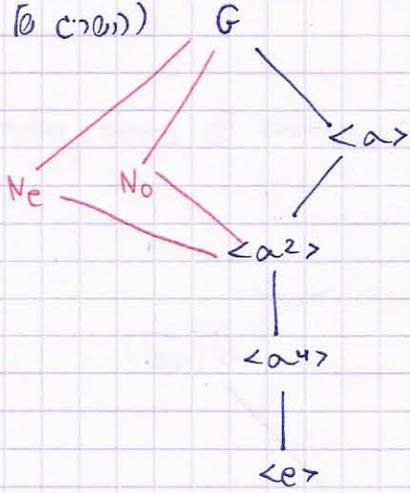
כיח

וכן נמשיר אם את $\langle \alpha^2 \rangle$ ו- $\langle \alpha^4 \rangle$ טקוס.

$$\langle \alpha^2 \rangle \triangleleft G \quad \langle \alpha^4 \rangle \triangleleft G$$

(הוכחה של תתי-רכיבות נרמלות)

מה שמתקבל
היות הרכיב של
תתי-רכיבות
(תת-רכיבות)



יהי $N \triangleleft G$ כך ש: $N \not\triangleleft \langle \alpha \rangle$ $N \triangleleft \langle \alpha^2 \rangle$ $N \triangleleft \langle \alpha^4 \rangle$ $N \triangleleft \langle e \rangle$

קודם צריך להבין מהו σ ומתחיל עם τ

$$-k = 1 \pmod{8}$$

$$\Rightarrow k = 7$$

$$\sigma_7 = \alpha^3$$

$$\begin{cases} \sigma \tau(i) = \sigma(-i) = -\sigma(i) = -i \\ \sigma \tau(\sqrt{2}) = \sigma(\sqrt{2}) = \epsilon_8^7 \sqrt{2} \\ \sigma \sigma_k(i) = -i \\ \sigma \sigma_k(\sqrt{2}) = \tau \epsilon_8^k \sqrt{2} = \epsilon_8^{-k} \sqrt{2} \end{cases}$$

$$\Rightarrow \sigma \tau = \tau \alpha^3$$

$$\tau \alpha = \alpha^3 \tau$$

מתחילים מחזרות נימך אכתוב את G :

$$G = \{ \alpha, \tau \mid \alpha^8 = 1, \tau^2 = 1, \alpha \tau = \tau \alpha^3 \}$$

$$N \ni \alpha^7 \alpha^k \tau \alpha =$$

נימך אכתוב אלקסל:

$$= a^7 a^k a^3 \tau = a^{k+2} \tau$$

$$\Rightarrow \left\{ a^k \tau, a^{k+2} \tau, a^{k+4} \tau, a^{k+6} \tau \right\}$$

$$\Rightarrow \left\{ 1, a^2, a^4, a^6 \right\}$$

$\in \mathbb{N}$

מס K מסוים SM נתון \mathbb{N} : מס :

