מבנים אלגבריים 2 - שיעור מס' 1

מרצה: פרופ' אהוד דה-שליט
חדר 102 בנין איינשטיין
email: deshalit@math.huji.ac.il
שעת קבלה: יום א' שעה 12:00

מתרגל: אורי שפירא, ימים א' ו-ג'.

חובת הגשה של תרגילים, 70% של התרגילים.

ספר הקורס: Ian Stewart / Galois Theory

(בנוסף כל ספר בנושא Field / Galois Theory)

הסמסטר נתעסק במבנים האלגבריים הבאים: **שדות** ו-**חוגים** כאשר הדגש יהיה על שדות.

נחפש פתרונות למשוואות פולינומיאליות, בעולם, שלפעמים הוא לא מספיק עשיר.

נרצה לדעת מתי יש פתרונות, כמה יש, מה המבנה שלהם ואיך מרחיבים אוסף מסוים של מספרים על מנת לקבל יותר פתרונות.

בקורס נעסוק במתמטיקה של המאה ה-19 שקשורה בעיקר לאבל (Abel) וגלואה (Galois).

בהקדמה לספר יש את סיפור חייו של גלואה, שמת בגיל מאוד צעיר בדו-קרב.

עתה ניגש לחומר עצמו.

חוגים

(פרקים I,II בספר של סטיוארט וגם בספר אלגברה א' של טיגנר)

חוג - זה קבוצת איברים R עם שתי פעולות $\cdot$, $+$ דו-מקומיות ועם שני איברים מיוחדים $0, 1$ (שונים זה מזה) שמקיימת את האקסיומות הבאות:

- $x+(y+z)=(x+y)+z$
- $x+y=y+x$
- $x+0=x$
- לכל x קיים איבר שסימונו $(-x)$ כך ש $x+(-x)=0$

ניתן לומר בקצרה כי $(R,+)$ = חבורה קומוטטיבית.

כמו כן מתקיים

- $x(y\cdot z)=(x\cdot y)\cdot z$
- $x\cdot 1=1\cdot x=x$
- $x(y+z)=xy+xz$
- $(y+z)\cdot x=yx+z\cdot x$

חוג קומוטטיבי: אם בנוסף $x\cdot y = yx$ (בנוסף לדרישות הקודמות)

שדה: חוג קומוטטיבי כך שלכל $x\neq 0$ קיים x' (הפכי) כך ש: $x\cdot x'=1$

כמה דוגמאות:

שדות:

- $\mathbb{Q} = \{\frac{n}{m},\ n,m\in\mathbb{Z}\}$
- $\mathbb{R}$
- $\mathbb{C}$
- לכל ראשוני p חוג השאריות מודולו p:

$$\{\bar{0},\bar{1},\dots,\overline{p-1}\} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

עם חיבור וכפל של שאריות מהווה **שדה**.

הוכחה: אסוציאטיביות ודיסטריביוטיביות של כפל וחיבור נובעים מהתכונות המקבילות ב-$\mathbb{Z}$

קיום נגדי: $\bar{a}+\overline{p-a}=\bar{0}$

נותרת הטענה של קיום הפכי בכפל:

נסתכל על $\bar{a}\neq 0$ ובכפולותיו:

$$\bar{a}\cdot\bar{1},\ \bar{a}\cdot\bar{2},\dots\ \bar{a}\cdot\overline{p-1}$$

נטען כי כולן שונות:

אם $\bar{a}\cdot\bar{x}=\bar{a}\cdot\bar{y}$

$$\bar{a}(\bar{x}-\bar{y})=0$$

$$\Downarrow$$

$$p\,|\,a(x-y)=0$$

$p|x-y \Leftarrow$ ראשוני $= p\nmid a$

$\Leftarrow$ $\bar{x}=\bar{y}$ (כי $a\neq 0 \Leftarrow x-y=0$)

ומכאן שיש b כך ש: $\bar{a}\cdot\bar{b}=1$ (עקרון שובך היונים)

26-2-2007

דוגמאות לחוגים שאינם שדות:

חוגים קומוטטיביים שאינם שדות:

תחומי שלמות }
- $\mathbb{Z}$
- $\mathbb{R}[x]$ = חוג הפולינומים מעל הממשיים

ל-2 אין הפכי ב-$\mathbb{Z}$ ול-x אין הפכי ב-$\mathbb{R}[x]$ ולכן אלו אינם שדות.

- $\mathbb{Z}/n\mathbb{Z}$ n=כלשהו

הטענה היא שאם n אינו ראשוני זהו אינו שדה.

טענה: אם n אינו ראשוני אזי $\mathbb{Z}/n\mathbb{Z}$ אינו שדה.

הוכחה: n לא ראשוני $\Leftarrow$ יש פירוק $n = a \cdot b$ כאשר $n > a, b > 1$

כמו כן: $\bar{0} = \bar{a} \cdot \bar{b}$ $\bar{a}, \bar{b}$ שונה מאפס ולכן קיבלנו

שני איברים שונים מאפס שמכפלתם אפס.

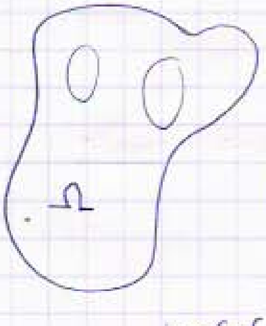
בשדה $x, y \neq 0 \Leftarrow x \cdot y \neq 0$ כי אחרת $x \cdot y = 0$

$y = x' x \cdot y = x' 0 = 0$

אבל ב-$\mathbb{Z}/n\mathbb{Z}$ (n פריק) יש מחלקי אפס ($x \neq 0$, $y \neq 0$ רק ש: $x \cdot y = 0$)

ולכן זהו אינו שדה.

הגדרה: חוג קומוטטיבי R כך ש $x \neq 0, y \neq 0 \Rightarrow xy \neq 0$ נקרא תחום שלמות (Domain)



Ω - תחום (קב' פתוחה וקשירה) במישור המרוכב

$O(\Omega)$ = אוסף הפונקציות האנליטיות ב-Ω עם חיבור וכפל רגיל

זהו חוג. המבנה האלגברי מאפיין את התחום Ω עד כדי

שקילות קונפורמית (זה רק לידע כללי - כדי להראות קשר בין אלגברה לאנליזה)

חוגים לא קומוטטיביים שאינם שדות:

- $M_n(\mathbb{R})$ חוג המטריצות מעל הממשיים.
- $\mathbb{H}$ חוג הקווטרניונים של המילטון.

$\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$

$\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$

$\boxed{ij = k}$

ניתן לעשות כפל לפי נוסחא של הקומוטטיביות

• אם R חוג קומוטטיבי או לא קומוטטיבי, אבל יש בו 1, נסמן

$$R^* = \{u \in R \mid \exists v \in R \text{ כך ש: } u\cdot v = v\cdot u = 1\}$$

(כל אלה שיש להם הפכי משני הצדדים)
(כי לא מניחים קומוטטיביות)

קל לבדוק כי R^* היא חבורה = חבורת היחידות (units) של R.

ובצורה כזו, מתוך כל חוג ניתן לקבל חבורה כפלית.

דוגמא • $\mathbb{Z}^* = \{\pm 1\}$ • $F^* = F - \{0\}$, F שדה.

• $\mathbb{R}^* = \mathbb{R}[x]^*$

• $M_n(\mathbb{R})^* = GL_n(\mathbb{R})$ חבורת המטריצות ההפיכות

• תרגיל: לחשב את היחידות ב $(\mathbb{Z}/n\mathbb{Z})^* = ??$

נכניס עכשיו כמה מושגים:

תת-חוג $S \subset R$ בפרט $0,1 \in S$ והפעולות ב S הן הפעולות של R
(חוג "ירושה" מ-R)

די להראות: $x,y \in S \Leftarrow x \pm y \in S$, $xy \in S$ ואז כל האקסיומות יתקיימו ויתקיים סגירות תחת הפעולות.

תת-שדה (אותו הדבר רק שמדובר בשדה) צריך לבדוק גם
$x \neq 0 \Leftarrow \frac{1}{x} = x^{-1} \in S$

הגדרה: הומומורפיזם של חוגים (או שדות) הינו העתקה

$$\varphi: S \longrightarrow R$$

כך ש:

$$\varphi(0) = 0$$
$$\varphi(1) = 1$$
$$\varphi(x+y) = \varphi(x) + \varphi(y)$$
$$\varphi(x\cdot y) = \varphi(x)\cdot\varphi(y)$$

נסמן, כמו בתורת החבורות: $\{a \in R \mid \varphi(a) = 0\} = Ker\varphi$

הגרעין הוא תת חבורה חיבורית: $a,b \in Ker\varphi \Longrightarrow a \pm b \in Ker\varphi$

כמו כן מתקיים:

$\varphi(ax)=\varphi(a)\varphi(x)=0$ $\quad x\in R \quad , a\in Ker\,\varphi$

$\varphi(xa)=\varphi(x)\varphi(a)=0$ (כי לא הנחנו קומוטטיביות)

$$\Downarrow$$

$$\left.\begin{matrix} xa \\ ax \end{matrix}\right\} \in Ker\,\varphi$$

הגדרה: אידיאל בחוג R הינו קבוצה חלקית $I \subsetneq R$ כך ש:

$$a,b\in I \Longrightarrow a\pm b\in I$$

$$a\in I,\ x\in R \Longrightarrow \left.\begin{matrix} ax \\ xa \end{matrix}\right\} \in I$$

$I = Ker\,\varphi$ הגרעין הינו אידיאל

הערות: $1\notin I$ ולכן I אינו תת-חוג (כי לפי הגדרתנו תת-חוג מכיל את 1 ואם האידיאל יכיל את 1 הוא יכיל את כל איברי החוג והנחנו הרגע ש $I \subsetneq R$)

דוגמאות:

$$(n) = n\mathbb{Z} = \{n\cdot x \mid x\in\mathbb{Z}\} \qquad (1<n)$$

אלו הם כל האידיאלים כי אלו הן כל החבורות.

∞

אם R קומוטטיבי נסמן ב- $(a)=a\cdot R$ את אוסף כל הכפולות של a

מתקיים:
$$(a\cdot x)y = a(xy)$$
$$ax\pm ay = a(x\pm y)$$

$R=(a) \Longleftrightarrow$ קיים b כך ש $ab=1$

$$a(bx)=x \quad \forall x\in R$$

ולכן אם a אינו הפיך, כלומר $a\notin R^*$ אזי (a) אידיאל של R.

סימון נוסף: (תזכורת: R עתה קומוטטיבי עם יחידה)

אם $a_1,\dots,a_n \in R$ (סמן ב- $(a_1,\dots,a_n) = a_1R + \dots + a_nR =$

$$= \{a_1b_1 + a_2b_2 + \dots + a_nb_n \mid b_i \in R\}$$

אז יש שתי אפשרויות: $I = (a_1,\dots,a_n)$ הינו אידיאל או כל החוג.

זהו **האידיאל הנוצר** ע"י $(a_1,\dots,a_n)$.

אידיאל שנוצר ע"י איבר אחד נקרא **אידיאל ראשי**.

(חוג בו כל האידיאלים הם אידיאלים ראשיים הוא חוג ראשי. והנה הגדרה מדויקת:)

הגדרה: תחום שלמות (חוג קומוטטיבי ללא מחלקי אפס) יקרא **חוג ראשי** אם כל אידיאל שלו הינו ראשי.

דוגמאות:

1) $\mathbb{Z}$ חוג ראשי.

2) $\mathbb{R}[x,y]$ = חוג הפולינומים בשני משתנים **אינו** חוג ראשי

כי: אם ניקח את האידיאל $I = (x,y)$

ונתבונן בהומומורפיזם $\varphi: \mathbb{R}[x,y] \longrightarrow \mathbb{R}$

כך ש: $\varphi(f) = f(0,0)$ (לוקחים פולינום וערך שלו בראשית)

$$\varphi(f \pm g) = (f \pm g)(0,0) = \varphi(f) \pm \varphi(g)$$

נטען כי I הוא הגרעין שלו: $I = \ker\varphi$

כי הפולינום שלי הוא:

$$f = \sum c_{ij} x^i y^j$$

$\varphi(f) = f(0,0) = c_{0,0}$ (האיבר החופשי של הפולינום)

בדרך הבאה ניתן לראות כי:

$$x^2y^3 = x(xy^2) = y(x^2y^2)$$

תרגיל: $I = (x,y) \overset{?}{\neq} (f)$ (רמז: שיקולי דרגה)

לכן זהו לא חוג ראשי.

משפט: יהי F שדה, חוג הפולינומים $F[x]$ הינו חוג ראשי.

הוכחה: נסתמך על קיום אלגוריתם אוקלידי או על קיום חילוק עם שארית.

בהינתן $f,g\neq 0$ ב $F[x]$ קיימת הצגה יחידה $f=h\cdot g+r$

כאשר $\deg(r)<\deg(g)$ או $r=0$.

דוגמא לחלוקת פולינומים:

$$\begin{array}{l|l} \multicolumn{1}{l}{x+1} & \\ \hline x^3+x^2-x+1 & x^2+5 \\ x^3+\quad 5x & \\ \hline x^2-6x+1 & \\ x^2\quad +5 & \\ \hline -6x-4 & \end{array}$$

(כפלים כמה שמחלקים)

די כבר שארית כי דרגתה קטנה מדרגת המחלק.

$$x^3+x^2-x+1=\underbrace{(x+1)}_{h}\underbrace{(x^2+5)}_{g}+\underbrace{(-6x-4)}_{r}$$

הוכחת המשפט: יהיה I אידיאל. אם $I\neq 0$. נבחר ב I פולינום מדרגה קטנה ביותר, נסמנו g.

ברור שכל הכפולות של g מוכלות באידיאל $(g)\subseteq I$ (הערה: ההצגה יחידה כי אם
$f=h_1g+r_1$
$f=h_2g+r_2$
$(h_2-h_1)g=r_2-r_1$
($\deg\geq\deg g$ $\deg<\deg g$)

מאידך, אם $f\in I$ נבצע חילוק עם שארית $f=h\cdot g+r$

$\Rightarrow r=\underbrace{f}_{\in I}-\underbrace{hg}_{\in I}\in I$ (עפ"י ההנחה)

אם $r\neq 0$ אז $\deg r<\deg g$ או $r=0$.

$r\neq 0\Rightarrow$ יש פולינום ב-I מדרגה קטנה מדרגת g, סתירה לבחירת g.

לכן $r=0$, $f=h\cdot g\Rightarrow f\in(g)$

ולכן האידיאל ראשי $(g)=I$

■

27-2-2007

חוגים ואלגברות 2 - שיעור מס' 2

B חוג קומוטטיבי

I אידיאל

$$(0) \subseteq I \subsetneq B$$

$$\left.\begin{matrix} a,b \in I \\ x \in B \end{matrix}\right\} \Rightarrow \begin{matrix} a \pm b \in I \\ xa \in I \end{matrix}$$

$$(a) = a \cdot B$$

אידיאל ראשי (בתנאי $a \notin B^*$)

הערה: שדה מאופיין כחוג קומוטטיבי שהאידיאל היחידי בו הינו אידיאל האפס (0) (כי בשדה כל איבר אחר הוא הפיך)

מאידך אם יש חוג שיש בו איבר שאינו הפיך להשלים את ההערה:

הערה: אחת הדרכים לקבל אידיאל היא כגרעין של הומומורפיזם.

$\varphi: B \to S$ הומומורפיזם $I = \ker\varphi$ הינו אידיאל.

הגדרה: בהינתן $I \subset B$ נבנה את חוג המנה B/I כך: איבריו

$$\bar{a} = a + I = \{a+m \mid m \in I\}$$

החיבור והכפל נעשים ע"י נציגים

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

$$\bar{0} = 0$$

$$\bar{1} = 1$$

$m,n \in I \qquad (a+m)(b+n) = ab + \underbrace{mb + an + mn}_{I}$

הגדרנו את תכונות המנה ולכן ניתן לדבר על ההומומורפיזם הקנוני

$$\psi: R \longrightarrow R/I$$

$$\psi(a) = \bar{a}$$

$$Ker\psi = I$$ (כל האיברים שמתלקחים נמחקת לאפס)

משפט ההומומורפיזם הראשון: (לא נוכיח כי ההוכחה מדויק כמו בחבורות)

יהי $\varphi: R \to S$ הומומורפיזם של חוגים, אזי $Im\varphi$ הינה תת-חוג של S.

! φ משרה איזומורפיזם טבעי:

$$\bar{\varphi}: R/Ker\varphi \simeq Im\varphi$$

$$\bar{\varphi}(\bar{a}) = \varphi(a)$$

כמה סימונים:

הומומורפיזם שהוא חח"ע נקרא מונומורפיזם או שיכון (embedding)

" " על נקרא אפימורפיזם

" " חח"ע ועל נקרא איזומורפיזם (ואז ניתן לדבר על האיזומורפיזם ההפיך)

∞

- נניח $\varphi: F \to K$ הוא הומומורפיזם של שדות

אז הוא חח"ע תמיד (כי הגרעין הוא אידיאל היחיד שהוא אידיאל האפס)

ולכן נובע שההומומורפיזם תהיה חח"ע). $(Ker\varphi = 0)$

- יהיו שלושה חוגים ושני הומומורפיזמים:

$$R \xrightarrow{\varphi} S \xrightarrow{\psi} T \qquad \varphi \circ \psi$$

אז ההרכבה היא גם הומומורפיזם

בין R ל-T

הגדרה: אידיאל מקסימלי בחוג R הינו אידיאל M שאינו מוכל בשום אידיאל גדול יותר.

דוגמה: (2) (5)

$(10) \subset (2),\ (10) \subset (5)$

טענה: R/M שדה $\Longleftrightarrow$ M מקסימלי.

הוכחה: R/M שדה $\Longleftarrow$

נניח בשלילה כי M אינו מקסימלי.

אז יהיה $M \subsetneq I$ $\Leftarrow$ קיים $a\in I$, $a\notin M$ כלומר $\bar a \neq \bar 0$ ולכן יש לו הפכי:

$\bar a \bar b = 1$ (כי חוג המנה הוא שדה) $\Leftarrow$ $\bar a\cdot\bar b - 1 \in M \subset I$ מוכל אם $ab\in I$ ע"פ ההנחה

ואם נחסר ביניהם (כי יש סגירות תחת חיבור/חיסור) נקבל $1\in I$ - וזו סתירה.

בכיוון השני: נניח כי M מקסימלי וניקח $\bar R \ni \bar a \neq \bar 0$

צ"ל $\bar a$ הפיך. $I = M + Ra \supsetneq M$

ממקסימליות M, $I = R$ $\Leftarrow$ בפרט 1 יכול להכתב: $1 = m + ra$ כאשר $m\in M$, $r\in R$

ואם נשים לב ש- $\bar 1 = \bar r\cdot \bar a$ ומצאנו הפכי ל- a.

▨

אידיאל מסוג קצת שונה הוא אידיאל ראשוני.

הגדרה: P יקרא אידיאל ראשוני אם לכל $a,b\in R$

$$a\cdot b\in P \rightarrow a\in P \text{ או } b\in P$$

דוגמה: (6) אינו ראשוני כי $2\cdot 3\in(6)$ $2\notin(6)$ $3\notin(6)$

טענה: R/P תחום שלמות $\Longleftrightarrow$ P ראשוני

הוכחה: נניח R/P תחום שלמות אז:

$\bar a\cdot\bar b = 0 \Rightarrow \bar a = \bar 0$ או $\bar b = \bar 0$

$\Updownarrow$ מה שקול

$ab\in P \Rightarrow a\in P$ או $b\in P$ וזו בדיוק ההגדרה.

מסקנה עיקרית: M מקסימלי $\Longrightarrow$ M ראשוני

הוכחה:

$$\begin{array}{ccc} M \text{ maximal} & \Longrightarrow & M \text{ prime} \\ \Updownarrow & & \Updownarrow \\ R/M \text{ field} & \Longrightarrow & R/M \text{ integral domain} \end{array}$$

R/M שדה $\Longrightarrow$ R/M תחום שלמות

דוגמאות: (x) ב- $\mathbb{R}[x,y]$ חוג פולינומים בשני משתנים

נתבונן בהומומורפיזם

$$\varphi : \mathbb{R}[x,y] \longrightarrow \mathbb{R}[y]$$

$$\varphi(f) = f(0,y)$$

נראה כי $\ker\varphi = (x)$ (כל הכפולות של x) (תרגיל)

$$\operatorname{Im}\varphi = \mathbb{R}[y]$$

$$\Longleftarrow \quad \mathbb{R}[x,y]/(x) \cong \mathbb{R}[y]$$

זהו תחום שלמות שאינו שדה.

מכאן (x) ראשוני אך לא מקסימלי. ואכן הוא מוכל באידיאל גדול יותר:

$$(x) \subsetneq (x,y)$$

ב- $\mathbb{R}[x]$: (0) ראשוני (לא) מקסימלי.

$$(0) \subsetneq (x)$$

(x^2+1) הוא ראשוני ומקסימלי

מעתה, נעסוק רק בחוגים ראשיים בהם המושג אידיאל ראשוני ואידיאל מקסימלי הם חופפים פרט למקרה של האידיאל ה-(0) שהוא יוצא דופן.

פריקות בחוגים ראשיים

חוג R הינו ראשי אם כל אידיאל $I=(a)$ ראשי. (חוג ראשי הוא תמיד תחום שלמות קומוטטיבי)

דוגמאות:

$\mathbb{Z}$

$F[x]$ (F שדה)

בחוג ראשי $a|b$ (a מחלק את b) אם $b=a\cdot x$

$(x^3-1)=(x-1)(x^2+x+1)$

$12=4\cdot 3$

טענה: $a|b$ אם ורק אם $(b)\subseteq(a)$ (האידיאל הראשי הנוצר ע"י b מוכל בזה הנוצר ע"י a)

הוכחה: $b=ax \Leftarrow a|b$

$b\in(a)$

$(b)\subseteq(a)$

בכיוון השני:

$.b=ax \Leftarrow b\in(a) \Leftarrow (b)\subseteq(a)$

הגדרה: (נאמר כי) $a\sim b$ (a,b חברים) אם $a|b$ וגם $b|a$

כלומר אם האידיאלים שהם יוצרים שווים $(a)=(b)$

$b=ax$

$a=by$

נציב אחד בשני ונקבל:

$b=byx$

והיות ואנחנו בתחום שלמות נקבל:

$b(1-yx)=0$

$b\neq 0$ ולכן $x,y\in R^* \Leftarrow yx=1$ (איברים הפיכים)

6-3-2007

מבנים אלגבריים ב' - שעור מס' 3

(שחר עזב מחליף את אורי פה-שלם.)

המטרה היום להראות כי $\mathbb{C}$ שדה סגור אלגברית.

משפט: $\mathbb{C}$, שדה המספרים המרוכבים, הוא שדה סגור אלגברית.

(זהו המשפט היסודי של האלגברה)

הגדרה: שדה F יקרא שדה סגור אלגברית אם לכל פולינום $f(x)\in F[x]$ ממעלה ≥ 1 יש שורש $\alpha\in F$.

(כאשר $\alpha\in F$ שורש של $f\in F[x]$ אם $f(\alpha)=0$.)

$f\in F[x]$

$\alpha\in F$ שורש של f $\Longleftrightarrow$ $x-\alpha$ מחלק את f כלומר $f(x)=(x-\alpha)g(x)$ עבור איזשהו $g(x)\in F[x]$.

$f(x)\in F[x]$ ו- $\alpha\in F$. נחלק את $f(x)$ עם שארית ב- $(x-\alpha)$ ונקבל כי קיימים $g(x)\in F[x]$, $r(x)\in F[x]$ כך ש: $f(x)=(x-\alpha)\cdot g(x)+r(x)$ אז:

או $r(x)=0$ או $\deg(r(x))<\deg(x-\alpha)=1$ כלומר $\deg(r(x))=0$

כלומר $r(x)=\beta\in F$ ולכן מתקיים

$$f(x)=(x-\alpha)g(x)+\beta$$

נציב α ונקבל

$$f(\alpha)=(\alpha-\alpha)g(\alpha)+\beta=$$

$$=0g(\alpha)+\beta=\beta$$

טענה: F שדה סגור אלגברית אם ורק אם כל פולינום ממעלה ≥ 1 ניתן לפרוק כמכפלת פולינומים לינאריים. (תזכורת: פולינום לינארי $\Longleftrightarrow$ פולינום ממעלה 1)

<u>הוכחה</u>: ⟹ נניח כי $f(x)$ הוא פולינום ממעלה $d=\deg f\ge 1$

אז לפי ההנחה ניתן לרשום $f(x)=\prod_{i=1}^{d} g_i(x)$

כאשר לכל $1\le i\le d$ $\deg g_i(x)=1$

נתבונן ב $g_1(x)=ax+b$ כאשר $a,b\in F$

וברור כי עבור $\alpha=\frac{-b}{a}$ $g_1(\alpha)=0$

ולכן גם $f(\alpha)=\prod_{1}^{d} g_i(\alpha)=0$

בכיוון השני, נניח כי F שדה סגור אלגברית ונראה באינדוקציה כי כל פולינום $f\in F[x]$ ממעלה $1\le d$ הוא מכפלת d פולינומים לינאריים ב $F[x]$.

עבור $d=1$ ברור.

יהי $f\in F[x]$ ממעלה $1<d$ ונניח כי הוכחנו כבר את הטענה לפולינומים ממעלות קטנות מ-d וגדולות מ-1.

ל-f יש שורש $\alpha\in F$ כי F שדה סגור אלגברית ולכן f מתחלק ב- $x-\alpha$

$f(x)=(x-\alpha)g(x)$ $\deg g(x)=\deg f(x)-1=d-1$

ולכן לפי הנחת האינדוקציה $g(x)$ מתפרק למכפלת $d-1$ פולינומים לינאריים ב $F[x]$

∎

נעבור עתה להוכחת המשפט היסודי:

יהי $f(z)\in\mathbb{C}[z]$ ורוצים להראות כי קיים $w_0\in\mathbb{C}$ כך ש: $f(w_0)=0$

נרצה להראות כי: - ל $|f(z)|$ יש מינימום

- המינימום אינו יכול להיות >0

משני הדברים האלו תנבע הטענה שלנו.