$$\mathbb{N}_0 \{ \tau, a^2 \tau, a^4 \tau, a^6 \tau, 1, a^2, a^4, a^6 \}$$

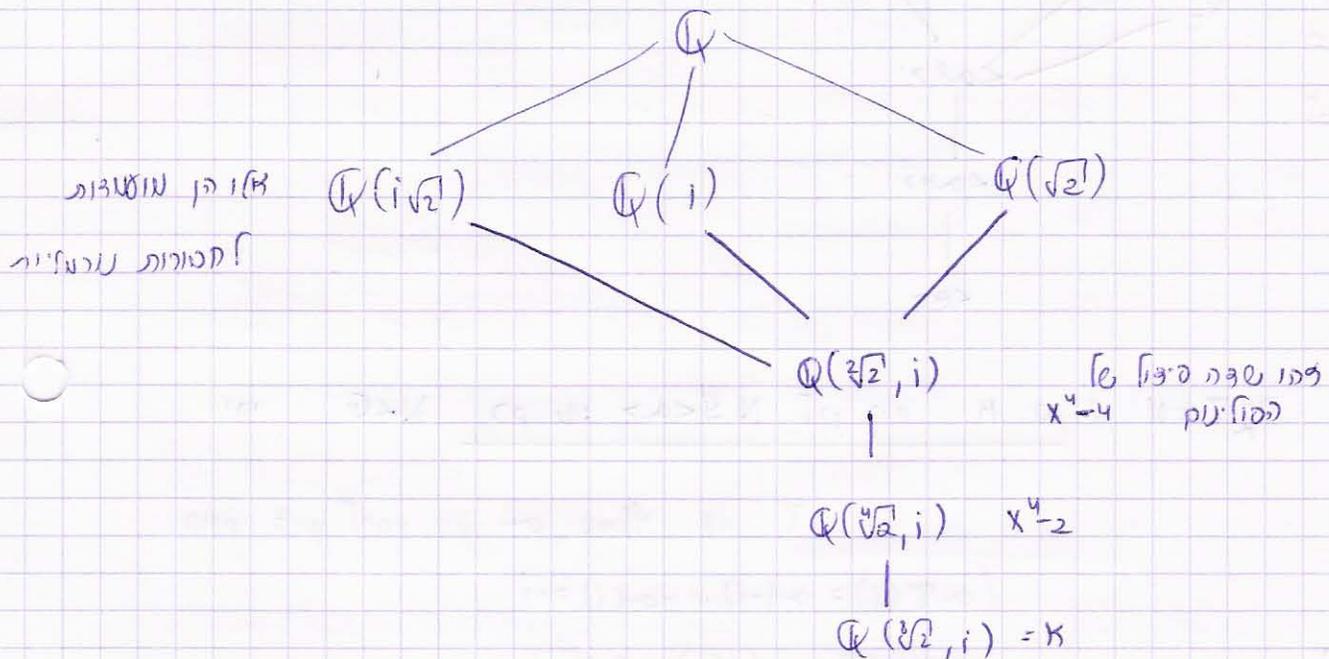
(even)

מס K מסוים SM :

$$\mathbb{N}_0 \{ a \tau, a^3 \tau, a^5 \tau, a^7 \tau, 1, a^2, a^4, a^6 \}$$

(odd)

נתון מסים של הרחבות הנוצרות:



מסכים אמצעיים - תבואה מס' 11 (אחרון)

נכונות היחס אחר שאלות 1 ו-2 מתקיימים 9

\bar{F}/F - מסך אמצעי K/F הרחבה אמצעית סופית.

$$i/F = id$$

סימון: $i_{K/F} =$ מסך היסודות הנאכסרים.

$$[K:F] = n$$

שאלה 1

(*) F - K יש לה היות n , F -שיכונים לתוך \bar{F}

$$i_{K/F} \leq [K:F]$$

הוכחה: האינדוקציה על מסך היוצרים של K/F $K = F(\alpha_1, \dots, \alpha_r)$

נתחיל עבור $r=1$

הצרכים: אם $K = F(\alpha)$ מס' השיכונים הנ"ל הוא בזיוק מסך השורשים הפולינום

$$K \cong F[x]/m_\alpha \quad \text{המינימלי של } \alpha \text{ מעל } F$$

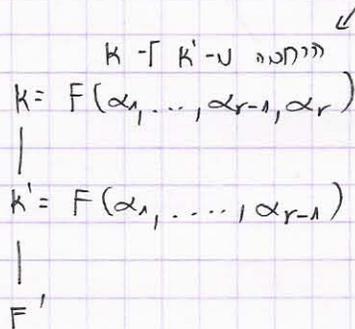
← המתקנה $r=1$ נכונה

כי מסך השורשים של $[K:F] \geq m_\alpha$ שיוויון $\iff \alpha$ ספרטי.