ההוכחה בעמ' הבא:

תחילה נוכיח למה:

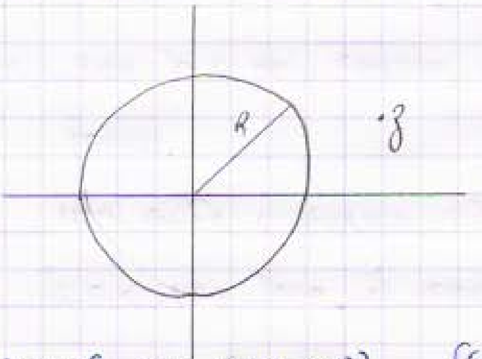
למה: יהי $f(z) \in \mathbb{C}[z]$ פולינום ממעלה ≥ 1

אזי יש $w \in \mathbb{C}$ כך ש $|f(z)|$ מקבל מינימום

כלומר יש $w \in \mathbb{C}$ כך שלכל $z \in \mathbb{C}$ $|f(w)| \leq |f(z)|$

הוכחת הלמה: קיים רדיוס R כך שלכל $z \in \mathbb{C}$ כך ש: $|z| > R$

$$|f(z)| > |f(0)|$$



נרשום את $f(z)$ באופן הבא:

$$f(z) = a_0 + a_1 z + a_2 z^2 + \dots + a_d z^d$$

כאשר $a_d \neq 0$! $d \geq 1$

אז ניתן לרשום:

$$f(z) = z^d(a_d + a_{d-1} z^{-1} + a_{d-2} z^{-2} + \dots + a_0 z^{-d}) =$$ (דרך כתיבה שונה לאותו הדבר)

$$= z^d(a_d + g(z^{-1}))$$

כאשר $g(u) = a_{d-1}u + a_{d-2}u^2 + \dots + a_0 u^d$ (וב- $g(u)$ נציב z^{-1})

ונשים לב ש $z \neq 0$ (ולכן ניתן לדבר על z^{-1}).

אז: $f(z) = z^d(a_d + g(z^{-1}))$

$$|f(z)| = |z|^d |a_d + g(z^{-1})| \geq |z|^d(|a_d| - |g(z^{-1})|)$$ (מי שוויון המשולש)

$$a_{d-1}u + \dots + a_0 u^d = g(u)$$

היא פונקציה רציפה ! $g(0) = 0 \Leftarrow$

$\Leftarrow$ אם $|u|$ מספיק קטן אז: $|g(u)| < \frac{|a_d|}{2}$ (וזהו ה-ε שבחרנו)

$$\Leftarrow \quad |f(z)| \geq |z|^d \cdot \frac{|a_d|}{2}$$

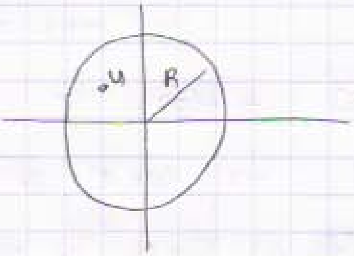
נבחר R כך ש: $R^d \frac{|a_d|}{2} > |f(0)|$

ונקבל כי לכל $z \in \mathbb{C}$ כך ש: $R < |z|$ ומתקיים $|f(z)| > |f(0)|$

נזכור כי לפונקציה רציפה על קבוצה קומפקטית יש מינימום ולכן

קיים $w \in B_R = \{z \in \mathbb{C} \mid |z| < R\}$

כך ש: $|f(w)| \leq |f(u)|$ לכל $u \in B_R$



טענה: $\forall z\in\mathbb{C} \quad |f(\omega)| \le |f(z)|$

עבור $z\in B_R$ כי בחירת ω

עבור $z\notin B_R$

$$|f(z)| \ge |f(0)| \ge |f(\omega)|$$

סוף הוכחת הלמה.

הוכחת המשפט היסודי של האלגברה:

הערה: נשים לב כי אם המינימום של $|f(z)|$ הוא 0 אז יש ל-$f(z)$ שורש וסיימנו.

נניח בשלילה כי המינימום (הגלובלי) של $f(z)$ הוא >0

בה"כ ניתן להניח כי המינימום של $|f(z)|$ מתקבל ב-$z=0$ ו-$f(0)=1$.

אם המינימום היה בנקודה ω נגדיר:

$$g(z)=f(z+\omega)$$

ע"י כפל ב-$\frac{1}{g(0)}$ (קבוע) סוגיים:

$$h(z)=\frac{1}{g(0)}\cdot g(z)$$

כך שהמינימום מתקבל ב-0 ושווה ל-1.

$$f(z)=1+a_1z+a_2z^2+\dots+a_dz^d \quad (a_d\neq 0)$$

יהי $d\ge k\ge 1$ מינימלי כך ש: $a_k\neq 0$ ונקבל $f(z)=1+a_kz^k+z^kp(z)$

כאשר $\mathbb{C}[z]\ni p(z)=a_{k+1}z+\dots+a_dz^{d-k}$

נבחר $z=t\left(\frac{1}{\sqrt[k]{a_k}}e^{\frac{\pi i}{k}}\right)$ כאשר $0<t<1$ קטן

$$f(z)=1+a_k(\quad)^k+z^k\cdot p(z) \quad =1+t^k(-1)$$

אם נבחר $z=t\cdot\frac{1}{\sqrt[k]{a_k}}e^{\frac{\pi i}{k}}$ (במשוואה $f(z)=1+a_kz^k+z^kp(z)$)

אז נקבל: $f(z)=1-t^k+t^k\left(\frac{-1}{a_k}\right)p(t\ \dots)$ (*)

t^{k+1} (משהו-)

עבור $\varepsilon>0$ כאשר $0<t<\varepsilon$ מספיק קטן (קטן כי $|t^k|>|*|$)

$$|f(z)|=|1-t^k+t^{k+1}\text{משהו}|\le|1-t^k|+|t^{k+1}\text{משהו}|<1$$

▨

12-3-2007

מבנים 2 - תרגול מס' 4

היום נחזור לחוגים ראשיים ובפרט חוג פולינומים

תזכורת:

חוג קומוטטיבי עם 1 יקרא ראשי אם כל אידיאל I ב- R

$$I=(a)=Ra$$

דוגמאות: $\mathbb{Z}$, $F[x]$

פריקות בחוגים ראשיים

$a|b$ "a מחלק את b"

$b=a\cdot x$ $\exists x\in R$

$3|6$ $6=3\cdot 2$

$(x-1)|(x^3-1)$ $x^3-1=(x-1)(x^2+x+1)$

בחוג הפולינומים $F[x]$ $x-\alpha | f(x) \iff f(\alpha)=0$

ניתן לאפיין חלוקה באמצעות אידיאלים:

$$a|b \iff (b)\subseteq(a)$$

אם $a|b$ וגם $b|a$ אומרים ש- a ו- b חברים ומסמנים $a\sim b$

נניח כי R תחום שלמות:

$$b=ax$$
$$a=by$$

נציב ונקבל $b=byx$

$$b(1-yx)=0$$
$$\Downarrow$$
$$yx=1$$

ולכן $x,y\in R^{\times}$ (הפיכים) יחידות (הם הפיכים)

מנחיות אידיאלים $(a)=(b) \iff a\sim b$.

כשמדברים על פריקות בשלמים מתעלמים מדרך מהאפשרות לכפול ב-± 1 מסוגיונים אז בחושבם כללים תמיד מדברים על פריקות עד כדי כפל באיבר הפיך.

ישנם שני מושגים די קרובים זה לזה אך במחשבה שקולה יותר הם לא תמיד זהים: להיות איבר ראשוני ולהיות איבר אי-פריק.

R תחום שלמות

$\pi\in R$ יקרא <u>אי-פריק</u> אם לכל כתיבה $\pi=x\cdot y$ או $y\in R^{x}$ ו-$\pi\sim x$ או $x\in R^{x}$ ו-$\pi\sim y$

$\pi\in R$ יקרא <u>ראשוני</u> אם $\pi|xy \Longrightarrow \pi|x$ או $\pi|y$

בשלמים, $\mathbb{Z}$ ראשוני $\equiv$ אי-פריק. $2,3,5,7,11,13,17..$ (הראשוניים הרגילים שאנו מכירים).

<u>טענה:</u> בכל תחום שלמות (א) (π) ראשוני $\iff$ π ראשוני

(ב) (π) אידיאל ראשי מקסימלי $\iff$ π אי-פריק.

(ראשי מקסימלי אינו מוכל ממש בשום אידיאל ראשי גדול ממש ממנו).

<u>הוכחה:</u>

(א) (π) ראשוני $\iff$ $R/(\pi)$ תחום שלמות

$\iff$ לכל $x,y\in R$ $[\bar{x}\cdot\bar{y}=0 \Longrightarrow \bar{x}=0$ או $\bar{y}=0]$

$\iff$ לכל $x,y\in R$ $[x\cdot y\in(\pi) \Longrightarrow x\in(\pi)$ או $y\in(\pi)]$

$\iff$ $\pi|xy \Longrightarrow \pi|y$ או $\pi|x$, כלומר π, ע"פ ההגדרה הוא ראשוני)

②

(ב) נניח כי π אי-פריק:

אם $(\pi) \subseteq (x) \Longrightarrow \pi = x\cdot y$ אך מאי פריקות π יש שתי אפשרויות:

- y הפיך ואז $\pi \sim x$, $(\pi) = (x)$
- x הפיך $(x) = R$ וזה לא אידאל

הכיוון השני:

נניח (π) ראשי מקסימלי אזי $\pi = xy$

$(\pi) \subseteq (x)$

- $(x) = (\pi) \Downarrow$ $x \sim \pi$, $y \in R^{\times}$
- $(x) = R \Downarrow$ $x \in R^{\times}$

טענה: (א) בתחום שלמות π ראשוני $\Longrightarrow$ π אי פריק

(ב) בתחום ראשי גם ההפך π אי-פריק $\Longrightarrow$ π ראשוני ולכן אי פריק $\equiv$ ראשוני

הוכחה: (א) נניח π ראשוני ויהיה $\pi = x\cdot y$ אזי $\pi | xy$ ולכן בה"כ $\pi | x$ אבל הרי גם $x | \pi$ ולכן $x \sim \pi$ ולכן $y \in R^{\times}$.

(ב) בתחום ראשי אידאל ראשי מקסימלי $\equiv$ אידאל מקסימלי

ולכן π אי-פריק $\Longrightarrow$ (π) מקסימלי $\Longrightarrow$ (π) ראשוני $\Longrightarrow$ π ראשוני. ▨

אנחנו נסתכל כמעט ורק בתחומים ראשיים

דוגמאות:

סתירה

$$\mathbb{Z}[\sqrt{-5}] = \{n+m\sqrt{-5} \mid n,m\in\mathbb{Z}\}$$

$$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

$$2 \mid \underbrace{(1+\sqrt{-5})}_{x}\underbrace{(1-\sqrt{-5})}_{y}$$

אם $2 \nmid x$

$2 \nmid y$

כי $\frac{1\pm\sqrt{-5}}{2} \notin R$

$\Leftarrow$ 2 אינו ראשוני, בחוג $\mathbb{Z}[\sqrt{-5}]$.

אך 2 הוא אי-פריק כי אם

$$2 = (m+n\sqrt{-5})(u+v\sqrt{-5})$$

ניקח ערכים מוחלטים: $4 = (m^2+5n^2)(u^2+5v^2)$

ומכאן קל לראות כי 2 הוא אי-פריק.

אז ראינו איבר שהוא לא ראשוני אך כן אי-פריק וזה יכול להיות כי החוג אינו חוג ראשי.

מסקנה: בחוג הפולינומים $F[x]$ האיבר f הינו אי-פריק $\Longleftrightarrow$ ראשוני

ולכן ניתן לקחת כמה דוגמאות:

* x^2+1 אי פריק ב $\mathbb{Q}[x]$

* x^3-2 אי פריק ב $\mathbb{Q}[x]$

(הוכחה 3: אם פריק $\leftarrow$ יש שורש $\leftarrow$ $\sqrt[3]{2}$ ב $\mathbb{Q}$ וזו סתירה)

אך ב- $R[x]$ $(x^2-\sqrt[3]{2}) \mid (x^2-2)$

* x^2+1 ב- $\mathbb{F}_5[x]$ פריק $(x^2+1)=(x+2)(x-2)$

ב $\mathbb{F}_7[x]$ אי-פריק <u>תרגיל</u>

(רמז לתרגיל:) מחבורה ציקלית מסדר 6 (שבה החבורה הכפלית משדה בן 7 איברים) אין איבר מסדר 4 כי $4 \nmid 6$, יש אחת כזו קומוטטיבית)

12-3-2007 ③

מסקנה נוספת: תחום ראשי R, אידאל מקסימלי $\equiv$ אידאל ראשוני $\neq 0$

הוכחה:

(π) מקסימלי $\Leftarrow$

π אי-פריק $\Leftarrow$ $(\pi \neq c)$

π ראשוני $\Leftrightarrow$

(π) ראשוני.

אם נתבונן ב- $K = \mathbb{Q}[x]/(x^2+1)$ (חוג; (x^2+1) אידאל מקסימלי)

אז K שדה, $i = \bar{x}$

$i^2 = \bar{x}^2 = \overline{x^2} = \overline{-1} = -1$

השדה הזה מתקבל כאשר לוקחים את $K = \mathbb{Q} + \mathbb{Q}\cdot i = \{r+si \mid r,s \in \mathbb{Q}\}$

$\mathbb{F}_7[x]/(x^2+1) = L$

זהו גם שדה כי x^2+1 אינו פריק

שוב נעשה את אותו הטריק $i = \bar{x}$

$\mathbb{F}_7 + \mathbb{F}_7 \cdot i = L$

$\#(L) = 49 = 7^2$ (מס' האיברים ב-L)

דוגמא (שהשבוע נסביר בצורה מסודרת):

$K = \mathbb{Q}[x]/(x^2+1)$

האיברים במנה כזו הם מחלקות:

$\bar{f} = f + \mathbb{Q}[x](x^2+1)$

$\bar{x} = i$

$i^2 = \bar{x}^2 = \overline{x^2} = -1$ $\qquad \overline{x^2+1} = \bar{0}$, $\overline{x^2} = \overline{-1}$

(כפל בין מחלקות עושים ע"י כפל בין שני נציגים ואז לוקחים את המחלקה של התוצאה)

$$K = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}i^2 + \mathbb{Q}i^3 + \dots$$

השאלה הנשאלת, היא למה זה סכום ישר, כלומר למה:

$$\mathbb{Q} + \mathbb{Q}i = \{r+si\}$$

$$r+si = 0$$

$$\overline{r+sX} = \overline{0}$$

$x^2+1 \mid r+sX$ אך משיקולי דרגה פולינום מדרגה 2 לא יכול לחלק אותו

אלא אם כן $r+sX$ זהו פולינום (או מחלקת) האפס.

$$\Downarrow$$

$$r = s = 0$$

∞

תזכורת: שדה נקרא ממציין p אם p הינו המספר הטבעי הקטן ביותר כך ש: $p \cdot 1 = 0$ $\quad \underbrace{1+1+\dots+1}_{p \text{ פעמים}} = 0$

אם אין p כזה $\mathrm{char}F = 0$

מדוע p כזה חייב להיות ראשוני? נגדיר הומומורפיזם: $\mathbb{Z} \xrightarrow{\varphi} F$

$$n \longmapsto \underbrace{1+1+\dots+1}_{n \text{ פעמים}} = n\cdot 1$$

זהו הומומורפיזם של חוגים

$$P = \mathrm{Ker}\varphi$$

(ההומומורפיזם הטבעי, הישרון) $\leftarrow$ $\underbrace{\mathbb{Z}/P}_{\text{אין מחלקי אפס}} \xhookrightarrow{\bar{\varphi}} F$

ראשוני $P = (p) = \mathbb{Z}\cdot p$

p ← גם ראשוני

נסמן: $p = \mathrm{char}F$

12-3-2007 (4)

אם F ממציין p

$\mathbb{F}_p \subseteq F$

השדות הראשוניים

אם F ממציין 0

$\mathbb{Q} \subseteq F$

פריקות חד-ערכית בחוגים ראשיים

הגדרה: R תחום שלמות קומוטטיבי הינו חוג עם פריקות אם כל איבר של R ניתן לכתיבה כמכפלה של איברים אי-פריקים.

R חוג עם פריקות חד ערכית אם בנוסף

$$a=\pi_1\cdot\ldots\cdot\pi_n=\lambda_1\cdot\ldots\cdot\lambda_m$$

מכפלת אי-פריקים, אז $n=m$ ואחרי שינוי סדר $\lambda_i\sim\pi_i$

משפט: חוג ראשי הינו חוג עם פריקות חד-ערכית

הגדרה: חוג נותרי הינו חוג בו כל סדרה עולה של אידיאלים

$$I_1\subseteq I_2\subseteq I_3\subseteq I_4\ldots$$

קיים אינדקס n כך ש:

$$I_n=I_{n+1}=I_{n+2}=\ldots$$

דוגמא: $(24)\subset(12)\subset(4)\subset(2)$

הערה: R ראשי ⟸ R נותרי.

הוכחת ההערה: בהינתן סדרה עולה של אידיאלים נגדיר אידיאל חדש

$J=\bigcup I_i$ (האיחוד הוא אידיאל כי הם מוכלים אחד בשני)

$(a)=J$ ⟸ (R ראשי)

קיים n כך ש: $a\in I_n$ ואז $I_n=J$

∎

טענה: בתחום נותרי יש פריקות.

הוכחה: אם לא, נבחר a_1 שאינו מכפלת אי-פריקים.

מכאן a_1 פריק וניתן לכתוב $a_1 = a_2 \cdot b_2$

וב.ה.כ ניתן להניח ש- a_2 אינו מכפלת אי-פריקים $a_2 = a_3 \cdot b_3$

a_3 לא מכפלת אי-פריקים $a_3 = a_4 \cdot b_4$ וכן הלאה

מה קורה לאידיאלים שהם יוצרים?

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$$

עם בלי די, בסתירה לנותריות.

▨

המשך להוכחת המשפט (חלק ב'):

נוכיח כי R ראשי $\Rightarrow$ R עם פח"ע.

הוכחה: נשתמש במה שראינו שבתחום ראשי אי-פריק $\Rightarrow$ ראשוני

נניח $\pi_1 \cdots \pi_n = a = \lambda_1 \cdots \lambda_m$

מכפלה של אי-פריקים בשתי צורות.

π_1 אי פריק $\Rightarrow$ ראשוני $\Rightarrow$ אחרי שינוי הסדר ניתן להניח $\pi_1 \mid \lambda_1$

$\lambda_1 = \pi_1 \cdot \varepsilon_1$ | ε_1 בהכרח הפיך אז $\lambda_1 \sim \pi_1$

אז ניתן לצמצם:

$$\pi_1 \pi_2 \cdots \pi_n = \pi_1 \varepsilon_1 \lambda_2 \cdots \lambda_m$$

בתחום שלמות ניתן לצמצם

$$\pi_2 \cdots \pi_n = (\varepsilon_1 \lambda_2) \cdots \lambda_m$$

וממשיכים באינדוקציה.

▨ סוף הוכחת המשפט

הגדרות:

כ.מ.מ = כפולה משותפת מינימלית (l.c.m)

מ.מ.מ = מחלק משותף מקסימלי (g.c.d)

נראה כי ניתן לתאר את ה gcd ו- lcm בעזרת אידיאלים

(בשיעור הבא)

12-3-2007 (5)

$a \sim \pi_1^{e_1}\pi_2^{e_2}\cdots\pi_r^{e_r}$

$b \sim \pi_1^{f_1}\pi_2^{f_2}\cdots\pi_r^{f_r}$

$\pi_i =$ אי-פריקים לא חברים בזוגות $(\pi_i \not\sim \pi_j)$

$e_i \geq 0,\ f_i \geq 0$

$$gcd(a,b) \sim \prod \pi_i^{\min(e_i,f_i)}$$

$$lcm(a,b) \sim \prod \pi_i^{\max(e_i,f_i)}$$

האפיון באמצעות אידיאלים:

$gcd(a,b)=d \iff d|a,\ d|b$ וגם $d'|a\ d'|b \Rightarrow d'|d$

דוגמה: $gcd(24,36)=12$

במונחים של אידיאלים: $(a)\subseteq(d)$

$(b)\subseteq(d)$

וגם $(a),(b)\subseteq(d')$

$(d)\subseteq(d')$ כלומר (d) האידיאל הכי קטן שמכיל גם את (a) וגם את (b)

הערה: בכל חוג קומוטטיבי, אם I, J אידיאלים, האידיאל הקטן ביותר המכיל את I וגם את J הינו: $I+J=\{x+y \mid x\in I,\ y\in J\}$

* זהו אידיאל של החוג.

<u>מסקנה:</u> בחוג ראשי R אם $d=gcd(a,b)$ $(d)=(a)+(b)=(a,b)$

* נחזור רגע לשלמים:

למשל: $\gcd(15,14)=1$

ולכן ניתן לכתוב $(15)+(14)=\mathbb{Z}$

כי $15-14=1$

* דוגמא נוספת: $(5,7)=1$ כי $3\cdot 7-4\cdot 5=1$

∎

13-3-2007

①

מבנים 2 - שיעור מס' 5

בניה של שדות מחוגים

(א) נתון לנו R חוג קומוטטיבי עם 1

M אידיאל מקסימלי

אז R/M שדה (= חוג המנה)

נתאר עכשיו בניה נוספת:

(ב) שדה שברים:

$$\mathbb{Z} \rightsquigarrow \mathbb{Q}$$

$2, 3, 7 \qquad \frac{2}{3}, \frac{7}{10}$

$$\frac{2}{3} + \frac{7}{10} = \frac{20+21}{30} = \frac{41}{30}$$

* מה שמסומן ב-* עלינו לבדוק לבד

יהיה R תחום שלמות (חוג קומוטטיבי עם יחידה וללא מחלקי אפס)

נגדיר על אוסף הזוגות (r,s) כאשר $s\neq 0$ יחס שקילות*:

$$(r,s)\sim(r',s') \iff rs' = sr' \quad \text{(כפל מוצלב)}$$

למשל $(2,3)\sim(4,6)$ כי $2\cdot 6 = 3\cdot 4$

צריך לבדוק שזה אכן יחס שקילות: רפלקסיביות וסימטריות זה טריוויאלי.

הטרנזיטיביות מורכבת מעט ומושארת לנו כתרגיל.

נסמן ב- $Q=Q(R)$ את אוסף מחלקות השקילות.

את מחלקת השקילות של הזוג (r,s) נסמן ב- $\frac{r}{s}$.

נגדיר:

$$\frac{r}{s}+\frac{r'}{s'} = \frac{rs'+r's}{ss'} \qquad 1=\frac{1}{1}$$

$$0=\frac{0}{1}$$

$$\frac{r}{s}\cdot\frac{r'}{s'} = \frac{rr'}{s\cdot s'}$$

(לבדוק כי: $\left(\frac{r}{s}\right)^{-1} = \frac{s}{r}$)

משפט: (א)* בהגדרות אלו Q מהווה שדה.

(ב)* ההעתקה $r \longrightarrow \frac{r}{1}$

הינה הומומורפיזם חד-חד ערכי (שיכון) של R ב Q

דוגמא: F שדה $R=F[x]$

Q = שדה הפונקציות הרציונליות מעל F שמסומן $F(x)$

פונקציה רציונלית הינה ביטוי

$\frac{f(x)}{g(x)}$ f,g פולינומים

$$\frac{f_1(x)}{g_1(x)} = \frac{f_2(x)}{g_2(x)} \Longleftrightarrow f_1 g_2 = f_2 g_1$$

(וזוהי רק משוואה בין פולינומים)

זהו שדה מאוד מעניין והוא גם מהווה דוגמא ראשונה לשדה ממציין אינסופי.

(F = שדה הקבועים)

$\mathbb{F}_p(x)$ זה כל הביטויים מהצורה $\frac{a_0+a_1x+\dots+a_nx^n}{b_0+b_1x+\dots+b_mx^m}$ ($a_i, b_i \in \mathbb{F}_p$ כאשר שדה בן p איברים)

משל: $F[x,y]$ $\sum\limits_{0 \le i,j} a_{ij}x^iy^j$

$F(x,y)$

נעבור עתה לדון קצת יותר מעמיק בחוג הפולינומים וניתן כמה מונחים שילוו אותנו.

חוגי פולינומים

F שדה (שדה הקבועים)

$F[x]$ = חוג הפולינומים $f=a_0+a_1x+\dots+a_nx^n$

אם $a_n \neq 0$ אז $\deg f = n$

↑ המקדם העליון

a_0 הוא המקדם החופשי.

13-3-2007

②

$F^\times = F[x]^\times$ היחידות הם הסקלרים ששונים מאפס.

$$a_n^{-1} f \sim f$$

$$\hookrightarrow a_n^{-1}a_0 + a_n^{-1}a_1 x + \dots + x^n$$

$a_n = 1$ <u>הפולינום המתוקן</u> (המקדם של החזקה הגבוהה ביותר הוא 1).

$$\deg(f+g) \leq \max(\deg f, \deg g)$$

$$\deg(f \cdot g) = \deg f + \deg g$$

<u>הערה</u>: אין לבלבל את הפולינום כביטוי פורמלי עם הפונקציה הפולינומיאלית שהוא מגדיר:

כלומר: כל פולינום f מגדיר פונקציה פולינומיאלית

$$\tilde{f} : F \longrightarrow F$$

ע"י הערכה:

$$\tilde{f}(a) = f(a)$$

בשדה $\mathbb{F}_p$ $f(x) = x^p - x$

$\tilde{f} = 0$ (בשדה טין p איברים כל מס' מחזקת p הוא עצמו)

ואז לכל x $\tilde{f}$ יהיה 0 למרות ש $f(x)$ <u>אינו</u> פולינום האפס.

אם F שדה אינסופי $\tilde{f} = 0$ רק אם $f = 0$ כי לפולינום מדרגה n יש לכל היותר n שורשים.

<u>הערה נוספת</u>: אם α שורש של f $f(\alpha) = 0$

אז: $f(x) = (x-\alpha)^m h(x)$

$(m \geq 1)$ $h(\alpha) \neq 0$ ואז $m = \text{ord}_\alpha f$

m נקרא <u>הסדר</u> (או הריבוי) של f ב-α (של α כשורש של f).

<u>מסקנה</u> אם $\alpha_1, \dots, \alpha_r$ כל השורשים של f בשדה F

ניתן לכתוב $f(x) = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2} \cdot \dots \dots (x-\alpha_r)^{m_r} \cdot h(x)$

ו- $h(x)$ אין שורשים בשדה F

מסקנה אם F שדה סגור אלגברית, לכל פולינום, שאינו קבוע, יש שורש ואז ניתן לכתוב את f באופן הבא:

$$f = c\cdot(x-\alpha_1)^{m_1}\cdot\ldots\cdot(x-\alpha_r)^{m_r}$$

ואומרים כי f <u>מתפצל</u> למכפלת גורמים לינאריים. (לדוגמא בשדה המרוכבים זה קורה)

בפולינום:

$$x^p - x = x(x-1)(x-2)\ldots(x-p+1)$$

$mod\,p$ למקדמים (או ב-$\mathbb{F}_p[x]$) (פותרים ב-$\mathbb{Z}$ ולוקחים את המקדמים $mod\,p$)

$\Downarrow$

מתוך השוואת המקדם ל-x נקבל את משפט וילסון:

משפט וילסון:

$$(p-1)! \equiv 1 \bmod p$$

הערה נוספת שקשורה מאינפי:

אנו יודעים כי כל פולינום ניתן לגזירה, אך באינפי הנגזרת מוגדרת מהמשמעות גבולות וכל מיני מושגים שאינם אלגבריים, אך ישנן נגזרות שהינן מאוד אלגברי:

נגזרת ב- $F[x]$

אם
$$f = a_0 + a_1x + \ldots + a_nx^n$$
נגדיר:
$$f' = a_1 + 2a_2 + \ldots + na_nx^{n-1}$$

למשל:
$$(x^p - x)' = -1$$

ב-$\mathbb{F}_p[x]$ כי $p\cdot x^{(p-1)} - 1$, כאשר $p = 0$ ב-$\mathbb{F}_p$

כל כללי הגזירה מאינפי 1 תקפים לגבי הנגזרת הזו. (הנגזרת הפורמלית)

הגדרה: שורש α של f(x) יקרא שורש פשוט

אם $ord_\alpha f=1 \iff (x-\alpha)|f$ אבל $(x-\alpha)^2 \nmid f$

שורש מרובה = שורש לא פשוט (ריבוי גדול מ-1)

טענה: α הינו שורש מרובה של f $\iff f'(\alpha)=f(\alpha)=0$

הוכחה: $f=(x-\alpha)^m\cdot h \quad h(\alpha)\neq 0$

$$f'=m(x-\alpha)^{m-1}\cdot h+(x-\alpha)^m\cdot h'$$

$$f'(\alpha)=\begin{cases} h(\alpha) & m=1 \\ 0 & m\geq 2 \end{cases}$$

☒

הגדרה: פולינום f המקיים $\gcd(f,f')=1$ (ל-f ול-f' אין גורם משותף מתוך הפולינומים $F[x]$)

קוראים פולינום ספרבילי.

מסקנה מהטענה: אם f הינו פולינום ספרבילי, כל שורש של f הינו פשוט.

הוכחת המסקנה: אחרת, אם α שורש מרובה, אז $f(\alpha)=f'(\alpha)=0$ ולכן $(x-\alpha)|f$ וגם $(x-\alpha)|f'$ ובפרט הם לא זרים $1\neq\gcd(f,f')$

מבנים אלגבריים 2 - שיעור מס' 6

ראינו שאם K שדה ו- $f \in F[x]$ פולינום אז $K[x]/(f)$ שדה $\Longleftrightarrow$ f אי-פריק

לאור העובדה הנ"ל יש חשיבות רבה לקריטריונים לגבי אי-פריקות של פולינומים.

הרחבות של שדות

יש לנו שני שדות K, L

כל הומומורפיזם $i: K \to L$ הינו מונומורפיזם (שיכון/חח"ע)

על כן, מהיותן עצמן כבר נזהה את תמונת K בתוך L עם K עצמו

כלומר, נזהה ע"י i את K עם $i(K)$ (עם תמונתו) (הזיהוי תלוי בשיכון i)

ונאמר ש: L הינו __הרחבה__ של K (או ש- K תת-שדה של L)

$K \subseteq L$ $\quad L/K$ ("L מעל K")

∞

נראה כמה דוגמאות:

$\mathbb{Q} \subseteq \mathbb{R}$ $\quad$ *

$\mathbb{R} \subseteq \mathbb{C}$

$\mathbb{Q} \subseteq \mathbb{C}$

$\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{C}$

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

יש לנו שתי דרכים לשכן את $\mathbb{Q}(i)$ ב- $\mathbb{C}$:

דרך אחת: מגדירה הקנונית

דרך שניה:

$\varphi(a+bi) = a-bi \in \mathbb{C}$

$\varphi(z) = \bar{z}$ $\quad$ זהו שיכון

$\overline{z+w} = \bar{z} + \bar{w}$

$\overline{zw} = \bar{z} \cdot \bar{w}$

דוגמא נוספת

* דיברנו על שדה הפונקציות הרציונליות בשדה $K(x)$ $\left(\frac{p(x)}{q(x)}\right)$

אז $K \subseteq K(x)$ (זוהי הרחבה של השדה K)

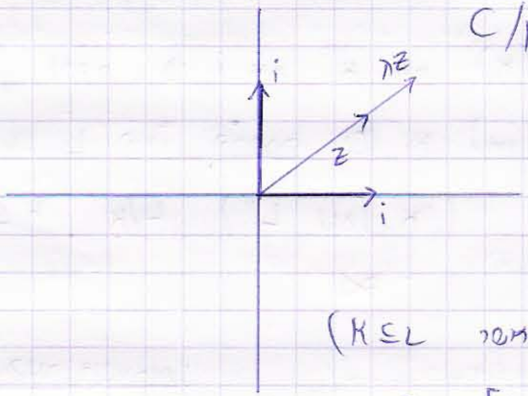
נקודת מבט חשובה: אם L שדה הרחבה של K אז נפרש L מרחב וקטורי מעל K

$x,y \in L$ $a \in K$ הפעולות: $x \pm y$

$a \cdot x$

אקסיומות המרחב הוקטורי מתקיימות.

נתבונן בדוגמא הכי מוכרת: $C/\mathbb{R}$
(ההרחבה של $\mathbb{R}$ ל- C)



$u,v \in \mathbb{R}$

$\mathbb{C} = \{u+iv\}$

<u>הגדרה:</u> דרגת L מעל K (כאשר $K \subseteq L$)

תסומן: $[L:K] = \dim_K L$ הממד כמרחב וקטורי.

אם הממד סופי $= n$, <u>בסיס</u> של L מעל K הינו n איברים $\omega_1, ..., \omega_n$

של L כך שכל איבר של L נתון כצירוף $a_1\omega_1 + ... + a_n\omega_n$

כאשר $a_i \in K$ באופן אחד ויחיד.

על מנת לשמור את מבנה L כשדה, בהינתן הבסיס, די לדעת את המכפלה של

איברי הבסיס $\omega_i \cdot \omega_j = \sum_{k=1}^{n} c_{ij}^{k} \omega_k$

כאשר $1 \le k \le n$ $(c_{ij} \in K)$

קוראים להם לפעמים "קבועי המבנה" של השדה.

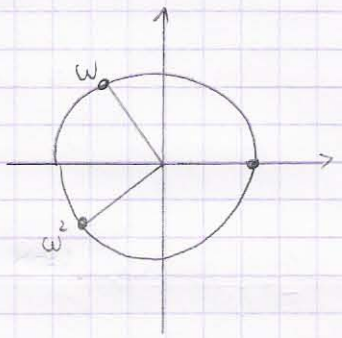
ואז זה נתון: $\left(\sum_i a_i\omega_i\right)\left(\sum_j b_j\omega_j\right) =$

אז מחוקי השדה נקבל: $\sum_{i,j} a_i b_j \sum_k c_{ij}^{k} \omega_k$

19-3-2007

דוגמא נוספת:

(השורש השלישי של היחידה) $e^{\frac{2\pi i}{3}} = \omega$



$\mathbb{Q}(\omega)$

נשים לב כי: $\omega^2+\omega+1=0$

$\omega^3-1=0$

$(\omega-1)(\omega^2+\omega+1)$

$\omega-1 \neq 0$, $\omega^2+\omega+1 = 0$

אז נסיק כי: $\omega^2=-\omega-1$

$\mathbb{Q}(\omega)=\mathbb{Q}\oplus\mathbb{Q}\cdot\omega$

בסיס $1,\omega$

$[\mathbb{Q}(\omega):\mathbb{Q}]=2$

$1\cdot 1=1$

$1\cdot\omega=\omega\cdot 1=\omega$

$\omega\cdot\omega=-1-\omega$

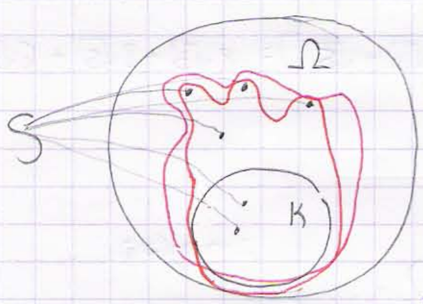
עדיין לא הוכחנו שום דבר אבל הראינו כאן כמה נקודות מבט חשובות של מ״ו.

הגדרה: תהיה $\Omega \supset K$ הרחבת שדות.

תהיה S קבוצת איברים מתוך Ω (סופית או אינסופית)

השדה הנוצר מעל K ע״י S הינו <u>חיתוך</u> כל תת-השדות של Ω

המכילים את $K\cup S$



סימון $= K(S) = \bigcap L$

$K\cup S\subset L\subset\Omega$, L שדה

הערה: חיתוך של משפחה לא ריקה של תת-שדות של Ω

הינה גם כן תת-שדה.

לכן $K(S)$ הינו שדה, וזהו השדה הקטן ביותר המכיל גם את K וגם את

האיברים S.

ההגדרה הזו היא מאוד לא קונסטרוקטיבית

הערה ב: $K(S)$ = כל האיברים של Ω המתקבלים מאיברי K ואיברי S ע״י

פעולות השדה $\frac{f(s_1,\dots,s_m)}{g(t_1,\dots,t_n)}$ f,g פולינומים מעל K

$s_i,t_j\in S$

כמה סימונים: אם $S = \{\alpha_1, \ldots, \alpha_n\}$

$$K(S) = K(\alpha_1, \ldots, \alpha_n)$$

נפרט אם $S = \{\alpha\}$

$$K(S) = K(\alpha)$$

הרחבה פשוטה (הרחבה הנוצרת ע"י איבר אחד).

דוגמא: $\mathbb{Q}(i)$ הרחבה פשוטה של $\mathbb{Q}$

$\mathbb{Q}(i, i+1)$

$\mathbb{Q}(\sqrt{3}, \sqrt{5})$ — תרגיל להראות $\sqrt{5} \neq a + b\sqrt{3}$

וכן: $\sqrt{3} \neq c + d\sqrt{5}$

↓

נוכיח כי כותי הרחבה פשוטה

כי ניתן לכתוב $\mathbb{Q}(\sqrt{3} + \sqrt{5})$

כלומר $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$

הערה: אם S, T שתי קבוצות ב-Ω כדי להוכיח שהשדה שנוצר ע"י סיסוה הראשונה שווה לשדה שנוצר ע"י סטח השניה $K(S) = K(T)$

ד. להראות $S \subset K(T)$ וגם $T \subset K(S)$

הסבר: אם $S \subseteq K(T)$ אז $K(S) \subseteq K(T)$ מהגדרת $K(S)$.

לכן במקרה שלנו די להראות:

$$\sqrt{3}, \sqrt{5} \in \mathbb{Q}(\sqrt{3} + \sqrt{5})$$

$$(\sqrt{3} + \sqrt{5})^2 = 8 + 2\sqrt{15}$$

$$(\sqrt{3} + \sqrt{5})^3 = (8 + 2\sqrt{15})(\sqrt{3} + \sqrt{5}) = 8\sqrt{3} + 8\sqrt{5} + 6\sqrt{5} + 10\sqrt{3} =$$

$$= 18\sqrt{3} + 14\sqrt{5}$$

קיבלנו כי:

$$\left.\begin{aligned} \sqrt{3} + \sqrt{5} &= \alpha \\ 18\sqrt{3} + 14\sqrt{5} &= \beta \end{aligned}\right\} \in \mathbb{Q}(\sqrt{3} + \sqrt{5})$$

עכשיו נותר לפתור שתי משוואות בשני נעלמים (לבודד) את $\sqrt{3}$ ו- $\sqrt{5}$ כסכומים אינדיבידואלים של איברי השדה.

$$\beta - 14\alpha = 4\sqrt{3}$$

$$\frac{\beta - 14\alpha}{4} = \sqrt{3}$$

לעשה זה ביטאנו את $\sqrt{3}$

19-3-2007

(3) סימון נוסף:

Ω

$K|_L$ או ע"י $L|_K$ השדה הנוצר ע"י $= L(K) = K(L)$

שני תת-שדות K , L

שדה זה יסומן $K \cdot L$

נדגיש כי כל זה קורה - רק אם אנחנו נמצאים בתוך שדה גדול (Ω)

כי אחרת לא בטוח תהיה משמעות לפעולות.

מנסים לבנות מהשדה הקטן לשדה (השלם) עם פולינומים, ההרחבה פשוטה ומתחילים $K(\alpha)$

נתחיל מהמקרה הכי פשוט.

יהיה K שדה

Ω הרחבה של K

! $\alpha \in \Omega$ $\quad L = K(\alpha)$ (ההרחבה הפשוטה)

נגדיר:

$$\varphi : K[x] \longrightarrow \Omega$$

$$\varphi(f) = f(\alpha)$$

$$\varphi(a_0 + a_1 x + \dots + a_n x^n) = a_0 + a_1\alpha + \dots + a_n\alpha^n$$

תכונות מיידיות של φ:

(1) φ הומומורפיזם:

$$\varphi(f \pm g) = (f \pm g)(\alpha) = f(\alpha) \pm g(\alpha) = \varphi(f) \pm \varphi(g)$$ (וכנ"ל לכפל)

(2) $\mathrm{im}\,\varphi \subseteq L$

(3) $\varphi|_K$ הינו הזהות

(4) $\mathrm{Ker}\,\varphi =$ אידיאל ראשוני כי:

משפט ההומומורפיזם הראשון: $\dfrac{K[x]}{\mathrm{Ker}\,\varphi} \cong \mathrm{Ker}\,\varphi$

|| תחום שלמות

(כי התמונה איזומורפית לשדה $L \subseteq \Omega$ ולכן אין בה מחלקי אפס)

(ותחום שלמות הוא אידיאל רק אם אין בו מחלקי אפס).

נתבונן כעת ב- $\mathrm{Ker}\,\varphi$, יש לנו התפצלות לשני מקרים

$\mathrm{Ker}\,\varphi = 0$

$\mathrm{Ker}\,\varphi \neq 0 = (f)$ (מקסימלי) ו-f אי-פריק

הגדרה: α יקרא **טרנסצנדנטי** מעל K אם $\operatorname{Ker}\varphi=0$ כלומר אם **אין** פולינום $0\neq f\in K[x]$ כך ש- $f(\alpha)=0$

$\operatorname{Ker}\varphi=\{f\in K[x]\mid f(\alpha)=0\}$ כל הפולינומים עם מקדמים מ-K המאפסים את α (ב-Ω)

דוגמא ידועה (ללא הוכחה): (להוכיח שמשהו הוא טרנסצנדנטי זה קשה)

$K=\mathbb{Q}$

$\Omega=\mathbb{C}$

$\alpha=\pi \qquad (a_i\in\mathbb{Q})$

$$\varphi(a_0+a_1x+\dots+a_nx^n)=a_0+a_1\pi+\dots+a_n\pi^n$$

משפט (עמוק): π הינו טרנסצנדנטי מעל $\mathbb{Q}$

כנ"ל e (לא נוכיח)

הגדרה: איבר **שאינו טרנסצנדנטי** יקרא **אלגברי** מעל K.

כלומר:

α אלגברי $\Longleftrightarrow$ יש $0\neq f\in K[x]$ כך ש: $f(\alpha)=0$

במילים אחרות: $\operatorname{Ker}\varphi\neq 0$

ראינו ש- $\operatorname{Ker}\varphi=(f_\alpha)$ (נוצר ע"י איזשהו פולינום)

f_α פולינום אי-פריק והוא יחיד עד כדי כפל בסקלר $\neq 0$

הגדרה: יהיה α איבר אלגברי מעל K, <u>הפולינום המינימלי</u> שלו, של α מעל K הינו היוצר <u>המתוקן</u> היחיד של $\operatorname{Ker}\varphi=(f_\alpha)$

התכונות שלו:

(א) $f_\alpha(\alpha)=0$ (f_α מתוקן !)

(ב) כל פולינום את המאפס את α $g(\alpha)=0$ $g\in K[x]$

$\Longleftarrow$ $g=f_\alpha\cdot h$ (הוא כפולה של f_α)

(ג) f_α הוא אי-פריק.

19-3-2007

<u>טענה</u>: יהיה g פולינום מדרגה קטנה ביותר המאפס את α

אזי $f_\alpha \sim g$

<u>הוכחה</u>: $g = f_\alpha \cdot h$

$$\deg g = \deg f_\alpha + \deg h$$

אבל $\deg g \le \deg f_\alpha$

ממינימליות ולכן אין ברירה אלא ש: $\deg g = \deg f_\alpha$, $\deg h = 0$

כלומר h = סקלר

<u>דוגמא</u>: הפולינום המינימלי של i מעל $\mathbb{Q}$ הינו x^2+1 כי:

(א) $i^2+1=0$

(ב) אין פולינום מדרגה < 2 $a+bx$

$a,b \in \mathbb{Q}$ המאפס את i.

∞

<u>טענה</u>: אם g הינו פולינום <u>אי-פריק</u> המאפס את α, אזי שוב $g \sim f_\alpha$

<u>הוכחה</u>: היות ו- $g(\alpha)=0$. $g = f_\alpha \cdot h$, f_α אינו סקלר

g אי-פריק $\Longleftarrow$ h סקלר $g \sim f_\alpha$.

אם $\alpha \in K$, $L = K$

$f_\alpha = x - \alpha$

וזה המקרה היחיד בו $\deg f_\alpha = 1$

<u>הערה</u>: הפולינום המינימלי של α יכול להשתנות כשמשנים את K.

x^2+1 מעל $\mathbb{Q}$

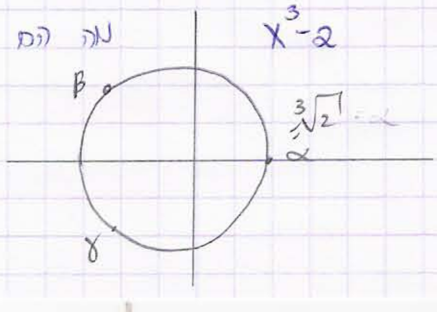
$x - i$ מעל $\mathbb{Q}(i)$

<u>דוגמא</u>: x^3-2 מה הם השורשים שלו:

$\alpha = \sqrt[3]{2}$

$\beta = e^{\frac{2\pi i}{3}} \sqrt[3]{2}$

$\gamma = e^{\frac{4\pi i}{3}} \sqrt[3]{2}$



x^3-2 הינו אי־פריק מעל $\mathbb{Q}$ כי:

$\alpha, \beta, \gamma \in \mathbb{Q}$

ואם היה פריק (מעל דרגה ≤ 3) היה לו שורש רציונלי.

$f_\beta = x^3-2$ מעל $\mathbb{Q}$

שאלה: מהו הפולינום המינימלי של β מעל $\mathbb{Q}(\alpha)$

x^3-2 פריק מעל $\mathbb{Q}(\alpha)$

$$x^3-2=(x-\alpha)\underbrace{(x-\beta)(x-\gamma)}$$
$$=(x-\alpha)h(x)$$

$h(x)$ מדרגה 2

$h(x) \in \mathbb{Q}(\alpha)[x]$

$$\frac{x^3-2}{x-\alpha}=h(x)$$

$\beta \notin \mathbb{R}$ ולכן $\beta \notin \mathbb{Q}(\alpha)$ $\Leftarrow$ $h(x)$ הינו הפולינום המינימלי של β מעל $\mathbb{Q}(\alpha)$

$f=q\cdot h+r$

ב- $K[x]$

ב- $L[x]$

$K \subset L$ כך

מעל $\mathbb{Q}(\alpha)$ אפשר לכתוב:

$$x^3-2=(x-\alpha)\cdot q+r$$

$\deg r=0$

ישאר נכון גם ב- $\mathbb{C}[x]$

20-3-2007 (1)

מבנים אלגבריים 2 - שעור מס' 7

נמשיך את מה שהתחלנו אתמול:

$K \subseteq \Omega$ הרחבת שדות

$\alpha \in \Omega$ אלגברי מעל K

משפט: יהי $\varphi_\alpha : K[x] \longrightarrow \Omega$ ההומומורפיזם $\varphi_\alpha(h) = h(\alpha)$ (לזכור שזה ההומומורפיזם שמוגדר רק על פולינומים עם מקדמים מ-K ולא מ-Ω)

אזי:

(א) $\ker\varphi_\alpha$ = אידיאל ראשוני מקסימלי = (f_α)

כאשר f_α הפולינום המינימלי של α מעל K.

(ב) $K(\alpha) = \operatorname{im}\varphi_\alpha$

(ג) $\deg f_\alpha = n = [K(\alpha):K]$ ובסיס ל $K(\alpha)$ כמרחב וקטורי מעל K

נתון למשל ע"י: $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$

הוכחה: (א) הוכחנו אתמול. (שעור מס' 6)

(ב) היות ו (f_α) הינו אידיאל מקסימלי חוג המנה $K[x]/f_\alpha$

הוא שדה (ע"פ המשפט שלמדנו לפני כמה שעורים) אבל $K[x]/(f_\alpha) \cong \operatorname{Im}\varphi_\alpha$

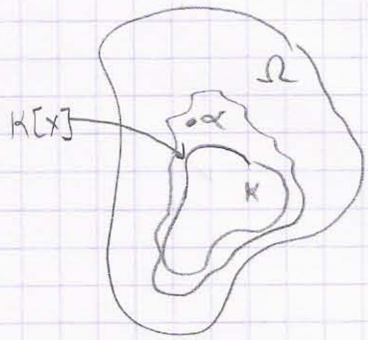
(ע"פ משפט ההומומורפיזם הראשון) ולכן $\operatorname{im}\varphi_\alpha$ הינו שדה

והוא מכיל את $\varphi_\alpha(x) = \alpha$

מאחר ו $K(\alpha)$ הינו השדה הקטן ביותר המכיל את $K \cup \{\alpha\}$ זהו $\operatorname{im}\varphi_\alpha$

(φ_α הוא לתוך $K(\alpha)$ כפי שראינו אתמול ולכן ישנה הכלה לשני הכיוונים)

$$\varphi_\alpha(a_0 + a_1x + \dots + a_rx^r) = a_0 + a_1\alpha + \dots + a_r\alpha^r \in K(\alpha)$$



(ג) $\alpha \longleftrightarrow \bar{x}$

קיבלנו כי $K(\alpha) \cong K[x]/(f_\alpha)$

נסמן n: $n = \deg f_\alpha$

$$f_\alpha = c_0 + c_1x + \dots + c_{n-1}x^{n-1} + x^n$$

נתבונן במחלקות ונעביר אגפים:

$$\bar{x}^n = -c_0 - c_1\bar{x} - \dots - c_{n-1}\bar{x}^{n-1}$$

נכפול ב-x ונקבל את החזקה ה- $n+1$

$$\bar{x}^{n+1} = -c_0\bar{x} - c_1\bar{x}^2 + \dots - c_{n-1}\bar{x}^n =$$ צירוף ליניארי של $1, \bar{x}, \dots, \bar{x}^{n-1}$

ו ממשיכים באינדוקציה $\Longleftarrow$

$\Longleftarrow$ $1, \bar{x}, \ldots, \bar{x}^{n-1}$ מערכת יוצרים ל $K[x]/(f_\alpha)$

וגם בלתי-תלויים כי אם

$$a_0 + a_1\bar{x} + \ldots + a_{n-1}\bar{x}^{n-1} = 0$$

$$f_\alpha(x) \mid a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$$

סתירה כי $\deg f_\alpha = n$ אלא אם כן ל $0 = a_i$

תחת האיזומורפיזם הקנוני המושרה מ- f_α הבסיס $1, \bar{x}, \ldots, \bar{x}^{n-1}$ עובר לבסיס $1, \alpha, \ldots, \alpha^{n-1}$.

הערה: המשפט אומר שכל איבר מ $K(\alpha)$ הינו פולינום ב- α ולא צריך לקחת מנות של פולינומים כאלה.

יהי $\beta = g(\alpha)$ $\quad \deg g \le n-1 \quad g \in K[x]$

כיצד נבטא את $\beta^{-1} = \frac{1}{g(\alpha)}$ כפולינום ב- α?

$$(f_\alpha, g) = (f_\alpha) + (g)$$

מתבוננים באידיאל שנוצר ע"י שני אלה.

$$\supsetneq (f_\alpha) = \text{אידיאל מקסימלי}$$

$$\Longrightarrow (f_\alpha, g) = K[x]$$

זה אומר שניתן לקחת

$1 = f_\alpha \cdot u + g \cdot v$ כאשר $u, v \in K[x]$

נעריך ב- α ונקבל:

$$1 = g(\alpha) \cdot v(\alpha)$$

$$\frac{1}{g(\alpha)} = v(\alpha)$$

20-3-2007

מקרה II

$K \subseteq \Omega$

$\alpha \in \Omega$ טרנסצנדנטי מעל K.