שלב האינדוקציה: $K = F(\alpha_1, \dots, \alpha_r)$ ונניח את הטענה ע"י $r-1$

$K' = F(\alpha_1, \dots, \alpha_{r-1})$ $i_{K'/F} < [K':F]$ מס' השיכונים מעל (המסך האמצעי של F).

$$K = K'(\alpha) \quad i_{K/F} = [K:F] \quad \text{תעניין נ:}$$



מסך הנבנים ארוחים ה שיכון של K'/F ה F'/F הוא בזיוק מסך השורשים

הישונים של הפולינום המינימלי של α_r מעל K' .

$$[K:K'] \leq [K':F] \leftarrow \text{שיכון של } K' \text{ על } K'$$

← מסכיות

$$i_{K/F} = i_{K'/F} \cdot i_{K/K'} \leq$$

$$\leq [K:K'] [K':F] = [K:F]$$

$$[K:F] = n$$

(כ)

$$iK/F = n \quad (1)$$

(1)

↑

(2) K נפרד מעל F ו' איברים סגורים $\iff K/F$ סגורה

(3) \iff כיוון זה נכון

(2) \iff (1) נכון מוכחת א' ראינו עם נוסף α ראשון \iff

ואם נוסף α שני \iff

(1) \iff (3) נניח K/F לא סגורה קיים α לא סגור (רחיב את α

$$K = F(\alpha_1, \alpha_2, \dots, \alpha_r) \quad K/F \text{ גרסיס}$$

$$[F(\alpha):F] < [K:F]$$

$$iK/F(\alpha) \leq [K:F(\alpha)]$$

\leftarrow מכפלות וקטן אי-שיוויון טעם.

(ג) K/F נרמלת \iff לכל α שכינים כל σ_1, σ_2 מתקיים $\sigma_1(\alpha) = \sigma_2(\alpha)$

הוכחה: נרמלות $\iff K/F$ שפה פשוט של אינברס פוליומ $F \iff f$ (יש לו קיום

אם לא) מתכנן סל תמונה \bar{K}/F \iff K/F ש' א מתוק \bar{F}

(אם קורה σ -א קורה סל תמונה) \iff כל תמונה ש' א תחת

$$F \left(\begin{matrix} f \\ \bar{F} \end{matrix} \right) \text{ ש' אינברס פוליומ}$$

אזו צוקא סוכיות, מצטבריות.

$$\left\{ \begin{array}{l} K/F \text{ סכטילי} \\ M/K \text{ סכטילי} \end{array} \right.$$

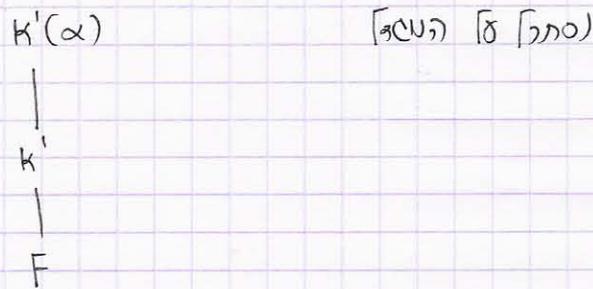
M/F סכטילי \Leftarrow

הוכחה: $\alpha \in M$, $\beta \in \mathbb{Z}$ סכטילי.

סכטן α סכטילי α סכטילי M_α את הכולנים הטייטלי של α סכטילי K

$$m_\alpha = \sum_{j=0}^n a_j x^j$$

סכטן α - K' את השדה $F(\alpha_1, \dots, \alpha_n)$



אפי סכטילי 1 α סכטילי אוראות של $[K'(\alpha):F]$

כל שייכין של K/F α סכטילי F/F ניתן להוכחה אפי סכטילי של $K'(\alpha)/F$

מאכר השורשים של הכולנים הטייטלי של α סכטילי K' פריים (אם α סכטילי סכטילי K)

אז α -סכטילי סכטילי K' = סכטילי השורשים של m_α

אפי סכטילי 1 סכטילי סכטילי $[K':F]$

סכטילי השורשים של $m_\alpha \iff [K'(\alpha):K] = m_\alpha$

שייכין α סכטילי סכטילי K