משפט: במקרה זה $Ker\varphi_\alpha = (0)$ ולכן

$$\varphi_\alpha : K[X] \hookrightarrow K(\alpha)$$

ושיכון זה ניתן להרחבה לאיזומורפיזם

$$\tilde{\varphi}_\alpha : K(X) \simeq K(\alpha)$$

$$\tilde{\varphi}_\alpha(X) = \alpha$$

במקרה זה $[K(\alpha):K] = \infty$

הוכחה: נגדיר: $\tilde{\varphi}_\alpha\left(\frac{f(x)}{g(x)}\right) = \frac{f(\alpha)}{g(\alpha)} = \frac{\varphi_\alpha(f)}{\varphi_\alpha(g)}$ צריך לבדוק שההגדרה הזו טובה:

נראה כי: 1) $g(\alpha) \neq 0$ כי נתון כי α טרנסצנדנטי ו- g פולינום עם מקדמים מ- K

2) צריך להראות שזה לא תלוי בנציגים:

$$\tilde{\varphi}_\alpha\left(\frac{f_1}{g_1}\right) = \tilde{\varphi}_\alpha\left(\frac{f_2}{g_2}\right)$$

אם $f_1 g_2 = f_2 g_1$

$$f_1(\alpha)g_2(\alpha) = f_2(\alpha)g_1(\alpha)$$

$$\frac{f_1(\alpha)}{g_1(\alpha)} = \frac{f_2(\alpha)}{g_2(\alpha)}$$

$\tilde{\varphi}_\alpha$ הומומורפיזם ✓

3) נותר להראות כי הוא על

$\tilde{\varphi}_\alpha$ על כי תמונתו הינה שדה המכיל את K ואת α ולכן את $K(\alpha)$.

הדרגה הינה אינסופית כי כמו $1, \alpha, \alpha^2, \ldots$ אינסוף איברים בת"ל מעל K כי כל תלות לינארית נותנת פולינום ב $K[X]$ המאפס את α. ▨

הערה חשובה: אם α, β שני איברים של Ω עם אותו פולינום מינימלי מעל K $f_\alpha = f_\beta$ אזי $K(\alpha) \cong K(\beta)$

$$K(\alpha) \cong K[x]/(f_\alpha) = K[x]/(f_\beta) \cong K(\beta)$$

(דוגמא שראינו אתמול x^3-2, $\sqrt[3]{2} = \alpha$, $e^{\frac{2\pi i}{3}}\sqrt[3]{2} = \beta$, $e^{\frac{4\pi i}{3}}\sqrt[3]{2} = \gamma$)

ההפך אינו נכון, אם α, β איברים שונים (נותנים את אותה הרחבה פשוטה $L = K(\beta) = K(\alpha)$) מתקבל כזה $f_\alpha \neq f_\beta$

(דוגמא: $\mathbb{Q}(i) \cong \mathbb{Q}[x]/(x^2+1)$
$\mathbb{Q}(i+1) \cong \mathbb{Q}[x]/((x-1)^2+1)$)

שאלה שנרצה לענות עליה בהמשך:
f, g אי-פריקים
איך יודעים אם

$$K[x]/(f) \cong K[x]/(g) \ ?$$

נענה בהמשך.

26-3-2007

מבנים אלגבריים 2 - שעור מס' 8

סיכום לשיעור שעבר:

ראינו כי אם יש לנו הרחבה $K \subset \Omega$

ואיבר $\alpha \in \Omega$ שהוא אלגברי מעל K

אז תמיד ניתן להגדיר את ההומומורפיזם

$$\varphi_\alpha : K[x] \longrightarrow K(\alpha)$$

והגרעין שלו $\bar{\varphi}_\alpha : K[x]/(f_\alpha) \cong K(\alpha)$

נשים לב כי ההומומורפיזם הזה מעתיק את המחלקה של x ל-α:

$$\bar{\varphi}_\alpha(\bar{x}) = \alpha$$

כאשר $\bar{x} = x + (f_\alpha)$.

הדוגמא שנתנו $\bar{\varphi}_i \quad \mathbb{Q}(i) \cong \mathbb{Q}[x]/(x^2+1)$ (תחת הזיהוי הזה המחלקה של x עוברת ל-i)

נניח עתה ש-K שדה ונתון $f \in K[x]$ פולינום אי-פריק

<u>משפט:</u> $L = K[x]/f$ הינו שדה המכיל את K, $[L:K] = \deg f$

ו- $\alpha = \bar{x}$ מקיים $f(\alpha) = 0$:

זה משהו שכבר הוכחנו אך נחזור על ההוכחה

<u>הוכחה:</u> f אי-פריק $\Leftarrow$ (f) מקסימלי $\Leftarrow$ L <u>שדה</u>.

ההומומורפיזם הקנוני $K[x] \to L$ הינו הומומורפיזם של חוגים והצמצום ל-K

הוא הומומורפיזם של שדות ולכן <u>שיכון של K ב-L</u>.

לגבי הטענה: ראינו כבר שאם

$n = \deg f$ $\quad \alpha = \bar{x}$ אז: $1, \alpha, \ldots, \alpha^{n-1}$ בסיס ל-L

כמרחב וקטורי מעל K. ולכן n היא דרגת $[L:K]$

ולבסוף, נניח $f(x) = a_0 + a_1x + \ldots + a_nx^n$ אז:

$$f(\alpha) = a_0 + a_1\bar{x} + \ldots + a_n(\bar{x})^n = \qquad (a_i \in K)$$

$$= \bar{a}_0 + \bar{a}_1\bar{x} + \ldots + \bar{a}_n\bar{x}^n =$$

↗ כי חושבים על הקבועים כתור המחלקות שלהם ב-K

$= a_0 + a_1 x + \dots + a_n x^n =$ (סכום של מרוכבות זה סכום של הצמודים)

$= \overline{f(x)} = 0$

(הראנו כי הצמוד α הוא שורש של הפולינום בשדה הבסיס יותר)

■

דוגמא: ניקח את $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ שדה בן p איברים

$\mathbb{F}_p^*$ היא, כפי שראינו במטלה 1, חבורה ציקלית מסדר $p-1$.

(חציים ריבועים וחציים אינם ריבועים)

נבחר $a \in \mathbb{F}_p^*$ שאינו ריבוע בחבורה

$\Leftarrow$ $x^2 - a$ אי-פריק $\Leftarrow$ ניתן לבנות את השדה

$L = \mathbb{F}_p[x]/_{x^2-a}$ כדוגמא לבנה שעשינו קודם ולכן

$[L : \mathbb{F}_p] = 2$

$L = \mathbb{F}_p \omega_1 \oplus \mathbb{F}_p \omega_2$

$|L| = p^2$

$\alpha = \bar{x} \in L$

כמה מסקנות מהבניה הנ"ל:

מסקנה 1: $f \in K[x]$ אי-פריק, אזי כל שתי הרחבות פשוטות $K(\alpha)$ ו- $K(\beta)$ הנוצרות ע"י שורשים α, β של f איזומורפיות מעל K:

כי: $K(\alpha) \cong K[x]/f \cong K(\beta)$

ומצד שני גם $K(\beta)$ איזומורפי.

ולכן $\bar{\varphi}_\beta \circ \bar{\varphi}_\alpha^{-1} : K(\alpha) \cong K(\beta)$

26-3-2007

מסקנה 2: לכל $f\in K[x]$ יש הרחבה $K\subset L$ בה ל-f יש שורש.

הוכחה: אם f אי-פריק, ניקח $L = K[x]/(f)$

אחרת אם f פריק, ויהיה f_1 גורם אי-פריק של f ב- $K[x]$

נמצא הרחבה בה ל- f_1 יש שורש, וכמובן הוא יהיה גם שורש של f.

מסקנה 3: לכל $f\in K[x]$ (מתוקן לצורך הנוחות אך לא חייב להיות מתוקן)

יש שדה $K\subset L$ בו f מתפרק למכפלת גורמים לינאריים:

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

הוכחה: יהיה L_1 שדה בו ל-f יש שורש α_1 ב $L_1[x]$ קיים

$$f(x)=(x-\alpha_1)\cdot f_1(x)$$

$\deg f=n$ $\quad$ $\deg f_1=n-1$ ונמשיך

נמצא שדה $K\subset L_1\subset L_2$ בו ל- f_1 יש שורש α_2

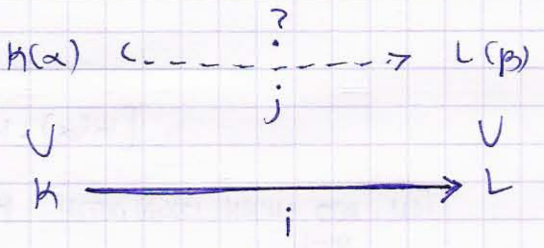
$$f=(x-\alpha_1)(x-\alpha_2)f_2 \quad \text{ב } L_2[x]$$

נמשיך ונבנה מגדל של הרחבות $K\subset L_1\subset L_2\subset\dots\subset L_n=L$ ובכל הרחבה

נקבל שורש נוסף עד שב- L f יתפרק לחלוטין.

(נראה עתה משפט שיהיה מאוד שימושי בהמשך)

משפט הרחבת (האיזומורפיזם) השיכון



סכימה: אלו הן הרחבות פשוטות

משפט: יהי $i: K\hookrightarrow L$ שיכון של שדות. נסמן ב- i גם את השיכון המתקבל מתוך הפולינומים:

$i: K[x]\hookrightarrow L[x]$.

יהיו $K(\alpha)$! $L(\beta)$ הרחבות אלגבריות פשוטות $\quad f_\alpha = irr(\alpha;K)$

(הפולינום האי-פריק של α מעל K)

! $f_\beta = irr(\beta:L)$

נניח כי: $f_\beta \mid i(f_\alpha)$

אזי יש שיכון יחיד $j: K(\alpha)\hookrightarrow L(\beta)$ כך ש:

$$\begin{cases} j|_K = i \\ j(\alpha)=\beta \end{cases}$$

(j מצומצם ל- K)

הוכחה: סכימה:

$$K(\alpha) \overset{\bar\varphi_\alpha}{\cong} \frac{K[x]]}{(f_\alpha)}$$ (זה שדה)

$$\downarrow i$$

$$\frac{L[x]}{(i(f_\alpha))}$$ (זה כבר לא בהכרח שדה אבל זה חוג)

$$\downarrow \pi$$

$$L(\beta) \overset{\bar\varphi_\beta}{\cong} \frac{L[x]}{(f_\beta)}$$

כי: $f_\beta \mid i(f_\alpha)$

ולכן $(i(f_\alpha)) \subseteq (f_\beta)$

R חוג קומוטטיבי
אידיאלים $J \subseteq I$
$R/J \longrightarrow R/I$

נגדיר: $j: K(\alpha) \longrightarrow L(\beta)$

$$j = \bar\varphi_\beta \circ \pi \circ i \circ \bar\varphi_\alpha^{-1}$$

j הינו הומומורפיזם של שדות ולכן שיכון ולכן $j|_K = i$ (כנדרש)

$j(\alpha) = \beta$ ∎

מסקנה: אם $i: K \cong L$! $i(f_\alpha) = f_\beta$ (*) אזי יש איזומורפיזם

$j: K(\alpha) \cong L(\beta)$

כך ש- $j|_K = i$

$j(\alpha) = \beta$

$$[K(\alpha):K] = \deg f_\alpha \overset{(*)}{=} \deg f_\beta = [L(\beta):L]$$

$K(\alpha) \subset L(\beta)$ מרחב וקטורי ממימד סופי מעל $K = L$

ולכן מתלכדים.

26-3-2007

③ נחזור לדיון בדרגת ההרחבה:

דרגת ההרחבה:

$$\dim_K L = [L:K]$$

הערה: אם $K \subset L \subset M$ אזי $[L:K] \le [M:K]$

ואם $[M:K] < \infty$ שוויון קיים אם ורק אם $L = M$

משפט: יהיו $K \subset L \subset M$ שדות. אזי:

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

הוכחה: אם $[L:K] = \infty$ אז בוודאי $[M:K] = \infty$

אם $[M:L] = \infty$ אזי יש לנו אינסוף איברים ב-M בלתי תלויים ליניארית

מעל L, והם בפרט בת"ל מעל K ולכן שוב $[M:K] = \infty$.

נניח שסופיים $[L:K] = n$

(כלומר כאן שני המימדים סופיים) $[M:L] = m$

יהיו $\alpha_1, \dots, \alpha_n$ בסיס של L מעל K.

יהיו $\beta_1, \dots, \beta_m$ בסיס של M מעל L

טענה: $\alpha_i \beta_j$ $\quad 1 \le i \le n$, $1 \le j \le m$

בסיס של M מעל K.

(נסיק מכך כי: $\Longrightarrow [M:K] = m \cdot n$)

הוכחת הטענה: יש להראות שני דברים: (א) קבוצה פורשת (ב) בת"ל:

(א) כל איבר $x \in M$ $\quad c_j \in L$ $\quad x = \sum_{j=1}^{m} c_j \beta_j$

מאידך $c_j = \sum_{i=1}^{n} a_{ij} \alpha_i$

$$a_{ij} \in K$$

$$x = \sum_{i,j} a_{ij} \alpha_i \beta_j$$

$\Longleftarrow$ $\{\alpha_i \cdot \beta_j\}$ פורשים את M מעל K.

בת"ל: נניח $a_{ij} \in K$

$$0=\sum_{ij} a_{ij}\alpha_i\beta_j =$$

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

נסמן c_j כמקדם $c_j \in L$

β_j בת"ל מעל L $\Longleftarrow$ $\forall j\ c_j=0$

$$0=\sum_{i=1}^{n} a_{ij}\alpha_i$$

α_i בת"ל מעל K $\Longleftarrow$ $\forall i,j\ a_{ij}=0$

ולכן מסתיימת הוכחת המשפט.

▨

לא להתבלבל: כשדות $[\mathbb{C}:\mathbb{R}]=2$ כי הדגמא

כחבורות חיבוריות $[\mathbb{C}:\mathbb{R}]=\infty$ זה האינדקס.

כמה דוגמאות:

① $\underbrace{\mathbb{Q}}_{K} \subset \underbrace{\mathbb{Q}(\sqrt{2})}_{L,\ \{1,\sqrt{2}\}} \subset \underbrace{\mathbb{Q}(\sqrt{2},\sqrt{3})}_{L(\sqrt{3}),\ \{1,\sqrt{3}\}}$ (each step of degree 2)

$X^2-3=0$ ואין לו שורש ב- $\mathbb{Q}(\sqrt{2})$

$$(a+b\sqrt{2})^2=3$$

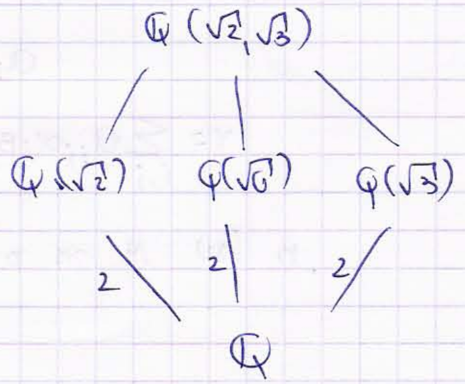
$$a^2+2b^2+2ab\sqrt{2}=3$$

$$\vdots$$

להשלים ולהראות ש $\sqrt{3}$ לא שייך לשדה.

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$$

הבסיס הוא: $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$



26-3-2007

<u>מסקנה</u>: אם $[L:K]$ = מס' ראשוני

אז כל שדה בינים, אינו K, הוא כבר כל L.

<u>הגדרה</u>: הרחבה $K \subseteq L$ תקרא נוצרת סופית אם יש $\alpha_1, \dots, \alpha_r \in L$ כך ש $L = K(\alpha_1, \dots, \alpha_r)$.

<u>הגדרה</u>: הרחבה $K \subseteq L$ תקרא אלגברית אם כל איבר $\alpha \in L$ אלגברי מעל K

(כלומר: ישנו $0 \neq f \in K[x]$, $f(\alpha) = 0$)

<u>משפט</u>: $K \subseteq L$ הרחבה סופית (כלומר $[L:K] < \infty$ (לא "נוצרת סופית"))

אם ורק אם: (א) L נוצרת סופית מעל K.

(ב) L אלגברית מעל K.

<u>הוכחה</u>: "$\Longrightarrow$" (א) יהיה $\omega_1, \dots, \omega_n$ בסיס של L מעל K כמרחב וקטורי

אזי כל איבר של L הינו $a_1\omega_1 + \dots + a_n\omega_n$ כאשר $a_i \in K$ ולכן

L נוצר ע"י $L = K(\omega_1, \dots, \omega_n)$

(ב) יהיה $\alpha \in L$ כל שהוא ונסתכל על שדה הבינים שמתקבל $K \subset K(\alpha) \subset L$

$$[L:K] < \infty \Rightarrow [K(\alpha):K] < \infty$$

$\Downarrow$ (לפי מה שראינו שבוע שעבר)

α אלגברי מעל K.

"$\Longleftarrow$" (א),(ב) נתונים אז נניח $L = K(\alpha_1, \dots, \alpha_r)$! α_i אלגבריים מעל K

בודאי α_i אלגברי מעל השדה שמתקבל מהוספת $L_{i-1} = K(\alpha_1, \dots, \alpha_{i-1})$

ולכן אם, כמו קודם, נסמן $L_i = K(\alpha_1, \dots, \alpha_i)$ $L_0 = K$ אז

$$L_i = L_{i-1}(\alpha_i) \qquad [L_i : L_{i-1}] < \infty$$

$$L = L_r$$

$$[L:K] = [L_r : L_{r-1}][L_{r-1} : L_{r-2}] \dots [L_2 : L_1][L_1 : L_0] < \infty$$

$\blacksquare$

מבנים אלגבריים 2 - שעור מס' 9

משפט: (שעשינו אתמול)

הרחבה $K \subseteq L$ של שדות הינה סופית ($[L:K]<\infty$) $\Longleftrightarrow$

(א) כל איבר של L אלגברי מעל K

(ב) L נוצרת סופית מעל K

$$[K(\alpha_1,\dots,\alpha_i):K(\alpha_1,\dots,\alpha_{i-1})]<\infty$$

נניח עתה כי $K\subset\Omega$

הגדרה: הסגור האלגברי של K בתוך Ω הינו אוסף האיברים של Ω האלגבריים מעל K.

(למשל) $\mathbb{Q}\subset\mathbb{C}$

A = אוסף המספרים המרוכבים האלגבריים מעל $\mathbb{Q}$.

טענה: הסגור האלגברי של K בתוך Ω מהווה שדה.

הוכחה: (מה שצריך צריך להראות זה סגירות תחת הפעולות.)

נסמן ב-A את האוסף הנ"ל; די להראות שאם $\alpha,\beta\in A$ גם $\alpha\pm\beta$ גם $\alpha\cdot\beta$, β^{-1} שייכים ל-A. (לשם כך נשתמש במשפט קודם)

נתבונן בהרחבות $K\subset K(\alpha)\subset K(\alpha,\beta)$

(זוהי הרחבה סופית כי הנתון ש-α אלגברי; גם זו הרחבה סופית)

ולכן נובע כי $[K(\alpha,\beta):K]<\infty$ (מהמשפט על מכפלת דרגות הרחבה)

$$\left.\begin{matrix}\alpha\pm\beta\\ \alpha\cdot\beta\\ \beta^{-1}\end{matrix}\right\}\in K(\alpha,\beta)$$

ומהמשפט הקודם כל איבר $K(\alpha,\beta)$ אלגבריים מעל K.

$\blacksquare$

הערה: אוסף המספרים הטרנסצנדנטלים מעל $\mathbb{A}$ (המשלים של אוסף המספרים האלגבריים)

אינו מהווה שדה, אחרי א לא נמצאים בו, $1, 0$ לא נמצאים בו.

π טרנס'

$1-\pi$ טרנס' אחרת $\pi = 1-(1-\pi)$ היה אלגברי)

$1 = \pi + (1-\pi)$ אלגברי.

הערה: יש רק מס' בן מניה של מספרים אלגבריים (מעל $\mathbb{Q}$)

הוכחת ההערה: כל איבר של $\mathbb{A}$ הינו שורש של פולינום ב $\mathbb{Z}[x]$

אבל יש רק מס' בן-מניה של פולינומים ב- $\mathbb{Z}[x]$ (איחוד בן מניה של קבוצות בנות מניה)

ולכל פולינום מס' סופי של שורשים

כידוע $\aleph_0 < |\mathbb{C}|$.

וזה מרמז על קיום מספרים טרנסצנדנטלים.

∞

משפט: אם $K \subset L \subset M$ הרחבות

$\left\{\begin{array}{l} L \subset M \\ K \subset L \end{array}\right.$ הרחבות אלגבריות $\Longrightarrow$ $K \subset M$ הרחבה אלגברית.

(אנחנו לא מניחים כאן כי דרגת ההרחבות היא סופית)

$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7} \ldots)$
הרחבה אלגברית אינסופית של $\mathbb{Q}$

הוכחה: יהיה $\alpha \in M$.

α אלגברי מעל L ולכן ישנם $c_0, c_1, \ldots, c_n \in L$

כך ש: $c_0 + c_1\alpha + \ldots + c_n\alpha^n = 0$

נסתכל מהרחבות $K \subset \underbrace{K(c_0, c_1, \ldots, c_n)}_{B} \subset \underbrace{K(c_0, \ldots, c_n, \alpha)}_{S}$

אז B הרחבה סופית של K כי $[B:K] < \infty$ כי B נוצרת סופית וכל c_i

הם אלגבריים מעל K ולכן $[S:B] < \infty$ כי α היא $S = B(\alpha)$ ו- α אלגברי

מעל B (כי אפילו הרחבה פשוטה)

$\Longrightarrow \alpha \in S$

$[S:K] < \infty$

$\Longrightarrow$ α אלגברי מעל K

∎

27-3-2007

נראה עוד כמה דברים שנוגעים בסוגיות הרחבות:

תהי $L \supseteq K$ הרחבה סופית $n = [L:K]$

נקבע לה בסיס w_i כמרחב וקטורי $L = Kw_1 + \dots + Kw_n$

$a \in L$

נגדיר העתקה: $M_a : L \to L$

$M_a(x) = a \cdot x$

נטען כי M_a טרנספורמציה לינארית של L כמרחב וקטורי מעל K.

$M_a(w_i) = aw_i$

נשים לב כי $M_a \neq \begin{pmatrix} a & & \\ & a & \\ & & \ddots a \end{pmatrix}$ כי אנו רוצים מטריצה של סקלרים! a- הוא וקטור.

$$M_a = a \cdot w_i = \sum_{j=1}^{n} C_{ij} w_j$$

כאשר $C_{ij} \in K$

ולכן $[M_a] = (C_{ij})$

המטריצה של הטרנספורמציה $1 \leq i,j \leq n$

נראה דוגמא: $\mathbb{C} = \mathbb{R}_1 + \mathbb{R}i$

$a = 3 + 4i$

$$M_a = \begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix}$$

$ai = 3i - 4$

נשים לב כי: $tr(M_a) = a + \bar{a}$ (trace)

$\det(M_a) = a \cdot \bar{a}$

הגדרה: העקבה של a מההרחבה $L \supseteq K$ $tr_{L/K}(a) = tr(M_a)$

הנורמה של a מההרחבה $L \supseteq K$ $N_{L/K}(a) = \det(M_a)$

זה מושג הגיוני ולא תלוי בבסיס כי אם בוחרים בסיס אחר אז המטריצה M_a של הטרנספורמציה הלינארית מתחלפת ב PM_aP^{-1} (בדומה לה) ואז $tr(PM_aP^{-1}) = tr(M_a)$

והדטרמיננטה $\det(PM_aP^{-1}) = \det(M_a)$

$$tr_{L/K}(a) \in K$$

$$N_{L/K}(a) \in K$$

כמו כן:

$$tr_{L/K}(a+b) = tr(M_{a+b}) =$$

$$= tr(M_a + M_b) = tr_{L/K}(a) + tr_{L/K}(b)$$

$$\left[\begin{array}{l} [(a+b)x = ax + bx] \\ (M_{a+b}(x) = M_a(x) + M_b(x)) \end{array} \right]$$

$\Longleftarrow$ $tr_{L/K}$ הינה הומומורפיזם של החבורות החיבוריות: $L^+ \to K^+$.

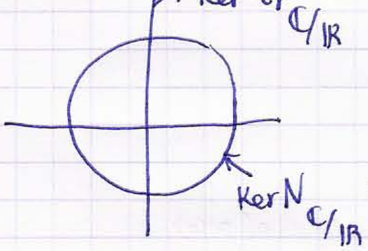
ובאותה הדרך:

(הנורמה) $N_{L/K}(a \cdot b) = \det(M_{a \cdot b}) = \det(M_a \cdot M_b) =$

$$= \det(M_a) \cdot \det(M_b) = N_{L/K}(a) \cdot N_{L/K}(b)$$

(החבורה הכפלית)

$\Longleftarrow$ $N_{L/K} : L^* \to K^*$ הינה הומומורפיזם של החבורות הכפליות.



במספרים המרוכבים

ציר המדומה היא גרעין העקבה

ומעגל היחידה הוא הגרעין של הנורמה

$$|x \cdot I - M_a| = f_{M_a}(x)$$

הפולינום האופייני של M_a

$$= x^n - tr(M_a)x^{n-1} + \ldots + (-1)^n \det(M_a)$$

מבנים אלגבריים 2 - שעור מס' 10 (שעור ראשון אחרי השביתה)

הסרגל שלנו אינו מסומן ↑

בניות בעזרת סרגל ומחוגה

אם יש לנו הרחבה של שדות $K \subset L$ אז ניתן להסתכל על L כמרחב וקטורי מעל K

ונזכור כי: $[L:M][M:K] = [L:K]$

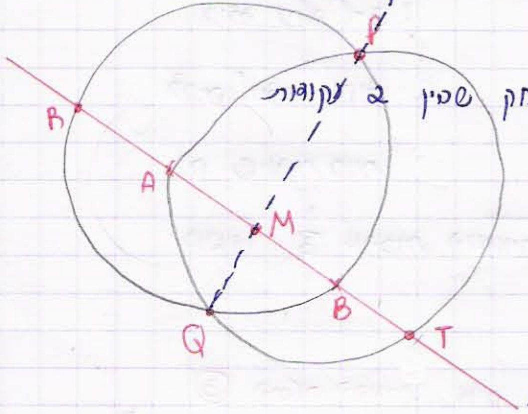
נעסוק עכשיו מעט בגאומטריה:

S = קבוצת נקודות במישור

מאפשרים לנו שתי פעולות: להעביר קווים ולשרטט מעגלים:

הפעולות הן: (א) להעביר קו ישר בין שתי נקודות מתוך S

(ב) לפתוח את המחוגה אל המרחק שבין 2 נקודות של S ולשרטט מעגל שמרכזו נקודה של S



המעגלים והישרים המתקבלים כך נקראים המעגלים והישרים המוגדרים על ידי S

נקודות החיתוך החדשות שמתקבלות (יחד עם נקודות S) נקראות נקודות הניתנות לבניה מתוך S בצעד אחד.

עכשיו נפריד את הנק' הנ"ל ל-S ונחזור על התהליך.

דוגמא: M = אמצע הקטע AB. (זוהי נקודה שניתנת לבניה באמצעות שני צעדים)

כל הנקודות שניתן לבנות באמצעות מס' סופי של צעדים כאלה יקראו מ-S.

השאלה: מה ניתן לבניה מתוך S?

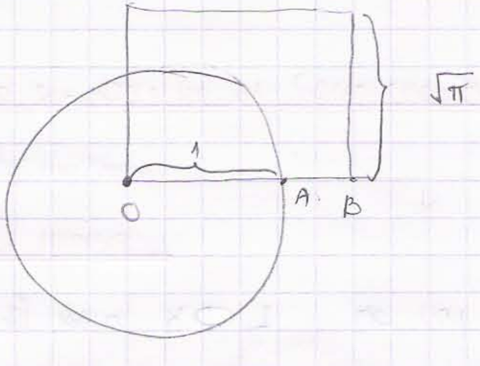
בעיות קלאסיות (מימי יוון)

① תרבוע העיגול: (רוצים לרבע את המעגל)

נתחיל משתי נקודות $S = \{O, A\}$

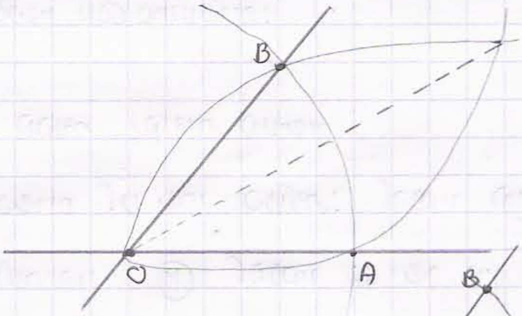
המטרה: לבנות נקודה B כך ששטח המעגל עם רדיוס OA = שטח הריבוע עם צלע OB

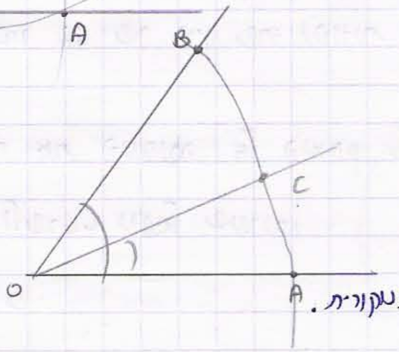
כאת המשימה:



② חלוקה של זוית לשלושה חלקים שווים:

תזכורת: חלוקה של זוית לשניים:





כיצד נחלק ל-3?

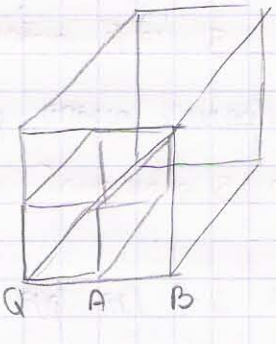
צריך למצוא נקודה C

כך שיוצרת זוית

בגודל $\frac{1}{3}$ מהזוית המקורית.

③ הכפלת הקוביה: איך בונים קוביה שהנפח שלה כפול מנפח קוביה נתונה.

$OB : OA = \sqrt[3]{2}$



אלו בעיות שניסו לפתור במשך אלפי שנים.

מאותם ימים לא הכירו הוכחות אי-יתכנות

כפי שנראה בהמשך

איך האלגברה נחלצה לעזרתנו?

נכניס קואורדינטות קרטזיות במישור ונניח: $|S| \ge 2$

בה"כ $(0,0) \in S$

$(1,0) \in S$

נניח הנקודה $p=(x,y)$ ניתנת לבניה מתוך S.

כלומר שיש לנו

$$S = S_0 \subset S_1 \subset \dots \subset S_n$$

$$S_i = S_{i-1} \cup \{P_i\}$$

P_i ניתנת לבניה מתוך S_{i-1} בצעד אחד.

$p = P_n$

הרעיון הוא להתבונן בשדות:

$$Q(S_i) = K_i$$

הנוצרים מעל Q ע"י קואורדינטות x ו-y של נקודות S_i

$$Q(S) = K = K_0 \subset \dots \subset K_n$$

K_i הרחבה של K_{i-1}

$$K_i = K_{i-1}(x_i, y_i)$$

$$P_i = (x_i, y_i)$$

טענה: $[K_i : K_{i-1}] = 2$ או 1 כלומר אם מוסיפים נקודה אחת או שלא שינינו את השדה או שכן הרחבה ריבועית (ממעלה 2)

הוכחה: P_i הינה חיתוך של:

(א) שני ישרים או

(ב) ישר ומעגל או

(ג) שני מעגלים המוגדרים ע"י S_{i-1}

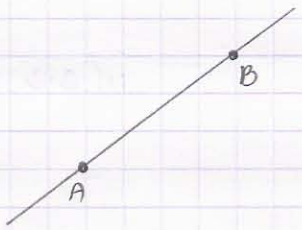
מקרה ⓓ: (את ⓐ ו- ⓒ נשאיר את זה כתרגיל - אותה הוכחה)

(*)

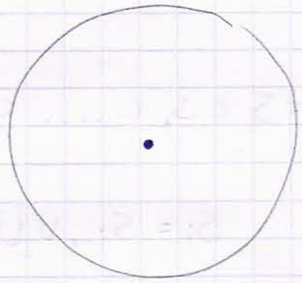
הישר משוואתו: $ax+by=c$

המעגל משוואתו: $(x-p)^2+(y-q)^2=m$

! a,b,c,p,q,m הם מתוך K_{i-1}



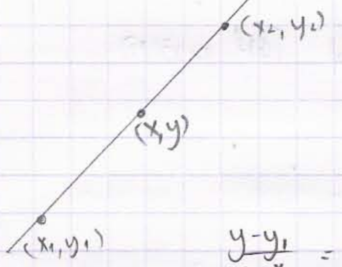
$A,B\in S_{i-1}$



$(p,q) =$ נקודה מ- S_{i-1}

$m=(x_1-x_2)^2+(y_1-y_2)^2$ $\quad x_1,y_1,x_2,y_2\in K_{i-1}$

רדיוס המעגל בריבוע (בעצם כמו שפתחנו את המחוגה)



עכשיו נפתור את שתי המשוואות (*):

נחלץ את y מהמשוואה הלינארית ונציב

במשוואה הריבועית

ונקבל משוואה ריבועית

ב- x_i

הצבת משוואת הישר:

$$\frac{y-y_1}{x-x_1}=\frac{y_2-y_1}{x_2-x_1}$$

ולכן $[K_{i-1}(x_i):K_{i-1}] = 1$ או 2

(ההסבר בעצם מדוע אנחנו נשארים בשדה)

(כי בעצם פתרנו משוואה ריבועית)

y_i, שנחלץ אחר מהמשוואה הלינארית, שייך כבר ל:

$$y_i\in K_{i-1}(x_i)$$

כי:

$$K_i=K_{i-1}(x_i,y_i)=K_{i-1}(x_i)$$

27-5-2007

מסקנה חשובה מהטענה: אם (x,y) ניתנת לבניה מתוך S

! $K=\mathbb{Q}(S)$ אזי דרגת $[K(x,y):K]$ היא חזקה של 2.

הוכחה: בסימונים של קודם,

$[K_i:K_{i-1}]=$ 1 או 2

ולכן $[K_n:K]=$

$=[K_n:K_{n-1}]\cdot[K_{n-1}:K_{n-2}]\cdots[K_1:K]$

היא חזקת 2.

$x,y\in K_n$ ולכן:

$K\subset K(x,y)\subset K_n$

ולכן $[K(x,y):K]$ מחלקת את $[K_n:K]$ ולכן גם היא חזקת 2.

הערה בנוגע למסקנה: ההיפך של המסקנה אינו בהכרח נכון, כלומר זה לא אם ורק אם. מה שכן נכון, זה שנקודה ניתנת לבניה אם ורק אם יש "הרחבה של שדות" שכל אחת היא הרחבה מסדר 2 והנקודה אליה אנו מתייחסים שייכת להרחבה האחרונה.

כעת ניגש להוכחת אי-היתכנות הראשונה:

משפט: אי-אפשר לרבע את המעגל בעזרת סרגל ומחוגה

הוכחה: נתונות $S=\left\{\begin{matrix}(0,0)\\(1,0)\end{matrix}\right\}$

עלינו לבנות את $(x,y)=(\sqrt{\pi},0)$

$$K=\mathbb{Q}(S)=\mathbb{Q}$$

$$K(x,y)=\mathbb{Q}(\pi)$$

נצטט ערכים משפט חשוב:

משפט לינדמן:

π הינו טרנסצנדנטי מעל $\mathbb{Q}$

$\Leftarrow$ $[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}]=\infty$
π ⊎

ולכן $[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}]$ ודאי אינו חזקה של 2

▨

חלוקת זווית ל-3:

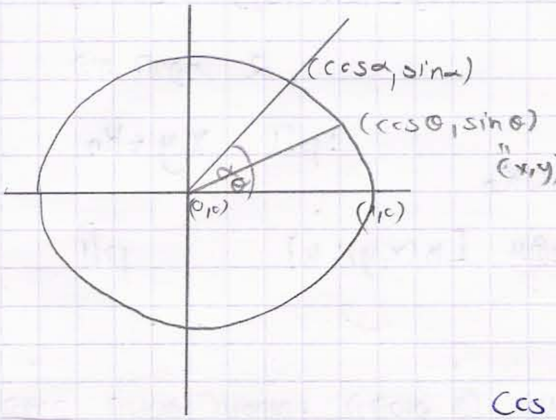
משפט: יש זוויות שאי-אפשר לחלק ל-3 בעזרת סרגל ומחוגה

הוכחה:

$$S = ((0,0),\ (1,0),\ (\cos\alpha, \sin\alpha))$$

$$K = \mathbb{Q}(\cos\alpha, \sin\alpha)$$

כי $(0,0)$, $(1,0)$ כבר שם [illegible].



צריך לבנות את (x,y)

נזכיר זהות שנשתמש בה:

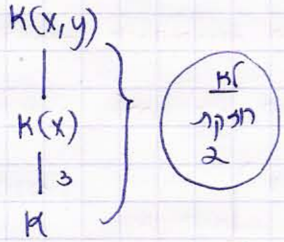
$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$$

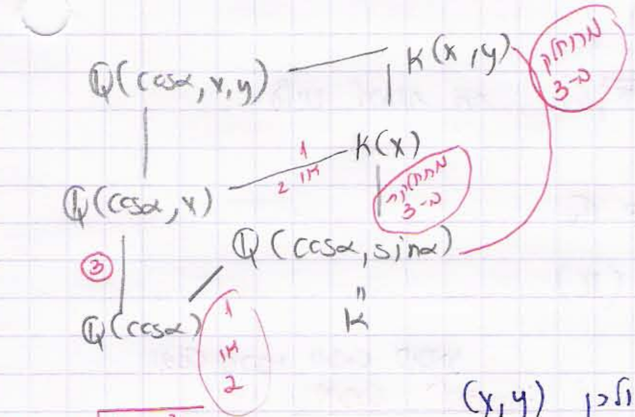
והגדרנו: $3\theta = \alpha$

$$4x^3 - 3x - \cos\alpha = 0$$

אם המשוואה הזאת אי-פריקה מעל K

$$[K(x):K] = 3$$





צ"ל להראות ש

$$4x^3 - 3x - \cos\alpha$$

אי-פריקה מעל $\mathbb{Q}(\cos\alpha)$

$$\Downarrow$$

$[K(x,y):K]$ אינו חזקת 2 ולכן (x,y)

אינה ניתנת לבניה.

דוגמא: $\alpha = 60^\circ$

אי אפשר לבנות מתוכה את $\theta = 20^\circ$

$$4x^3 - 3x - \frac{1}{2} = 0$$

$$\mathbb{Q}(\cos\alpha) = \mathbb{Q}$$

נסתכל במשוואה:

$$8x^3 - 6x - 1 = 0$$

$y = 2x$ $\qquad y^3 - 3y - 1$

$y = z+1$ $\qquad (z+1)^3 - 3(z+1) - 1 = 0$

קריטריון איזנשטיין $\qquad z^3 + 3z^2 - 3 = 0$

$p = 3$.

באותו האופן צריך להראות כי לא ניתן לבנות קוביה שנפחה כפול מנפח קוביה נתונה. $\boxed{\sqrt[3]{2} \quad x^3 - 2}$

נדבר עכשיו על מה שעתיד לבוא:

תורת גלואה:

$L \supset K$ הרחבה סופית

רוצים לציין את כל שדות הביניים:

$$L \supset M \supset K$$

(M – שדה ביניים)

הרעיון של גלואה הוא לתרגם מהאלגברה הלינארית ולעבור לתורת החבורות.

לא החבורה החיבורית של L או הכפלית, לא החבורות הטבעיות אלא החבורה הסימטרית, חבורת האוטומורפיזמים:

גלואה מגדיר להרחבה L/K חבורה סופית $= Gal(L/K)$

= חבורת האוטומורפיזמים של L מעל K (לאו דווקא קומוטטיבית)

ומצא "שבתנאים מסוימים" המבנה של כל שדות הביניים של L/K משתקף כמראה במבנה תת-החבורות של $Gal(L/K)$

$$\Gamma(L:K)$$
$$\parallel$$
$$Gal(L/K)$$

תזכורת: יהי L שדה.

אוטומורפיזם של L הינו העתקה חח"ע ועל

$$\sigma : L \longrightarrow L$$

$$\sigma(0)=0$$

$$\sigma(1)=1$$

$$\sigma(x+y)=\sigma(x)+\sigma(y)$$

$$\sigma(xy)=\sigma(x)\sigma(y)$$

דוגמא: ⊛ הזהות:

$$e(x)=x$$

$e=$ אוטומורפיזם הזהות (העתקת הזהות היא היחידה של חבורת האוטומורפיזמים)

⊛ הצמוד המרוכב:

$L=\mathbb{C}$ $\rho(z)=\bar{z}$ גם זהו אוטומורפיזם

⊛ $Char\, L=p$ (L שדה ממציין p)

$\sigma(x)=x^p$ (העלאה בחזקת p)

נטען כי σ הומומורפיזם של שדות (ולכן חח"ע, לפעמים על ולפעמים לא):

רק הדברים ברורים אך:

$$(x+y)^p = x^p + px^{p-1}y + \binom{p}{2}x^{p-2}y + \dots + pxy^{p-1} + y^p$$

עם בינום ניוטון

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$ אזי p $1<k\leq p-1$

$$p \mid \binom{p}{k}$$

ולכן $\binom{p}{k}_L=0$ ולכן:

$(x+y)^p = x^p + y^p$ ולכן העתקה כו היא הומומורפיזם

של פרובניוס (נראה מקרים שבהם זה גם כן יהיה אוטומורפיזם)

מבנים אלגבריים 2 - שיעור מס' 11

תורת גלואה

(זוהי תורה שמשלבת את תורת השדות ותורת החבורות)

חבורת האוטומורפיזמים של שדה L

$$Aut(L) = \{\sigma : L \to L \mid \sigma \text{ הינו אוטומורפיזם}\}$$

σ חח"ע ועל ומתקיים:

$\sigma(0) = 0$

$\sigma(1) = 1$

$\sigma(x+y) = \sigma(x) + \sigma(y)$

$\sigma(xy) = \sigma(x) \cdot \sigma(y)$

פעולת החבורה היא הרכבה

$$(\sigma \circ \tau)(x) = \sigma(\tau(x))$$

צריך כמובן להראות שההרכבה (ההרכבה) גם אוטומורפיזם:

למשל נראה את החיבור: $(\sigma\tau)(x+y) = \sigma(\tau(x+y)) =$

$$= \sigma(\tau(x) + \tau(y)) = \sigma(\tau(x)) + \sigma(\tau(y))$$

ורואים כי זה מתקיים.

היחידה: $e(x) = x$ (איבר היחידה)

ההפכי: $\sigma^{-1}(x) = y \iff x = \sigma(y)$

צריך לבדוק את אסוציאטיביות החבורה:

$$\sigma(\tau\rho)(x) = \sigma(\tau(\rho(x))) =$$

$$= (\sigma\tau)(\rho(x)) = (\sigma\tau)\rho(x)$$

זוהי תת חבורה מאוד [illegible] $\{e\} \subset Aut(L)$

דוגמאות: אם $Aut(L) = \{e\}$

$\mathbb{Q}$

$\mathbb{F}_p$

$\mathbb{R}$ (תרגיל: אין אוטומורפיזמים של $\mathbb{R}$ שונים מהזהות. רמז: $0 < x \in \mathbb{R} \iff x$ ריבוע)

$x=y^2$

$\sigma(x) = \sigma(y^2) = \sigma(y)^2 > 0$

ל- $\mathbb{C}$ כבר יש מספר בלתי ניתן להימנות של אוטומורפיזמים

הערה נוספת: החבורה הזו היא מדרך לא קומוטטיבית.

אנחנו, בתורת גלואה, לא מתעניינים בשדה אחד אלא בהרחבה של שדות:

L/K הרחבת שדות

הגדרה: חבורת גלואה של ההרחבה L/K הינה:

$$Gal(L/K) = \{\sigma \in Aut(L) \mid \sigma(x)=x \quad \forall x \in K\}$$

$$\sigma|_K = identity$$

הערה: $Gal(L/K)$ הינה אכן תת-חבורה של $Aut(L)$ כי:

3· להראות סגירות תחת הפעולות הרכבה והפכי:

אם: $\sigma, \tau \in Gal(L/K)$

אז גם ההרכבה: $\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x) = x$

(כי זו זהות)

הפכי: $x = \sigma^{-1}(x)$

נראה מהעשן כי: אם L/K סופית, אז $Gal(L/K)$ סופית:

$$|Gal(L/K)| \leq [L:K]$$

הרחבה סופית L/K שבה יהיה כאן שוויון תקרא הרחבת גלואה

28-5-2007 ②

<u>כמה דוגמאות:</u>

① $Gal(\mathbb{C}/\mathbb{R})=\{e,\rho\}$ $\mathbb{C}=\mathbb{R}(i)$

כאשר $\rho(z)=\bar{z}$ (הצמוד)

<u>הוכחה:</u> ודאי e,ρ שם.

אם $\sigma\in Gal(\mathbb{C}/\mathbb{R})$ נטען כי σ יעביר את i או ל-i או ל-$-i$

$$\sigma(i)^2=\sigma(i^2)=\sigma(-1)=-1 \Rightarrow \sigma(i)=\pm i$$

זה יגרור כי לכל $z=x+iy$ $x,y\in\mathbb{R}$

$$\sigma(x+iy)=\sigma(x)+\sigma(i)\sigma(y)=x\pm iy$$

אז או שקיבלנו זהות או שקיבלנו את הצמוד המרוכב ולכן אלו הם האוטומורפיזמים היחידים של ההרחבה $\mathbb{C}/\mathbb{R}$

(זוהי דוגמא להרחבת גלואה)

②

$K=\mathbb{Q}$

$L=\mathbb{Q}(\zeta)$

$\zeta=e^{2\pi i/p}$ שורש יחידה פרימיטיבי מסדר p

<u>p ראשוני:</u>

<u>טענה:</u> הפולינום המינימלי של ζ מעל $\mathbb{Q}$ הינו:

$$\Phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\dots+x+1$$

(זה נקרא הפולינום הציקלוטומי ה-p-י)

צריך להראות ש-ζ הוא שורש שלו ושהוא אי-פריק

קל לראות כי: $\Phi_p(\zeta)=0$

מדוע הוא אי-פריק?

$$\Phi_p(1+y)=\frac{(1+y)^p-1}{y}=$$

$$=\frac{y^p+py^{p-1}+\binom{p}{2}y^{p-2}+\dots+py}{y}=y^{p-1}+py^{p-2}+\dots+p$$

וקיבלנו פולינום איזנשטיין

(עבור p) להיות! $\binom{p}{k}$, המקדמים הבינומים מתחלקים ב-p עבור $1\le k<p-1$ ←

כלומר מתקיימים התנאים ולכן $\Phi_p(1+y)$ אי-פריק
מכאן שגם $\Phi_p(x)$ אי-פריק כי אם יש פירוק:

$$\Phi_p(x) = g(x)\cdot h(x)$$

$$\Phi_p(1+y) = g(1+y)\, h(1+y)$$

וזה אי פריק — לכן גם זה אי-פריק

<u>כמסקנה נקבל:</u>

$$[L:\mathbb{Q}] = p-1$$ (צנתי: גם הוכחת גלואה)

וגם:

$$\varphi_1 : \ \mathbb{Q}[x]/(\Phi_p) \simeq L$$

$$\varphi_1(x \bmod \Phi_p) = \zeta$$

זה כתיב אחר למחלקה של x ← $x+(\Phi_p)$ (האידיאל)

שורשי Φ_p הינם $e^{2\pi i a/p} = \zeta^a$

$a = 1,2,\dots,p-1$ (לא לוקחים את 1 כי 1 הינו לא שורש יחידה פרימיטיבי)

$$0 = \frac{(\zeta^a)^p - 1}{\zeta^a - 1} = \Phi_p(\zeta^a)$$

כל שורשי Φ_p <u>כבר ב-L</u> (זה לא תמיד קורה)

לכל $1 \le a \le p-1$

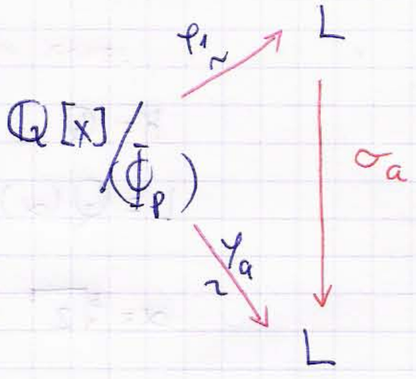
$$\varphi_a : \ \mathbb{Q}[x]/(\Phi_p) \xrightarrow{\sim} \mathbb{Q}(\zeta^a)$$

$$\varphi_a(x \bmod \Phi_p) = \zeta^a$$

אבל $\mathbb{Q}(\zeta^a) = L$ גם כן (כי $\subseteq$ והדרגות מעל $\mathbb{Q}$ שוות)

28-5-2007

אז מה קיבלנו:



יהיה $\sigma_a = \varphi_a \circ \varphi_1^{-1}$

יהיו אוטומורפיזם של L.

טענה: $Gal(L/\mathbb{Q}) = \{\overset{e}{\sigma_1}, \sigma_2, \dots \sigma_{p-1}\}$

שכן: $|Gal(L/\mathbb{Q})| = [L:\mathbb{Q}] = p-1$

$$\sigma_a(\zeta) = \zeta^a$$

(הערה: $\sigma_a(c_0 + c_1\zeta + c_2\zeta^2 + \dots + c_{p-2}\zeta^{p-2}) =$
$c_0 + c_1\zeta^a + c_2\zeta^{2a} + \dots c_{p-2}\zeta^{a(p-2)}$
רק שורש היחידה מוזז, לא הרציונלים!)

יהיה σ אוטומורפיזם כלשהו

$$\sigma(\zeta)^p = \sigma(\zeta^p) = \sigma(1) = 1$$

ולכן $\sigma(1) = 1$

$$\sigma(\zeta) = \zeta^a$$

$$1 \le a \le p-1$$

$$\left(\zeta^{p-1} = -\zeta^{p-2} - \zeta^{p-3} - \dots - p-1\right)$$

בדוגמא הנ"ל, מס' האיברים בחבורת גלואה הוא דרגת ההרחבה והאיברים הללו התקבלו מכך שהם לקחו את שורש היחידה הפרימיטיבי לאחד מהאחרים.

נסגור לדוגמא הבאה:

③

$K = \mathbb{Q}$

$L = \mathbb{Q}(\alpha)$

$\alpha = \sqrt[3]{2}$

הפולינום המינימלי הוא: $x^3 - 2$

$[L : \mathbb{Q}] = 2$

אבל נטען כי חבורת גלואה מכילה רק איבר אחד:

$Gal(L / \mathbb{Q}) = \{e\}$

כי אם:
$$\sigma(\alpha^3) = \sigma(\alpha)^3$$
$$\sigma(2) = 2$$

אבל הפתרון היחיד של $x^3 = 2$ ב- L הינו $x = \alpha$ (כי $L \subseteq \mathbb{R}$)

ולכן $\sigma(\alpha) = \alpha \Leftarrow \sigma = e$ (σ היא הזהות)

זוהי איננה הרחבת גלואה $(1 < 2)$

---

④ **מציין p**

(תהי) משפחה שהיא $K = \mathbb{F}_p(t)$ פונקציות רציונליות במשתנה t וזהו שדה אינסופי ממציין p.

$L = K(x)$

$x^p = t$ (זוהי הרחבה פשוטה כאשר x מקיים את המשוואה הזו).

$= K[x] / (x^p - t)$

יש כאן מקור לבלבול כי יש פה פולינומים מעל פולינומים.

כתור דוגמא ניקח:
$$\frac{t^2-1}{t+2}x^2 + \frac{3t-5}{t+1} \cdot x - t$$

עכשיו נתבונן ב: $x^p - t$.

28-5-2007

x^p-t אי-פריק מפאת קריטריון אייזנשטיין לראשוני t (קריטריון אייזנשטיין עובד לכל חוג ראשי)

(ראשוני כפולינום מדרגה 1)

אנלוגיה:

$\mathbb{F}_p[t]$	תחום ראשי	$\mathbb{Z}$
$\mathbb{F}_p[t]$	שדה השברים	$\mathbb{Q} = K$
t	אי-פריקים (ראשוניים)	5 $\quad K[x]$
x^p-t		x^p-5

הדגמה:

$t = x^p$

$$\mathbb{F}_p(x) = K(x)$$
$$|$$
$$\mathbb{F}_p(t) = K$$

$$\sigma \in Gal(L/K) = \{e\}$$

נניח $L \ni \sigma(x) = y$

$$y^p = \sigma(x)^p = \sigma(x^p) = \sigma(t) = t$$

אך מכיוון שאנחנו בשדה ממציין p העלאה בחזקת p היא הומומורפיזם של שדות.

<u>ממציין p</u>:

$$y^p - x^p = (y-x)^p$$
$$t - t =$$
$$0 =$$
$$\Longrightarrow y = x$$

אין אף פתרון אחר ל: $x^p = t$ או כולם אחדים

$$x^p - t = x^p - x^p = (x-x)^p$$

תופעה זו, נוכיח בהמשך, לא יכולה לקרות בשדה ממציין 0.

ג) הדוגמאות שראינו עד עכשיו הן הרחבות סופיות

נעבור עתה להגדרות העיקריות:

תהיה L

L/K

הרחבה סופית K

$$G = Gal(L/K)$$

שדות ביניים	תת-חבורות
$L \supseteq M \supseteq K$	$\{e\} \subset H \subset G$

<u>הגדרה</u>: תהיה H תת-חבורה של G

<u>שדה השבת של H</u> יהיה

$$\mathcal{F}(H) = \{x \in L \mid \alpha(x) \quad \forall \alpha \in H\}$$

(אוסף נקודות השבת, שלא זזות תחת אף אחת מהפונקציות של H)

<u>הגדרה</u>: יהיה $L \supseteq M \supseteq K$ שדה ביניים.

<u>החבורה</u> של M הינה

$$\mathcal{G}(M) = Gal(L/M)$$

28-5-2007

טענה 1: (א) $L \supseteq \mathcal{F}(H) \supseteq K$ והינו תת-שדה.

(ב) $\mathcal{F}(\{e\}) = L$ ~~לא נכון כי $\mathcal{F}(G)=K$~~ (אם כן ההרחבה היא הרחבת גלואה)

(ג) אם $H_1 \subset H_2$ $\mathcal{F}(H_1) \supset \mathcal{F}(H_2)$

הוכחה:

(א) אם $\sigma \in H$ אזי בפרט $\sigma \in G = Gal(L/K)$ ולכן $\sigma(x)=x$ לכל $x \in K$

ולכן $K \subseteq \mathcal{F}(H)$

$\mathcal{F}(H)$ שדה: נניח $x,y \in \mathcal{F}(H)$

$\sigma \in H$

$\sigma(x+y) = \sigma(x)+\sigma(y) = x+y$

$\sigma(xy) = \sigma(x)\cdot\sigma(y) = x\cdot y$ $\quad \sigma(x^{-1}) = x^{-1}$

(ב) כל איברי L מקובעים ע"י העתקת הזהות e

(ג) יותר אילוצים $\Leftarrow$ פחות פתרונות.

טענה 2: (א) $\{e\} \subseteq \mathcal{G}(M) \subseteq G$

$\mathcal{G}(M)$ תת חבורה.

(ב) $\mathcal{G}(L) = \{e\}$

$\mathcal{G}(K) = G$

(ג) אם $M_1 \supseteq M_2$ $\mathcal{G}(M_1) \subseteq \mathcal{G}(M_2)$

הוכחה: (א) $\mathcal{G}(M) = Gal(L/M)$ הינה תת-חבורה של $Aut(L)$ והיא מוכלת

ב: $G = \mathcal{G}(K)$

כי $M \supseteq K$

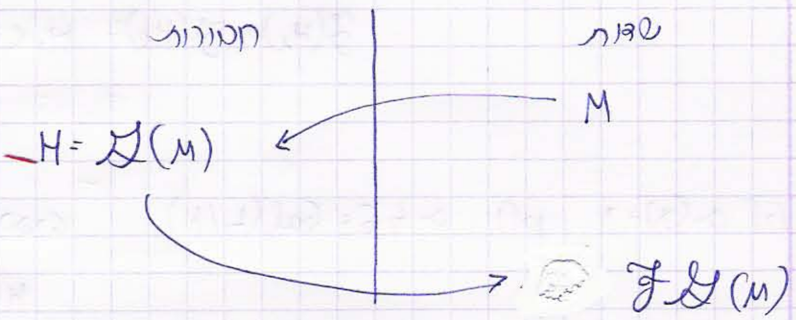
(ב) $\mathcal{G}(K) = G$ כי ההגדרה של G

$\mathcal{G}(L) = \{e\}$ כי שוב הגדרת הזהות.

(ג) יותר אילוצים $\Leftarrow$ פחות פתרונות.

טענה 3:

פינג - פונג



ובכן:

והטענה היא:

① $\mathcal{F}(\mathcal{G}(M)) \supseteq M$

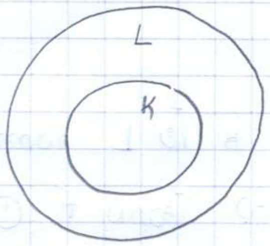
② $\mathcal{G}(\mathcal{F}(H)) \supseteq H$

אלו הן טענות טריוויאליות

29-5-2007

מבנים אלגבריים 2 - שעור מס' 12

ראינו אתמול:



יש לנו שני שדות $K \subset L$

$G = Gal(L/K)$ חבורת גלואה של ההרחבה.

כמו כן ראינו התאמה:

שדות ביניים	חבורות ביניים (תת-חבורות)
$H \longrightarrow \mathcal{F}(H)$	
$L \supseteq M \supseteq K$	$\{e\} \subseteq H \subseteq G$
$M \longrightarrow \mathcal{G}(M)$	

המשפט אליו אנו חותרים הוא:

אם L/K הרחבת גלואה $(|Gal(L/K)| = [L:K])$

אז ההתאמות הללו תהיינה הפכיות זו לזו.

ההתאמה של גלואה: Galois Correspondence

לפני כן נדבר על נורמליות

נורמליות

שדות פיצול יהיה K שדה. $f \in K[x]$ **מתפצל** ב-K אם

$$f = c(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$$

הרחבה L של K נקראת **שדה פיצול** עבור f אם:

① f מתפצל ב-L

② אם $K \subseteq L' \subseteq L$ ו-f מתפצל ב-L' אזי $L=L'$

(מה שקראנו מתפצל מינימלי)

הערה: אם f מתפצל ב-L $f=c(x-\alpha_1)\ldots(x-\alpha_n)$

אזי תת-השדה הקטן ביותר של L בו f מתפצל הינו $K(\alpha_1,\ldots,\alpha_n)$

ולכן תנאי המינימליות ② $\Longleftrightarrow$ $L=K(\alpha_1,\ldots\alpha_n)$

טענה: שדה פיצול L של f נתון קיים ואם $\deg f=n$

$$[L:K]\leq n!$$

הוכחה: באינדוקציה על n.

אם $n=1$ $L=K$

אחרת יהיה g גורם אי-פריק של f ויהיה $M = K[x]/(g)$

האיבר $\alpha_1 = x \bmod (g)$ הינו שורש של g ב-M

ולכן גם שורש של f ב-M

$$[M:K]=\deg g \leq n$$

על M $f=(x-\alpha_1)f_1$ $\deg f_1=n-1$ ומהנחת האינדוקציה

יש שדה פיצול ל-f_1 שיסומן L מעל M.

$f_1 = c(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)\ldots(x-\alpha_n)$ ב-L

$$L = M(\alpha_2,\ldots,\alpha_n) = K(\alpha_1,\alpha_2,\ldots,\alpha_n)$$

$[L:M]\leq(n-1)!$ מהנחת האינדוקציה

$$[L:K]=[L:M][M:K]\leq(n-1)!\cdot n = n!$$

▨

29-5-2007

למה: יהיה $i: K \longrightarrow \Omega$ שיכון של שדות (הומומורפיזם של שדות)

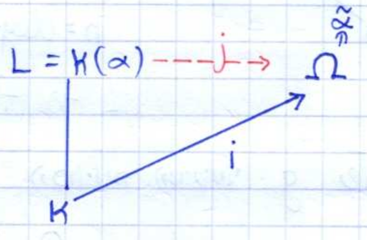
$L = K(\alpha)$ הרחבה פשוטה, הפולינום המינימלי של α = f

ונניח: $i(f)$ יש שורש

$\tilde{\alpha}$ ב-Ω אזי ניתן להרחיב את השיכון i לשיכון

$$j: L \longrightarrow \Omega$$

כך ש: $j(\alpha) = \tilde{\alpha}$



$j|_K = i$

$f \qquad i(f)$

$j(\alpha) = \tilde{\alpha}$

הוכחה: נגדיר $\varphi: K[x] \longrightarrow \Omega$

$$\varphi\left(\sum a_k x^k\right) = \sum i(a_k)\tilde{\alpha}^k$$

φ הינו הומומורפיזם $\qquad \varphi|_K = i$

$\varphi(x) = \tilde{\alpha}$

$f \in \operatorname{Ker}\varphi$

$\varphi(f) = i(f)(\tilde{\alpha}) = 0$

משרה הומומורפיזם $K[x]/(f) \xrightarrow{\bar{\varphi}} \Omega$

$$K[x]/(f) \overset{\bar{\psi}}{\cong} L$$

$$\bar{\psi}(x \bmod f) = \alpha$$

נגדיר $j = \bar{\varphi} \circ \bar{\psi}^{-1}$

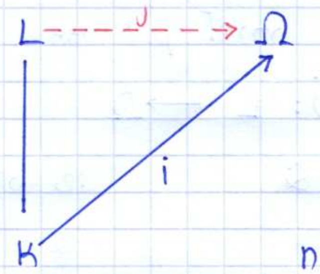
$j(\alpha) = \tilde{\alpha}$

$j|_K = i$

מסקנה: יהיה $f \in K[x]$ פולינום ויהיה L שדה פיצול שלו

אם $i: K \longrightarrow \Omega$ שיכון כך ש: $i(f)$ מתפצל ב-Ω

ניתן להרחיב את i לשיכון $j: L \longrightarrow \Omega$



הוכחה: באינדוקציה על $n = \deg f$

יהיה α_1 שורש של f ב-L

יהיה $L_1 = K(\alpha_1)$ הפולינום המינימלי g של α_1 מעל K מחלק את f

ולכן $i(g)$ מתפצל ב Ω

ובפרט יש לו גם שורש $\tilde{\alpha}_1$. מהלמה נרחיב את i לשיכון i_1

$$i_1 : L_1 \longrightarrow \Omega$$

$$i_1(\alpha_1) = \tilde{\alpha}_1$$

נחליף את K ב L_1

את i ב i_1

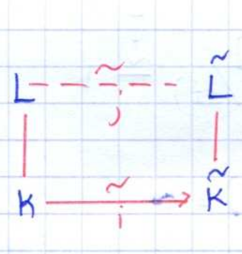
ואת f ב- $f_1 = \frac{f}{(x-\alpha_1)}$

$L =$ שדה פיצול של f_1 מעל L_1, אבל $\deg f_1$ קטנה יותר ולכן

מהנחת האינדוקציה ניתן להרחיב את i_1 ל-j כמבוקש.

מסקנה: יהיה $i: K \cong \tilde{K}$ איזומורפיזם של שדות.

$f \in K[x]$, L שדה פיצול של f, $\tilde{L}$ שדה פיצול של $\tilde{f} = i(f)$



$$f \longmapsto \tilde{f}$$

אזי יש הרחבה (לא יחידה) של i לאיזו $j: L \xrightarrow{\sim} \tilde{L}$

29-5-2007 ③

הוכחה:

ניקח את $\Omega = \tilde{L}$ בטענה הקודמת - הטענה הקודמת נותנת את קיום ההרחבה j

$j(L)$ הינו שדה פיצול של $i(f)$ כי L הינו שדה פיצול של f.

$$f = c(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$$

$$i(f) = i(c)(x-\tilde{\alpha}_1)\cdot\ldots\cdot(x-\tilde{\alpha}_n)$$

היות ו-$\tilde{L}$ היה שדה פיצול $j(L) = \tilde{L}$!

▨ הוכחת המסקנה.

נזכיר את ההגדרה של שדה פיצול:

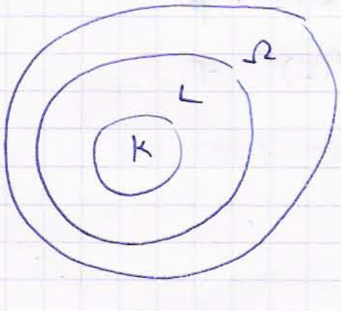
$L \supseteq K$ שדה פיצול של $f \in K[X]$ אם f מתפרק ב-L ו-L נוצר מעל K ע"י שורשי f

$L \overset{\sigma}{\cong} \tilde{L}$

$K \cong \tilde{K}$

$f \sim \tilde{f}$

למה: יהיה L שדה פיצול של פולינום f מעל K אם $K \subset L \subset \Omega$ ו-σ הינו אוטומורפיזם של Ω המקבע את K נקודתית, $\sigma \in Gal(\Omega/K)$, אזי $\sigma(L)=L$



הוכחה: נניח L שדה פיצול של f!

$f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

$f(x)=\sigma(f(x)) =$ נפעיל את σ ב-L.

$=\sigma(c)(x-\sigma(\alpha_1))\dots(x-\sigma(x_n))$

פרוק f יחיד עד כדי סדר הגורמים ולכן $\sigma(c)=c$ ו-$\sigma(\alpha_1),\dots,\sigma(\alpha_n)$

תמורה של $\alpha_1,\dots,\alpha_n$ אבל $L=K(\alpha_1\dots\alpha_n)$ ולכן לכל $x\in L$ $\sigma(x)\in L$.

▨

הגדרה: הרחבה L של K נקראית *נורמלית* אם לכל פולינום אי-פריק $f\in K[X]$

אם ל-f יש שורש אחד ב-L f מתפרק ב-L

אם x^3-2

$\mathbb{Q}(\sqrt[3]{2})$

אז $x^3-2=(x-\sqrt[3]{2})(x^2+\dots)$ כלומר הרחבה שאינה נורמלית כי הפולינום לא מתפרק

אם $\mathbb{Q}(e^{2\pi i/p})$, $e^{2\pi i/p}=\zeta$ זה כן מתפרק $\Phi_p=\prod_{a=1}^{p-1}(x-\zeta^a)$

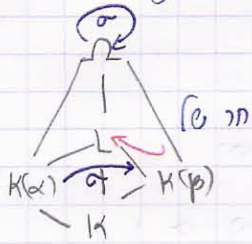
משפט: L/K הרחבה סופית אזי L/K נורמלית אם ורק אם L שדה פיצול של פולינום ב- $K[x]$.

הוכחה: $\Rightarrow$ נניח ש- L/K נורמלית.

נסמן $L=K(\theta_1,\dots,\theta_n)$ ויהיה g_i הפולינום המינימלי של θ_i מעל K. נסתכל ב- $f=g_1\cdots\cdots g_m$

כל g_i מפצל שורש ב- L ולכן מתפצל בו. לכן גם f מתפצל.

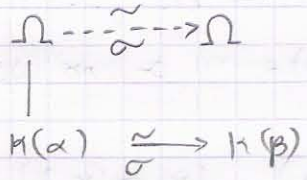
$\Leftarrow$ (לרסק, הכיוון הקשה יותר): נניח ש- L שדה פיצול של פולינום $g\in K[x]$ ויהיה f פולינום אי-פריק מעל K. יהיה Ω שדה פיצול של f מעל L. נניח α שורש של f ב- L. יהיה β שורש אחר של f ב- Ω.



$f=(x-\alpha)\cdots\cdots(x-\beta)\cdots\cdots$ ב- $\Omega[x]$

$K(\alpha)\simeq K(\beta)$ ע"י איזומורפיזם σ המעביר את α ל- β (כי שניהם איזומורפים ל- $K[x]/(f)$) ! $\sigma/K=$ הזהות.

(נסתכל בדיאגרמה:)



Ω הינו שדה פיצול של f,g מעל $K(\alpha)$ או $K(\beta)$

לפי טענה משפט שעבר ניתן להרחיב את σ לאוטומורפיזם של Ω

והיות ו- L שדה פיצול $\sigma\in Gal(\Omega/K)$; $\sigma(L)=L$ ובפרט

$\beta=\sigma(\alpha)\in L$

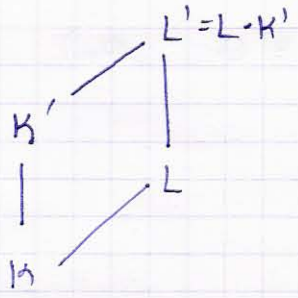
מ.ש.ל

נסיק כמה מסקנות לאור המשפט

מסקנה: יהיה $K\subset M\subset L$ מגדל של הרחבות. אזי אם L/K נורמלית.

הוכחה: L שדה פיצול של $f\in K[x]$ מעל K, לכן הוא בוודאי שדה פיצול של אותו פולינום מעל M.

מסקנה:



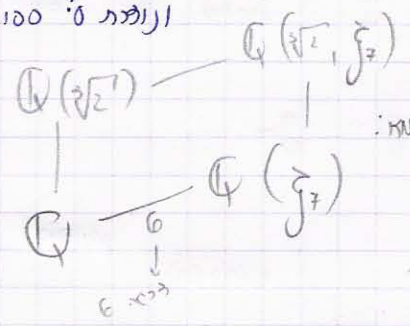
תהי L/K הרחבה סופית נורמלית.

K'/K הרחבה כלשהי (לאו דווקא אלגברית או שום דבר אחר)

אז תהי L' הרחבה של K' וגם L

הנוצרת ע"י ספוח L ו- K' (זה נקרא הקומפוזיטום = הרחבה שמכילה את שניהם ונוצרת ע"י ספוח של אחד מהם)

אזי גם L'/K' נורמלית



הוכחה: אם L שדה פיצול של f מעל K, לשם דוגמא:
אזי L' שדה פיצול של אותו f מעל K'.

מסקנה: כל הרחבה סופית ניתנת לשיכון בהרחבה נורמלית וקיימת אחת יחידה כזו קטנה ביותר והיא תקרא (סגור נורמלי)

הוכחה: נניח $L=K(\theta_1,\dots,\theta_m)$ יהיה g_i הפולינום המינימלי של θ_i.

יהיה Ω שדה פיצול למכפלת ה- g_i-ים $f=g_1\cdots g_m$ מעל L

$$K\subset L\subset\Omega$$

Ω הרחבה נורמלית סופית של K.

מצד שני בכל הרחבה נורמלית של K המכילה את L כל g_i מקבל שורש, הוא אי-פריק מעל K ולכן מתפצל ולכן f מתפצל ולכן Ω מוכל בשדה כזה (עד כדי איזומורפיזם)

שוב נסתכל שוב הדוגמא: $\mathbb{Q}(\sqrt[3]{2}, \omega)$ = שדה הפיצול של x^3-2

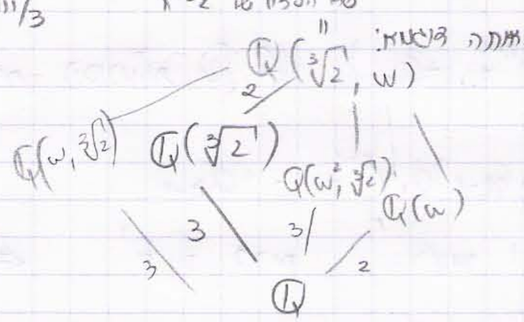
$\omega=e^{2\pi i/3}$

$\omega\sqrt[3]{2}$

$\omega^2\sqrt[3]{2}$

ω מקיים את המשוואה:

$x^2+x+1=0$



דוגמא: כל הרחבה מסדר 2 הינה נורמלית:

הוכחה: אם $L=K(\alpha)$ הרחבה מסדר 2 $\exists!$ α מקיים פולינום ריבועי מעל K

אז: $f=(x-\alpha)(x-\alpha')$

כאשר α' השורש האחר ולכן L שדה פיצול.

שאלה שהיתה מההפסקה:

$L = K(\theta_1, \dots, \theta_m)$

$|$

K

θ_i פולינום מינימלי

$g_i \in K[X]$

g_i אי-פריק

$\Leftarrow$ g_i מתפצל ב- L

$f = g_1 \cdots g_m$

(היתה כאן דיסאה קטנה שלא העתקתי)

ספרביליות

הגדרה: פולינום $f \in K[X]$ נקרא פולינום ספרבילי אם כל שורשיו בשדה פיצול שלו L, שונים.

L $c(x-\alpha_1)\cdots(x-\alpha_n)$

$|$

$K \ni f$

$\alpha_i \neq \alpha_j$

עבור $i \neq j$

(היות וכל שני שדות פיצול איזומורפיים ההגדרה לא תלויה בשדה הפיצול)

למה: תהיה f' הנגזרת הפורמלית של f. ($f = a_0x^n + a_1x^{n-1} + \dots + a_n$)

$f' = na_0x^{n-1} + (n-1)a_1x^{n-2} + \dots + a_{n-1}$ ((הנגזרת))

אז: f ספרבילי $\Longleftrightarrow$ f, f' זרים כלומר $\gcd(f, f') = 1$

הערה: אם f, אם f' הינם ב $K[X]$ והאלגוריתם האוקלידי נותן דרך פשוטה לחישוב (f, f')

הוכחה: יהיה L שדה פיצול של f ונניח

$$f=(x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}\cdots(x-\alpha_r)^{e_r}$$

כאשר α_i שונים $1\leq e_i$.

$$f'=\sum_{i=1}^{r} e_i\,(x-\alpha_1)^{e_1}\cdots(x-\alpha_i)^{e_i-1}\cdots(x-\alpha_r)^{e_r}$$

אם $1<e_i$ אז $(x-\alpha_i)^{e_i-1}$ מחלק כל מחובר ולכן מחלק את f' וכמובן גם את f והם לא זרים.

מצד שני, אם כל $e_i=1$, $(x-\alpha_i)$ אינו מחלק את f' כי הוא מחלק את כל המחוברים עם אינדקס $j\neq i$ ולא את המחובר ה-i.

[הערה: $0\neq e_i=1$]

אם $f=(x-\alpha)^p\cdot(x-\beta)$

$$f'=p(x-\alpha)^{p-1}(x-\beta)+(x-\alpha)^p$$

(כה מתאפס כי זה שדה ממציין p)

אם $e_i=1$ זה לא קורה.

אבל הגורמים הראשוניים היחידים של f ב-L הינם $(x-\alpha_i)$ $1\leq i\leq r$

ולכן אם אף אחד מהם לא מחלק את f' נובע ש $(f,f')=1$

▨

למען השלמות פרק הסיר:

$(f,f')=1$ בין אם מסתכלים ב- $K[x]$ או אם מסתכלים ב $L[x]$. (כי אנחנו מחשבים gcd באמצעות אלגוריתם אוקלידס)

יש כאן כמה מסקנות יפות:

מסקנה: ב(שדה מעל) מציין 0, פולינום אי-פריק הינו ספרבילי.

הוכחה: יהיה $f\in K[x]$ אי-פריק, $\deg f=n$ $\deg f'=n-1$

מכאן $f'\neq 0$ ולכן (f,f') הינו פולינום המחלק את f מדרגה $\leq n-1$ ומאי-פריקות f הוא 1.

דוגמא: $K=\mathbb{F}_p(t)$

$$f\in K[x]$$

$$f=x^p-t$$

f אי-פריק (קריטריון אייזנשטיין ביחס לראשוני t בחוג $\mathbb{F}_p[t]$)

אבל בשדה סגור אם $x^p=t$ $\quad f=(X-x)^p$

במקרה זה $\quad f'=pX^{p-1}=0$

ולכן $(f,f')=(f,0)=f$

f אי-פריק אבל לא ספרבילי.

הגדרה: תהיה L/K הרחבה אלגברית. איבר $\alpha\in L$ נקרא ספרבילי מעל K אם הפולינום המינימלי שלו מעל K ספרבילי.

דוגמא: כל איברי K ספרביליים מעל K.

במציין 0 כל איבר ספרבילי (כי פולינום מינימלי הינו אי-פריק)

ההרחבה L/K ספרבילית אם כל $\alpha\in L$ ספרבילי מעל K.

טענה: $K\subset M\subset L$: L/K ספרבילית

$\Rightarrow$ L/M ספרבילית

M/K ספרבילית

הוכחה: אם $\alpha\in L$ הפולינום המינימלי של α מעל M מחלק את הפולינום המינימלי של α מעל K ולכן אם האחרון ספרבילי, גם הראשון כזה.

L/K ספרבילי $\Longleftrightarrow$ כל איברי L ספרביליים מעל K

$\Downarrow$

M/K ספרבילית $\Longleftrightarrow$ גם איברי M ספרביליים מעל K

$\blacksquare$

4-6-2007

מבנים אלגבריים 2 - שעור מס' 14

(1)

בשעורים הקודמים דיברנו על L/K הרחבה סופית, $G=Gal(L/K)$

לאחר מכן דיברנו על מושגי הנורמליות והספרביליות. ראינו כי לפעמים מקבלים חבורה שגודלה כדרגת ההרחבה ולפעמים פחות וזה כי:

(1) היו שורשים מחוץ ל-L

או

(2) השורשים של הפולינום האי-פריק לא היו שונים זה מזה.

עתה נראה שאם לכל פולינום אי-פריק לא מתקיימים לא (1) ולא (2) אז זה יסתדר

(אנחנו כל הזמן מניחים L/K סופית, $G=Gal(L/K)$)

משפט: תהי L/K סופית, $G=Gal(L/K)$. אזי $|G| \le [L:K]$

ושוויון קיים אם ורק אם L/K נורמלית וספרבילית

הגדרה: ההרחבה L/K תקרא הרחבת גלואה אם $|G|=[L:K]$

מסקנה: המשפט הנ"ל אומר כי גלואה = נורמלי וספרבילי.

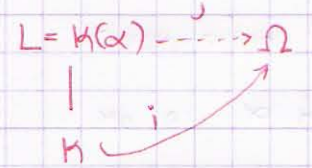
למה: (כבר הוכחנו אותה) תהי $L=K(\alpha)$ הרחבה פשוטה, f הפולינום (המינימלי) של α,

$i: K \hookrightarrow \Omega$ שיכון.

אז ההרחבות של i לשיכון $j: L \hookrightarrow \Omega$ הינן בהתאמה חח"ע עם שורשי $i(f)$ ב-Ω.

הוכחה: (תזכורת)

* ראינו שאם $\bar{\alpha}$ שורש של $i(f)$, אז ההעתקה $K[x] \xrightarrow{\varphi} \Omega$ כך ש $\varphi|_K = i$, $\varphi(x)=\bar{\alpha}$, משרה $\bar{\varphi}: K[x]/(f) \to \Omega$



* מצד שני יש איזומורפיזם $\tilde{\varphi}: K[x]/(f) \cong L$ ועכשיו להגדיר $j = \bar{\varphi} \circ \tilde{\varphi}^{-1}$ כך ש $j(\alpha)=\bar{\alpha}$.

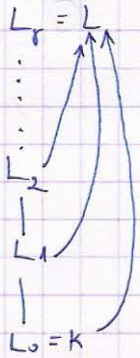
* מצד שלישי: כל שיכון צריך לקיים $0=j(f(\alpha))=i(f)(j(\alpha))$, ולכן חייב להיות שורש של $i(f)$.

מסקנה: מס' ההרחבות של i הינו $\le [L:K]$ ושוויון קיים $\Longleftrightarrow$ α ספרבילי מעל K, $i(f)$ מתפרק ב-Ω

הוכחה: אי שוויון: מס' ההרחבות השונות j של i הינו כמס' שורשי $i(f)$ ב-Ω

ומס' זה חסום ע"י: $\deg f = [L:K]$

שוויון: $i(f) \Longleftrightarrow$ מתפרק ב-Ω לגורמים ליניאריים שונים.



הוכחת המשפט: היות ו- L סופית מעל K $L=K(\alpha_1,\dots,\alpha_r)$

נסמן: $L_0=K$; $L_i=K(\alpha_1,\dots,\alpha_i)$ $L_i=L_{i-1}(\alpha_i)$ וניקח $\Omega=L$ בלמה.

הערה: * שיכון של L בעצמו שהינו הרחבה של K ≡ אוטומורפיזם של L/K

* מספר הדרכים להרחיב שיכון נתון של L_{i-1} לשיכון של L_i $\leq [L_i:L_{i-1}]$

ומס' הדרכים הכולל הינו $\leq [L:K]=[L_1:L_0]\cdot[L_2:L_1][L_3:L_2]\dots[L_r:L_{r-1}]$

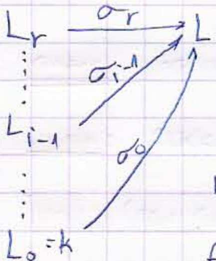
נניח עתה כי L/K נורמלית וספרבילית: משלב ה-i α_i ספרבילי מעל L_{i-1}.

הפולינום המינימלי של α_i מעל L_{i-1} גם כן מתפצל ב-L.

מהלמה, מס' הדרכים להרחיב כל שיכון של L_{i-1} לשיכון של L_i הוא מדויק $[L_i:L_{i-1}]$

ולכן מס' השיכונים של L בעצמו המרחיבים את הזהות של K הינו מדויק $[L:K]$.

נקודה עדינה: (שאמורה להיות באמצע ההוכחה אך הועברה לסוף על מנת שלא יסבך הרצף):



מס' ההרחבות של σ_{i-1} לשיכון σ_i של L_i ב-L

הינו מס' השורשים של $\sigma_i(g)$ (כאשר g הוא הפולינום

המינימלי של α_i מעל L_{i-1}).

יהי f הפולינום המינימלי של α_i מעל K, $g|f \Rightarrow \sigma_{i-1}(g)|\overbrace{\sigma_{i-1}(f)}^{f} \Rightarrow \sigma_{i-1}(g)|f$.

אם L נורמלית מעל K, f מתפצל לחלוטין ב-L (מקבל שורש אחד ולכן מתפצל)

$\Rightarrow \sigma_{i-1}(g)$.

* בעצם ההערה קיימת כיוון שבמשפט לא התייחסנו לשיכון אלא להרחבה.

המשך הוכחת המשפט: נניח ש- L/K אינה נורמלית וספרבילית: (עלינו להוכיח $|G|<[L:K]$)

אז יהי α איבר ב-L שהפולינום המינימלי שלו מעל K או אי-ספרבילי או ספרבילי

אך לא מתפצל ב-L (או שלא מתפצל לגורמים לינאריים, או שכן מתפצל לגורמים לינאריים

אך שאינם שונים זה מזה)

נבחר בהוכחה הקודמת $\alpha_1=\alpha$ ונשלים לקבוצת יוצרים $\alpha_1,\dots,\alpha_r$ כמקודם

במקרה זה, מס' ההרחבות של K ב-L לשיכון של L_1 כבר $<[L_1:K]$ (קטן ממש)

מכאן שמס' השיכונים של L בעצמו (המרחיבים את הזהות של K) $<[L:K]$

∎

4-6-2007 (2)

מסקנה: תהי L/K הרחבת גלואה. אזי לכל שדה ביניים $L \supseteq M \supseteq K$ מתקיים:

(1) L/M גם כן גלואה

(2) $|Gal(L/M)| = [L:M]$

(3) $|\mathcal{L}(M)| = [L:M]$

הוכחה: הראינו שנורמליות וספרביליות "עוברות בירושה" מ- L/K ל- L/M

ועתה - נמשיך לכיוון אחר...

נושא כיוון: נתחיל מחבורות ונגיע לשדות:

נתון מערכון חבורה סופית כלשהי G של אוטומורפיזמים של L $G \subseteq Aut(L)$

נסמן $K = \mathcal{F}(G) = \{x \in L \mid \forall \sigma \in G \ \ \sigma(x) = x\}$ - שדה השבת

משפט: בתנאים הנ"ל: $|G| \geq [L:K]$ (ההוכחה מהשעון)

מסקנה מהמשפט: במצב הזה $|G| = [L:K]$, $G = Gal(L/K)$, L/K גלואה.

הוכחה: ראשית, מהמשפט נובע ש L/K הרחבה סופית. כמו-כן $G \subset Gal(L/K)$

מהמשפט הקודם $|Gal(L/K)| \leq [L:K]$

מהמשפט החדש $|G| \geq [L:K]$

L
$|$ a
K

ולכן נקבל שוויונות במקום אי-שוויונות $\Longleftarrow G = Gal(L/K)$

הערה: אם $G = \{\sigma_1, \dots, \sigma_m\}$ - ו $|G| = m$ ו $\sigma \in G$

אזי $\sigma\sigma_1, \sigma\sigma_2, \dots, \sigma\sigma_m$ פרמוטציה של $\sigma_1, \sigma_2, \dots, \sigma_m$

משפט: (שוב) $|G| \geq [L:K]$ - בתנאים שקודם צויינו

הוכחה: יהיה $K = \mathcal{F}(G)$ שדה השבת של G.

נניח בשלילה כי $|G| < [L:K]$

אזי ניתן לבחור n איברים $\omega_1, \dots, \omega_n$ מתוך L שהם בלתי תלויים לינארית

מעל K כאשר $n > m$ (אנו עדיין לא יודעים שההרחבה היא סופית ולכן עדיין לא יודעים שיש מימד סופי)

נתבונן במטריצה $\sigma_i(\omega_j)$:

$$\begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \dots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \dots & \sigma_2(\omega_n) \\ \vdots & & & \\ \sigma_m(\omega_1) & \sigma_m(\omega_2) & \dots & \sigma_m(\omega_n) \end{pmatrix}$$

המטריצה מתקבלת מהפעלת כל האוטומורפיזמים שבחבורה של G על אותם איברים

מה״ל מ-א.

כלומר יש c_j כך ש:

$n > m$ ולכן יש תלות לינארית בין עמודות המטריצה (עם מקדמים מ-L): $\sum_{j=1}^{n} c_j\sigma_i(w_j)=0$

כאשר $1\le i\le m$, $c_j\in L$.

מבין כל התלויות הלינאריות בין עמודות המטריצה, נבחר כזו שמערבת מינימום של עמודות.

עכשיו נניח, אחרי סידור מחדש של w_j-ים, שהיא תלות לינארית בין r העמודות הראשונות. (כלומר r העמודות הראשונות ת״ל אם כל קבוצה של $r-1$ מביניהן בת״ל)

בה״כ $\sum_{j=1}^{r} c_j\sigma_i(w_j)=0$ $(1\le i\le m)$ - כאשר כל ה-c_j-ים אינם אפס (עבור $1\le j\le r$)

נחלק את התלויות הלינאריות ב-c_1 $(\neq 0)$ וכך נקבל $c_1=1$

נפעיל את אחת ה-$\sigma\in G$ על התלות: $\sum_{j=1}^{r}\sigma(c_j)\sigma\sigma_i(w_j)=0$ (כמובן שפועל גם על מקדמי המטריצה וגם על המקדמים)

היות ו-$\{\sigma\sigma_i\}$ פרמוטציה של $G=\{\sigma_i\}$, נקבל כי

$$\sum_{j=1}^{r}(\sigma(c_j)-c_j)\sigma_j(w_j)=0$$ (אחרי סידור חדש)

כעת נחסר את התלות המקורית שהנחנו מהתלות החדשה ונקבל:

$$\sum_{j=1}^{r}(\sigma(c_j)-c_j)\sigma_i(w_j)=0$$ (לכל $1\le i\le m$)

$c_1=1$ ולכן $\sigma(c_1)-c_1=0$ ולכן זוהי תלות לינארית בין $r-1$ העמודות $2\le j\le r$

אבל הנחנו שהעמודות הנ״ל בלתי תלויות לינארית (הנחת המינימליות של r) ולכן $\sigma(c_j)=c_j$

זה נכון לכל $\sigma\in G$, ולכן $c_j\in\mathcal{F}(G)=K$ ⟵ שייך לשדה השבת של G.

מהתלות המקורית נקבל $0=\sum_{j=1}^{r}c_j\sigma_i(w_j)\overset{*}{=}\sigma_i\left(\sum_{j=1}^{r}c_jw_j\right)$ (* כי אוטומורפיזם ומקבע את c_j)

מכאן, נקבל $\sum_{j=1}^{r}c_jw_j=0$ בסתירה לאי-תלות ה-w_j מעל K.

לכל מי שקורא את ההרצאה הזו,

זה סיכום שהתעדכנתי והשלמתי. אני אבדוק אותו שוב עבור

נוסף ובעריכה ויש טעויות אתקן אותן...

5-6-2007 (1)

מבנים אלגבריים 2 - שעור מס' 15

אז מה היה לנו עד כה? K/L הרחבה סופית.

<u>משפט 1:</u> $G=Gal(L/K)$, $|G|\le[L:K]$ ושיוויון $\Longleftrightarrow$ L/K נורמלית וספרבילית.

<u>משפט 2:</u> L שדה כלשהו, G חבורה סופית של אוטומורפיזמים של L,

$K=\mathcal{F}(G)$ - שדה השבת של G (איברים של L שמתחת לאחר G לא זזים)

אזי $[L:K]\le|G|$

<u>ההתאמה של גלואה:</u> תהי L/K הרחבת גלואה, $G=Gal(L/K)$

* הגדרות: אם $K\subseteq M\subseteq L$ שדה ביניים $\mathcal{G}(M)=Gal(L/M)=\{\sigma\in G \mid \forall x\in M\ \sigma(x)=x\}$

* אם $\{e\}\subseteq H\subseteq G$ $\mathcal{F}(H)=\{x\in L \mid \forall\sigma\in H\ \sigma(x)=x\}$

(שימו לב: ההגדרות הן תמיד קיימות (גם להרחבות שהן לא גלואה), המשפט שההתאמות אלו הפכיות כ"ל נכון רק להרחבת גלואה.)

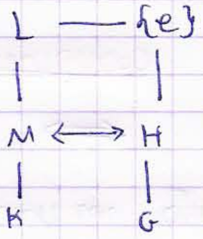
* <u>המשפט היסודי של תורת גלואה:</u>

תהי L/K הרחבת גלואה, $G=Gal(L/K)$

(א) ההעתקות $\mathcal{F}$ ו- $\mathcal{G}$ הפכיות זו לזו: $\mathcal{F}\mathcal{G}(M)=M$, $\mathcal{G}\mathcal{F}(H)=H$

כלומר $\mathcal{F}$ ו- $\mathcal{G}$ הן התאמות חח"ע ועל בין משפחת שדות הביניים ומשפחת תת החבורות.

(ב) ① $[L:M]=|\mathcal{G}(M)|$ ② $[L:\mathcal{F}(H)]=|H|$



<u>מסקנה:</u> אם G חבורה סופית של אוטומורפיזמים של L $[L:\mathcal{F}(G)]=|G|$

$G=Gal(L/K)$ $K=\mathcal{F}(G)$

משפט 1 ↘ משפט 2 ↙

$|Gal(L/K)|\le[L:K]\le|G|$

<u>הוכחת המשפט היסודי:</u>

(ב) * ראינו כבר L/K גלואה $\Longleftarrow$ L/M גלואה $\Longleftarrow$ $[L:M]=|Gal(L/M)|$

* השיוויון השני הינו המסקנה האחרונה (מיושמת ל- H במקום ל- G)

המשך $\longleftarrow$

(א) ידוע כי $\mathcal{G}\mathcal{F}(H)\supseteq H$ (זהו טאוטולוגיה)

$|H| \overset{②}{=} [L:\mathcal{F}(H)] \overset{①}{=} |\mathcal{G}\mathcal{F}(H)| \Rightarrow \mathcal{G}\mathcal{F}(H)=H$ ז"א כמובן שכל איבר של H מקבע את כל איברי השדה שמקובעים ע"י H, ואין עוד.

כמובן שהמעברים האלה לא נכונים לחבורה שאינה גלואה.

$[L:\mathcal{F}\mathcal{G}(H)] \overset{②}{=} |\mathcal{G}(M)| \overset{①}{=} [L:M]$

עוד טאוטולוגיה: $K\subseteq M\subseteq \mathcal{F}\mathcal{G}(M)\subseteq L \Rightarrow M=\mathcal{F}\mathcal{G}(M)$

השלמה למשפט היסודי:

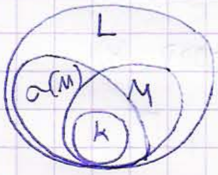
משפט: במצב שתואר במשפט היסודי; $M=\mathcal{F}(H)$, $H=Gal(L/M)$:

M/K נורמלית $\Leftrightarrow$ H נורמלית ב-G

ואז M/K בכלל גלואה $Gal(M/K)\cong G/H$

הגדרה: נורמליות: $H\lhd G$ (נורמלית) אם לכל $\alpha\in G$ $\alpha H\alpha^{-1}=H$ (החבורה הצמודה ל-H ע"י α)

למה: אם $M=\mathcal{F}(H)$; $\alpha\in G$, אזי $\alpha(M)=\mathcal{F}(\alpha H\alpha^{-1})$ ← (מצמידים את החבורה והשדה נותר ע"י α)



K ו-L נשארים מקובעים

הוכחה: $x\in\mathcal{F}(\alpha H\alpha^{-1})$

$\forall h\in H\ h\alpha^{-1}(x)=x \Leftrightarrow \forall h\in H\ h\alpha^{-1}(x)=\alpha^{-1}(x)$

$\alpha^{-1}(x)\in\mathcal{F}(H)=M$

$x\in\alpha(M)$.

הוכחת המשפט: H נורמלית $\Leftrightarrow$ $\forall\alpha\in G\ \alpha H\alpha^{-1}=H$

$\Leftrightarrow \alpha(M)=M\ \forall\alpha\in G$ ← מהלמה. המשך ההוכחה.

ראינו כבר קודם מהספר שאם M נורמלית אז $\alpha(M)=M$

מאידך אם M לא נורמלית נבחר $\alpha\in M$ כך שקיים השורשים β של הפולינום המינימלי שלו מחוץ ל-M

$\beta\notin M$, $\alpha\in M$, נרחיב את האיזומורפיזם (מעל K) $K(\alpha)\cong K(\beta)$

לאוטומורפיזם α של L אזי $\beta=\alpha(\alpha)\in M$ $\alpha(M)\neq M$

המשך ההוכחה בעמוד הבא.

המשפט הבא יש עוד תנאי - רק לבונה נורמלי + ספרבילי

אנחנו עוסקים בהרחבה $L|K$ הרחבת גלואה (סופית) $n=[L:K]$

והראינו את המשפט היסודי, שיש לנו התאמה בין:

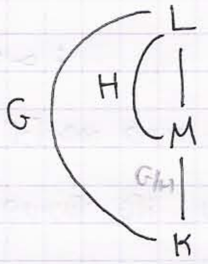
$$\left\{\text{תח"ש של } G\right\} \underset{g}{\overset{f}{\longleftrightarrow}} \left\{\begin{matrix}\text{שדות ביניים} \\ M \\ K\subset M\subset L\end{matrix}\right\}$$

$G = Gal(L|K)$ הסדר של G הוא דרגת ההרחבה $|G|=n$

$$f(H)=\{x\in L \mid \alpha(x)=x \ \ \forall\alpha\in H\}$$

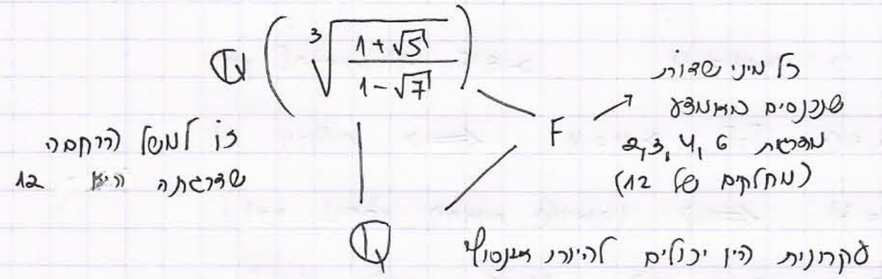
$$g(M)=Gal(L|M)=\{\alpha\in G \mid \alpha(x)=x \ \ \forall x\in M\}$$

$H = Gal(L|M)$



מסקנה: (מהמשפט היסודי שאינה מובנת מאליו):

(מהתאמת גלואה) להרחבת גלואה סופית יש רק מס' סופי של שדות ביניים.



הוכחת המסקנה: כי יש רק מס' סופי של תת-חבורות ל-G.

טיפ מהמרצה: לחזור על החומר של חבורות ציקליות, אבליות ופתירות כי נצטרך את זה לשיעורים הבאים.

נראה כי $M|K$ אינה צריכה להיות גלואה.

משפט: $M|K$ גם כן גלואה ($\equiv$ נורמלית) $\iff H \lhd G$
$H = Gal(L/M)$
(H היא החבורה שמתאימה ל- $L \backslash M$)

ואז $Gal(M|K) \cong G/H$

הוכחה:

למה: לכל $H \subseteq G$ (כל תת-חבורה) $\mathcal{F}(\alpha H \alpha^{-1}) = \alpha \mathcal{F}(H) \quad \forall \alpha \in G$

הוכחת הלמה:

$$x \in \mathcal{F}(\alpha H \alpha^{-1}) \iff$$

$$\forall h \in H \quad \alpha h \alpha^{-1}(x) = x \iff$$

$$\forall h \in H \quad h\alpha^{-1}(x) = \alpha^{-1}(x) \iff \quad // \alpha^{-1}$$

אם מפעילים α^{-1} משני הצדדים

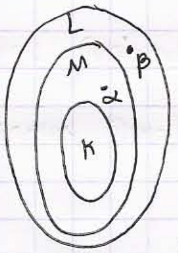
$$x \in \alpha(M) \iff \alpha^{-1}(x) \in \mathcal{F}(H) = M$$

הוכחת המשפט: M גלואית $\iff \alpha M = M$ לכל $\alpha \in G$:

אם $\alpha \in G$, אז ראינו כבר ש- $\alpha M = M$ לכל שדה ביניים נורמלי.

להיפך, אם M אינה נורמלית יש $\alpha \in M$ שפולינום המינימלי שלו מעל K

שיסומן f יש שורש אחר $\beta \in L \backslash M$



ישנו איזומורפיזם $K(\alpha) \cong K(\beta)$ המעביר את $\alpha \longmapsto \beta$

ממשפט הרחבת האיזומורפיזם מאחר ש- L גלואית (נורמלית)

ניתן להרחיבו ל- $\alpha \in G$ כי $\alpha M \neq M \quad \alpha\alpha = \beta$

M נורמלית $\iff \alpha M = M$ לכל $\alpha \in G \iff \mathcal{G}(\alpha M) = \mathcal{G}(M) \quad \forall \alpha \in G$

(וזה מתח"ע התאמת גלואה) $\iff \alpha H \alpha^{-1} = H$ לכל $\alpha \in G$ (מהלמה)

כלומר $H \lhd G$ (H נורמלית ב- G)

איך נחשב כעת הנה את $Gal(M|K)$?

נניח אם כן $M|K$ גלואה. לכל $\alpha \in G$ $\alpha|_M$ משרה איבר של $Gal(M/K)$

נסמן $\bar{\alpha} = \alpha|_M$

$$\overline{\alpha\tau} = \bar{\alpha}\bar{\tau}$$

ולכן ההעתקה $\alpha \longrightarrow \bar{\alpha}$ הינה הומומורפיזם של חבורות $Gal(L|K) = G \longrightarrow Gal(M/K)$

11-6-2007

נראה מהו הגרעין שלו:

$$\sigma\in H \iff \sigma|_M = e \iff \bar{\sigma} = e \text{ ---- (הזהות)}$$

מהמשפט היסודי של ההומומורפיזם $G/H \hookrightarrow Gal(M/K)$ (כלומר חח"ע מתקיים)

נשאר עכשיו לבדוק מה עם על:

כדי להראות שזה "על" מספיק להראות שכל אוטומורפיזם של M/K ניתן להרחבה ל- $\sigma\in G$ וזה נובע משפט הרחבת האיזומורפיזם

בדרך אחרת להראות שזה "על": פשוט לספור:

$$|G/H| = \frac{|G|}{|H|} = \frac{[L:K]}{[L:M]} = [M:K] = |Gal(M/K)|$$

(מכפליות הדרגה)

ולכן משיקולי ספירה

$$\boxed{G/H \cong Gal(M/K)}$$

לפני שנתחיל עם דוגמאות נזכיר כמה הגדרות:

<u>טרמינולוגיה:</u>

* אם $f\in K[x]$ פולינום אי-פריק (ומתפצל ב- L) ואם α,β הם שורשים של f ב- L אזי אומרים ש α, β <u>צמודים זה לזה</u>

אם למשל:

$\mathbb{C}/\mathbb{R}$

$0 = x^2+x+10$ זהו פולינום שאינו פריק מעל $\mathbb{R}$

השורשים שלו הם: $\alpha,\beta = \frac{-1\pm\sqrt{39}}{2}$ שני שורשים מרוכבים

ב- $\mathbb{C}$:

$\alpha = \bar{\beta}$

$\beta = \bar{\alpha}$

* אם $f \in K[x]$ פולינום אי-פריק ספרבילי ששדה הפיצול שלו הוא L אז $G = Gal(L/K)$ נקראית גם חבורת גלואה של הפולינום ומסומנת גם $G(f)$

אם $f=(x-\alpha_1)\cdots(x-\alpha_n)$ (מניחים f מתוקן) (הפיצול של f ב- L) אזי $L = K(\alpha_1,\dots,\alpha_n)$

ולכל $\sigma\in G$ σ משרה תמורה $\pi(\sigma)$ של השורשים:

$$f = \sigma f = (x-\sigma\alpha_1)(x-\sigma\alpha_2)\cdots(x-\sigma\alpha_n)$$

$\alpha = e \iff \pi(\alpha) = e$

($\alpha\alpha_i = \alpha_i$ לכל i) ולכן π מגדיר לנו את G כתת-חבורה של S_n.

$\boxed{G \subseteq S_n}$ G משוכנת ב-S_n אבל בדר"כ רחוקה מלהיות S_n כולה.

$[L:K] = |G|$
$\leq n!$ (אפילו מחלק את $n!$)

מה הסקנה מישהו שאל איך המונחים של גלואה של ספרביליות ונורמליות מתנהגים

התרחבות במגדל: L/K גלואה $\Rightarrow$ L/M גלואה

(M/K ספרבילית

אבל לאו דווקא נורמלית)

האם ניתן להסיק משהו על ההרחבה הגדולה אם יודעים משהו על שתי הקטנות?

הערה חשובה: נתון: M/K גלואה

L/M גלואה

לא נובע ש: L/K גלואה.

להלן דוגמא:

הרחבות ריבועיות במציין 0 הן תמיד גלואה.

למשל: $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ / 2 / $\mathbb{Q}(\sqrt{2})$ / 2 / $\mathbb{Q}$ (גלואה, גלואה)

..... צריך לבדוק $1+\sqrt{2} \neq (a+b\sqrt{2})^2$ (אנו מראים שמקבלים סוג הרחבה) $(a,b \in \mathbb{Q})$

אם זה נכון אז:

$$\begin{cases} 1 = a^2 + 2b^2 \\ 1 = 2ab \end{cases}$$

מחלקים ומראים שאין פתרון רציונלי

(נטען כי ההרחבה הגדולה אינה גלואה)

11-6-2007

דוגמא:

$\mathbb{Q}(\sqrt{3+2\sqrt2})$
|
$\mathbb{Q}(\sqrt2)$
↓
$\mathbb{Q}$

$\sqrt{3+2\sqrt2} = 1+\sqrt2$ מקרה ריצה

ולכן לא יצרנו שום שדה חדש ואין פה מאמת הרחבה של השדה.

זאת דוגמא לשונה מן ~~זה~~ כדוגמת הרחבה

נעשה את הדוגמא הקודמת:

<u>טענה:</u> $L=\mathbb{Q}(\sqrt{1+\sqrt2})$ איננו גלואה מעל $\mathbb{Q}$

<u>הוכחה:</u> $L\subseteq\mathbb{R}$

יהיה σ האוטומורפיזם הלא טריויאלי של $\mathbb{Q}(\sqrt2)$ $\quad \sigma(\sqrt2)=-\sqrt2$

$$\sigma(1+\sqrt2)=1-\sqrt2$$

נסמן $\alpha=\sqrt{1+\sqrt2}$. אי-אפשר להרחיב את σ לאוטומורפיזם של L

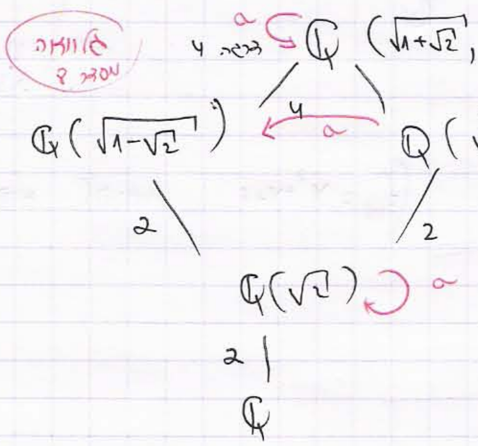
אילו היה ניתן $\sigma(\alpha)^2=\sigma(\alpha^2)$

$$=\sigma(1+\sqrt2)=1-\sqrt2<0$$

$$\sigma(\alpha)\notin\mathbb{R}$$

אם נרצה להרחיב את השדה כדי שהוא כן יהיה גלואה

דרך למשל:



נחזור עכשיו לדוגמא שכבר עסקנו בה

דוגמא: $f=x^3-2$

(א) ראינו כי f ב-$\mathbb{Q}[x]$ אי-פריק (אייזנשטיין)

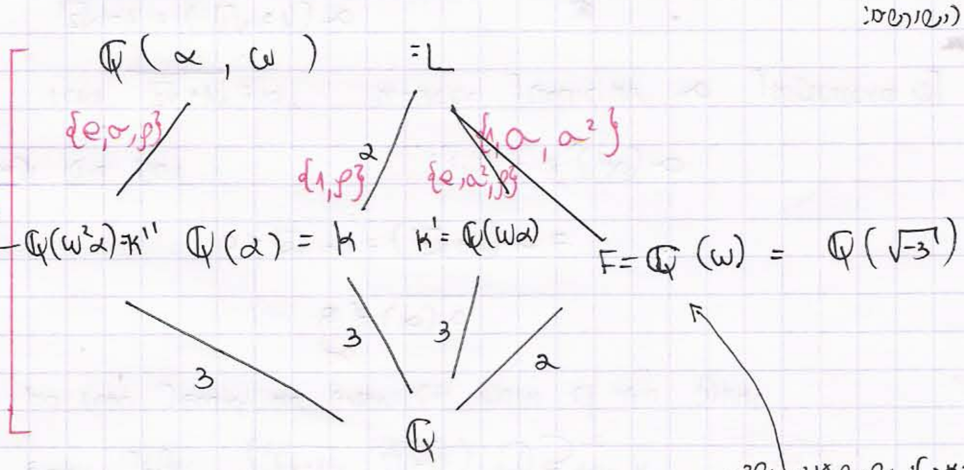
נסמן $\alpha=\sqrt[3]{2}$ ואנו יודעים כי $K=\mathbb{Q}(\alpha)$ הרחבה מדרגה 3

$$\begin{array}{c} K \\ 3 \,| \\ \mathbb{Q} \end{array}$$

$\omega\alpha,\ \omega^2\alpha$

$$\omega=e^{2\pi i/3}=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}=-\frac{1}{2}+\frac{i\sqrt{3}}{2}$$

ולכן שדה הפיצול של הפולינום מתקבל ע"י סיפוח שלושת השורשים:



← אלו הם 3 שדות איזומורפיים כי הם מתקבלים ע"י הוספה של 3 שורשים שונים לאותו הפולינום

כאן מראה לי שיש עוד שדה ביניים אמצע הבניה

$[L:K]=2$

כי $[L:\mathbb{Q}]$ מתחלק ב-2 וגם $[K:\mathbb{Q}]=3$ זר ל-2 ולכן $[L:K]$ מתחלק ב-2. מאידך הוא לכל היותר 2 כי ω מקיים $x^2+x+1\in K[x]$

(דרך אחרת היא להראות $f_\omega=x^2+x+1$)

אז כל דרגת ההרחבה $[L:\mathbb{Q}]=6$

המשך הדוגמא בעמוד הבא:

11-6-2007

נתחיל עכשיו לדון ב- $G=Gal(L|K)$ (עדיין מאותה דוגמא)

נתבונן עליה כחבורת תמורות של x^3-2:

$$|G|=6$$

$$G\subset S_3$$

נבדוק התמורות שהיא משרה על $\{\alpha,\omega\alpha,\omega^2\alpha\}$

משיקולי ספירה $G=S_3$ (כל תמורה של 3 השורשים צריכה להתקבל)

השורשים

G	α	$\omega\alpha$	$\omega^2\alpha$
e	α	$\omega\alpha$	$\omega^2\alpha$
ρ	α	$\omega^2\alpha$	$\omega\alpha$
σ	$\omega\alpha$	$\omega^2\alpha$	α
σ^2	$\omega^2\alpha$	α	$\omega\alpha$
$\sigma\rho$	$\omega\alpha$	α	$\omega^2\alpha$
$\sigma^2\rho$	$\omega^2\alpha$	$\omega\alpha$	α

לאן הם נשלחים

נסמן ב- σ את האוטומורפיזם של L/F כך ש: $\sigma(\alpha)=\omega\alpha$

$$\sigma(\omega\alpha)=\sigma(\omega)\sigma(\alpha)=\omega\cdot\omega\alpha=\omega^2\alpha$$

$$(\sigma\rho)(\omega\alpha)=\sigma(\omega^2\alpha)=\alpha$$

$$(\sigma^2\rho)(\omega\alpha)=\sigma^2(\omega^2\alpha)=\omega\alpha$$

$$\sigma\rho(\omega^2\alpha)=\omega^2\alpha$$

$$\boxed{\rho\sigma\rho^{-1}=\sigma^2}$$

ב- G יש 3 תמורות מסדר 2 (צמודות זו לזו)

$\{e,\rho\}$

$\{e,\sigma,\rho\}$

$\{e,\sigma^2,\rho\}$

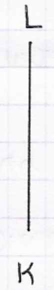
ותמונה אחת מסדר 3 (נורמלית) והיא $\{e,\sigma,\sigma^2\}$

ולכן אלו הם כל תתי השדות: F, K, K', K'', L, Q

היו לנו הרחבות, ניחשנו תתי שדות

מצאנו את צו חבורת גלואה

וחישבנו את היוצרים.

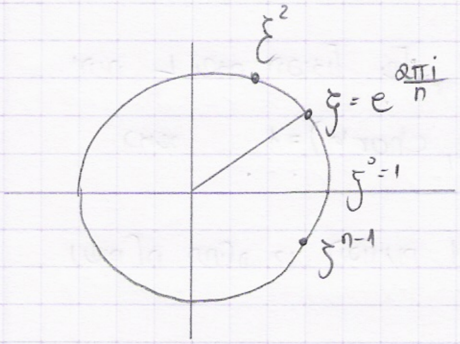


נעשה עכשיו את התהליך מסוף דוגמא:

K שדה שמציין זר ל-n

L = שדה הפיצול של x^n-1

L נקרא הרחבה ציקלוטומית של K והסיבה היא:



$$(x^n-1)=(x-1)(x-\zeta)\dots(x-\zeta^{n-1})$$

למה: אם F שדה $W \subseteq F^*$ תת-חבורה סופית של החבורה הכפלית של F אזי W ציקלית.

מסקנה: אם F שדה סופי, F^* ציקלית

הוכחה: W הינה חבורה אבלית סופית ולכן הינה מכפלה של תת-חבורות סילו שלה, לכל p המחלק את $n=|W|$.

$p^e \| n$ (p ראשוני)

נסמן $W=\prod_{p|n} W_p$

$|W_p| = p^e$, אם נוכיח W_p ציקלית (אז מכפלה של חבורות ציקליות מסדרים זרים גם תהיה)

אז W ציקלית כתוצ' מכפלה של חבורות ציקליות מסדרים זרים זה לזה.

נניח אם כן $|W|=p^e$.

אם יש ב-W איבר מסדר p^e בדיוק, אזי סיימנו $\longrightarrow$ W ציקלית

אחרת, לכל $x \in W$ $x^{p^{e-1}}=1$

אבל בשדה F למשוואה הנזכרת יש לכל היותר p^{e-1} שורשים, סתירה ל- $|W|=p^e$

(לכן חייב להיות איזשהו איבר מסדר p^e)

∎

אם $|W|=n$ אז כל איברי W מקיימים $x^n=1$ והם כל שורשי היחידה מסדר n.

יוצר של W נקרא שורש יחידה פרימיטיבי מסדר n (והמשפט אומר שיש כאלה)

הערה: אם $n=p$ ראשוני אז תת-החבורות היחידות של W הן W ו-$\{1\}$

ולכן יש $p-1$ שורשי יחידה פרימיטיביים.

אם $|W|=p^2$ (ונראה כי זוהי חבורה ציקלית)

במקרה זה יש ל-W תת-חבורה אחת מסדר p ולכן יש ב-W איבר אחד מסדר 1

$p-1$ איברים מסדר p

p^2-p איברים מסדר p^2

אלו שורשי יחידה פרימיטיביים.

יהיה L שדה הפיצול של x^n-1 מעל K

כאשר $(n, \text{char}K)=1$

נשים לב תחילה כי הפולינום $(x^n-1, nx^{n-1})=1$ (הנגזרת) (הפולינום זר לנגזרת שלו) $\Longleftarrow$ x^n-1 ספרבילי ולכן ב-L כל שורשיו שונים והם מהווים תת-חבורה W מסדר n של L^*.

$\Longleftarrow$ (מהמשפט) W ציקלית.

יהיה ζ שורש יחידה פרימיטיבי מסדר n

$$x^n-1=\prod_{i=0}^{n-1}(x-\zeta^i)$$

$$L=K(\zeta)$$

משפט: L/K הרחבת גלואה אבלית ($\equiv$ עם $Gal(L/K)$ אבלית)

יתרה מזאת $Gal(L/K)$ איזומורפית לתת-חבורה של $(\mathbb{Z}/n\mathbb{Z})^*$

$$\left((\mathbb{Z}/n\mathbb{Z})^*=\{a \bmod n \mid (a,n)=1\}\right)$$

הגדרה: אם L/K הרחבת גלואה נקרא לה ציקלית/אבלית/פתירה

אם $Gal(L/K)$ הינה ציקלית/אבלית/פתירה.

12-6-2007

הוכחה: L/K הינה גלואה כתור שדה פיצול של פולינום ספרבילי

נגדיר העתקה

$$\chi : \overset{G}{\overset{\shortparallel}{Gal(L/K)}} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

מאופיין הנ״ל: $\sigma \in G$

$$\sigma(\zeta) = \zeta^{\chi(\sigma)}$$

הצדקה:

$$\sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1$$

ולכן $\sigma(\zeta) = \zeta^i$ עבור $0 \le i \le n-1$

$$\zeta^{i+n} = \zeta^i$$

$$\Downarrow$$

$$i = \chi(\sigma) \in \mathbb{Z}/n\mathbb{Z}$$

מוגדר היטב

עדיין צריך להראות $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$

נראה זאת על-ידי שנראה $\chi(\sigma\tau) = \chi(\sigma)\cdot\chi(\tau)$

נסתכל על:

$$(\sigma\circ\tau)(\zeta) = \zeta^{\chi(\sigma\circ\tau)}$$

$$= \sigma(\tau(\zeta))$$

$$= \sigma(\zeta^{\chi(\tau)}) = \sigma(\zeta)^{\chi(\tau)} = (\zeta^{\chi(\sigma)})^{\chi(\tau)} = \zeta^{\chi(\sigma)\chi(\tau)}$$

עכשיו נקבל: אם ניקח $\tau = \sigma^{-1}$

$$\chi(e) = \chi(\sigma)\chi(\sigma^{-1})$$

ומכאן $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$

בנוסף קיבלנו ש- χ הינו הומומורפיזם של חבורות מ:

$$Gal(L/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

χ נקרא הקרקטר הציקלוטומי.

$(\mathbb{Z}/12\mathbb{Z})^*$

(לוח הכפל של $\mathbb{Z}/12\mathbb{Z}$)

	1	5	7	11
1	1			
5		1		
7		11	1	
11				

$$(\mathbb{Z}/12\mathbb{Z})^* = \mathbb{Z}_2 \times \mathbb{Z}_2$$

נשים לב ש- χ חח"ע

$$\chi(\alpha) \equiv 1$$
$$\Downarrow$$
$$\Leftarrow \quad \sigma(\zeta) = \zeta$$
$$\Leftarrow \quad \alpha = e$$

∎

$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ פונקציית φ של אוילר

$\varphi(p) = p-1$ ראשוני

$\varphi(p^2) = p^2 - p = p(p-1)$

מסקנה: $|G| = [L:K]$ מחלק את $\varphi(n)$

הערה: במקרה המיוחד ש $K=\mathbb{Q}$, χ הינו על $(\mathbb{Z}/n\mathbb{Z})^*$

הוכחה כאשר $n=p$: כבר ראינו שהפולינום המינימלי של ζ הינו מסדר $p-1$ $\Leftarrow$ χ על.

תתי-שדות של L:

הם בהתאמה חח"ע עם תתי-חבורות של G.

G אבלית $\Leftarrow$ כל תת-חבורה שלה גם כן אבלית ונורמלית $\Leftarrow$ כל תת השדות של L הינם גלואה ואבליים.

תרגיל:

$\mathbb{Q}(\zeta_7)$

2

$\mathbb{Q}(\cos\frac{2\pi}{7})$

3

$\mathbb{Q}$

6

σ = ציקלית מסדר 6

להוכיח!

18-6-2007

מבנים אלגבריים ב - שעור מס' 18

(רון ליבנה מחליף את אורי דה שליט)

הרחבות קומר

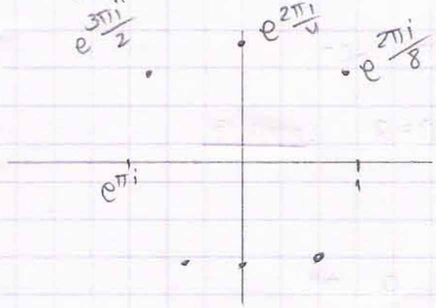
אנחנו מסתכלים על שדה K,

$n \geq 1$ שלם והוא זר למציין $\mathrm{Char}\,K$

נתון בשדה הבסיס: $0 \neq a \in K^*$ ($K^* = K - \{0\}$)

אנו מעוניינים להבין את חבורת גלואה של שדה הפיצול L של $x^n - a = 0$

כבר דובר במקרה $a=1$ שבו הי' כאמור הרחבה ציקלוטומית (= שורשי היחידה).



שורשי היחידה

מסדר 8 ב- $\mathbb{C}$

חבורת גלואה של שדה הפיצול L: $Gal(L/K)$

משוכנת לתוך החבורה הכפלית $(\mathbb{Z}/n\mathbb{Z})^*$ (הומומורפיזם חח"ע)

$\chi = \chi_n : Gal(L/K) \to (\mathbb{Z}/n\mathbb{Z})^*$

הערה: אם $K = \mathbb{Q}$ אז χ איזומורפיזם (גם על) (כי הפולינום הציקלוטומי מדרגה $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ והוא אי-פריק).

נעבור עתה למקרה של a כללי ($a \neq 1$ כמו כבר סימנו).

בשדה הפיצול $x^n - a = (x-\alpha_1)\cdots\cdots(x-\alpha_n)$

כאשר α_i השורשים של $x^n = a$, במילים אחרות, "השורשים ה-n-יים של a"

נשים לב כי לשורשים האלו יש תכונות מיוחדות.

למשל אם ניקח שני שורשים ונחלק אותם אחד בשני ונעלה בחזקת n: $\left(\frac{\alpha_i}{\alpha_j}\right)^n = \frac{a}{a} = 1$

ולכן $\frac{\alpha_i}{\alpha_j}$ פותר את $x^n = 1$, מקרה שכבר מוכר לנו.

מצד שני, α_i/α_j שייך לשדה הפיצול L ולכן L מכיל את השדה הציקלוטומי

$M = K(\zeta_n)$ כאשר ζ_n שורש יחידה מסדר n

L = שדה הפיצול שלנו

|

$M = K(\zeta_n)$ (הכנסנו באמצע שדה מוכר)

|

K

הערה: אם ζ_n הוא איזשהו שורש יחידה מסדר n אז:

$$a = 1\cdot a = (\zeta_n \alpha_i)^n$$

פתרון ל $x^n - a = 0$ ולכן נמצא בשדה הפיצול

כלומר השדה מספיק גדול והכיל את ζ_n הפתרונות הם בדיוק

$$\boxed{\alpha, \alpha\zeta_n, \alpha\zeta_n^2, \dots\dots, \alpha\zeta_n^{n-1}}$$

נובע בפרט $\frac{\alpha\zeta_n}{\alpha} = \zeta_n \in L$ (ולכן אפשר היה לקחת $L = \tilde{L}$ מלכתחילה)

כעת L גלואה מעל M (מדוע?)

כי: - גם נובע מהמשפט היסודי של תורת גלואה.

- גם רואים במפורש מהמקרה הזה.

דוגמאות: $n=2$ שורשי היחידה מסדר 2 הם $\pm 1 \in K$

$$\sqrt[2]{a} = \pm\sqrt{a}$$

אם a ריבוע בשדה K אז $L=K$

$Gal(L/K)$ טריוויאלית

אם a אינו ריבוע בשדה K $[L:K]=2$ $Gal(L/K) = \mathbb{Z}/2\mathbb{Z}$

עכשיו a הוא כללי: יהי σ איבר כלשהו בחבורת גלואה $Gal(L/M)$

אז מוכרח להתקיים $\sigma(\alpha) = $ (שורש אחר של $x^n-a=0$)

(α –) שורש של $x^n-a=0$

ולכן $\sigma(\alpha) = \zeta\alpha$

לאיזשהו ζ המקיים $\zeta^n=1$.

אז נקבע את α ואנו יודעים כי: $\sigma(\alpha)=\zeta\alpha$

יהי η איזשהו שורש יחידה מסדר n אז:

$$\sigma(\eta\alpha) = \underset{\hat{M}}{\sigma(\eta)}\sigma(\alpha) = \eta\zeta\alpha$$

אם יודע איך σ פועל על שורש אחד יודע איך פועל על כולם.

$Gal(L/M) \xrightarrow{\varphi}$ נגדיר שורשי היחידה מסדר n $\mu_n(K)$

$$\sigma \xrightarrow{\varphi} \eta = \varphi(\sigma)$$

הערה: מהחישוב הקודם $\varphi(\sigma)$ מוגדר היטב כלומר אינו תלוי בבחירת α.

כי α אחרת היא $\eta\alpha$ ואז

$$\frac{\sigma(\eta\alpha)}{\eta\alpha} = \zeta = \frac{\sigma(\alpha)}{\alpha} = \varphi(\sigma)$$

טענה: φ הומומורפיזם

הוכחה: $\sigma, \tau \in Gal(L/M)$ אזי

$$\varphi(\sigma\tau) = \frac{\varphi(\tau\alpha)}{\alpha} =$$

$$= \frac{\sigma(\varphi(\tau)\alpha)}{\alpha} = \frac{\varphi(\tau)\sigma(\alpha)}{\alpha} =$$

$$= \varphi(\tau)\varphi(\sigma)\frac{\alpha}{\alpha} = \varphi(\tau)\varphi(\sigma)$$

מ.ש.ל.

הערה: שום φ חח"ע

$\varphi(\sigma) = 1 = \frac{\sigma\alpha}{\alpha}$ כלומר $\sigma(\alpha) = \alpha$.

אזי ראינו $\eta\alpha = \sigma(\eta\alpha)$ ולכן

$\sigma : L \to L$ היא העתקת הזהות.

לכן $Gal(L/M)$ מזוהה דרך φ עם תת-חבורה של μ_n = חבורת

שורשי היחידה מסדר n-אין

זוהי חבורה ציקלית מסדר n.

לסיכום:

משפט: K שדה, $n \geq 1$ שלם $a \in K^*$ $1 = (n, char K)$

L שדה הפיצול של $x^n - a = 0$

M שדה הפיצול של $x^n - 1 = 0$

אזי $L \supset M \supset K$

כי ההרחבה גלואה $Gal(M/K) \underset{\chi}{\hookrightarrow} (\mathbb{Z}/n\mathbb{Z})$ אבלית

$Gal(L/M) \underset{\varphi}{\hookrightarrow} \mu_n$ חבורה ציקלית מסדר n

ולכן זו חבורה ציקלית מסדר המחלק את n

ולסיום $Gal(L/K)$

מכילה את $Gal(L/M)$

כתמורה חלקית נורמלית עם מנה $Gal(M/K)$

$$Gal(L/K) \rhd Gal(L/M)$$

אבלית

חבורת המנה אבלית

הגדרה: (תזכורת)

חבורה G (אולי סופית) תקרא פתירה אם קיימות $H_i < G$,

כך שמתקיים $H_0 = G \rhd H_1 \rhd H_2 \rhd \dots \rhd H_n = 1$

וכל המנות העוקבות

H_i / H_{i+1} הן אבליות

הגדרה: (עוד תזכורת)

חבורה G נקראת פשוטה אם אין לה חבורות חלקיות נורמליות פרט ל- $\{e\}$ ול- G.

הערה למשפט: הרחבות L/M נקראות הרחבות קומר: שדה הפיצול של $x^n - a$,

$1 = Char(M, n)$ ו- M מכיל את שורשי היחידה מסדר n.

ראינו בעבר דוגמאות לחבורות פשוטות:

* החבורה האלטרנטיבית A_n ⇐ פרמוטציות זוגיות על n אותיות) פשוטה ל- $n \geq 5$.

* (גם חבורה ציקלית מסדר ראשוני היא פשוטה).

* במשפט שלנו $Gal(L/K)$ היא פתירה.

טענה שלא נוכיח: (אולי היתה הוכחה במבחנים 1)

נניח כי $G \rhd H$ אזי G פתירה $\iff$ גם H וגם G/H פתירות

כיוון אחד קל: אם H, G/H פתירות נקבל

$$H_0 = H \rhd H_1 \rhd \dots \rhd H_n = 1$$

המנות H_i/H_{i+1} אבליות

$$K_0 = G/H \rhd K_1 \rhd \dots \rhd K_m$$

והמנות אבליות.

תהי $\tilde{K}_i$ המקור ב-G $\tilde{K}_i = \pi^{-1}(K_i)$ העתקת המנה $\pi: G \to G/H$

$$\tilde{K}_0 = G \rhd \tilde{K}_1 \rhd \dots \rhd \underset{H}{\tilde{K}_m} \rhd H_1 \rhd \dots H_n = 1$$

עם מנות עוקבות אבליות ולכן G פתירה.

הכיוון האחר קשה יותר (ולא נוכיח כרגע).

מסקנה מהטענה הזו:

S_n אינה פתירה ל- $n \ge 5$

(פרמוטציות על n סמלים)

הוכחה: לו S_n היתה פתירה אזי $S_n \rhd A_n$ היתה פתירה גם היא, אך היא פשוטה (ואינה אבלית!) סתירה.

הדוגמא מקודם $Gal(L/K)$

L שדה הפיצול של $x^n - a = 0$ נתנה חבורת גלואה פתירה (נדרשו רק שני שלבים)

$$Gal(L/K) \rhd Gal(L/M)$$

(אבלית, אבלית)

דוגמא: $x^3 - 2 = 0$ נותן $S_3 \rhd A_3 \rhd 1$

אפשר לבנות דוגמאות לחבורות גלואה שהן S_5 ומכאן אין פתירות.

נבנה כעת אחת כזו.

תחילה נרשום למה.

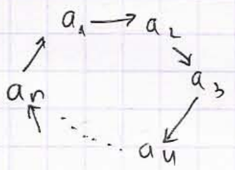
למה: יהי p ראשוני נניח כי

σ ציקלוס מאורך p

τ טרנספוזיציה ב- S_p אזי σ, τ יוצרים את S_p

תזכורת: חבורת הפרמוטציות S_n, n כלשהו,

כל איבר הוא מכפלה יחידה של ציקלוסים זרים $(a_1,\dots,a_n)(b_1,\dots b_s)\dots(d)$



הצמדה של ציקלוס בפרמוטציה σ מחליפה אותו בציקלוס מאותו הסוג:

$$\sigma(a_1\dots a_n)\sigma^{-1}=(\sigma(a_1)\dots\sigma(a_n))$$

ע"י שינוי שמות האותיות $\tau=(1\,2)$

והציקלוס הוא $\sigma=(1\,a_1\,a_2\dots a_{p-1})$

בדיקה $1\le k\le p-1$ σ^k גם הוא ציקלוס מסדר p

$(1\ a_k\dots)$

נבחר k הנכון $\sigma^k=(1\,2\dots)$

נחליף את σ ב- σ^k הרי הם יוצרים אותה חבורה כי שניהם מאותו סדר p כי p ראשוני.

כעת נמספר את הסמלים שנשארו (חוץ מ-1 2) מאחר ש: $\sigma=(1\,2\,3\dots p)$

$\tau=(1\,2)$

כעת $\sigma\tau\sigma^{-1}=(\sigma1\,\sigma2)=(2\,3)$

וכן הלאה: $\sigma^i\tau(\sigma^i)^{-1}=(i+1,i+2)$

כעת מהצמדות נוספות נקבל את כל הטרנספוזיציות

$(34)(23)(12)(23)(34)=(14)$ וכן הלאה.

החבורה ש σ ו- τ יוצרים מכילה לכן את כל הטרנספוזיציות ולכן היא כל S_p

(כל איבר ב- S_n הוא מכפלת טרנספוזיציות ל-n כלשהו)

☒

זה מוכיח את הלמה ועתה נכתוב למה נוספת לצורך בניית הדוגמא

18-6-2007

למה: נניח כי $f\in\mathbb{Q}[x]$ פולינום אי-פריק ממעלה p כך שבין השורשים שלו ב-$\mathbb{C}$ בדיוק 2 מרוכבים ושאר השורשים ממשיים אזי לשדה הפיצול L של f מעל $\mathbb{Q}$ יש חבורת גלואה $\cong S_p$

(מספר אינה פתירה לכל $5 \le p$)

הוכחה: יהיו $\alpha_1,\dots,\alpha_p$ השורשים ב-$\mathbb{C}$ אזי אפשר לקחת

$$L=\mathbb{Q}(\alpha_1,\dots,\alpha_p)$$

(כרגיל מקרה זה נכון) כל איבר ב-$Gal(L|\mathbb{Q})$ נותן פרמוטציה על השורשים כך שמתקבל הומומורפיזם חח"ע

$Gal(L|\mathbb{Q}) \longrightarrow ($ הפרמוטציות על השורשים $\cong S_p)$

מספר נוכל לראות את $Gal(L|\mathbb{Q})$ כתת-חבורה של S_p בדרך השיכון

הרי מצד אחד f אי-פריק לכן $[\mathbb{Q}(\alpha_1):\mathbb{Q}]=\deg f=p$

ולכן בוודאי $p \mid [L:\mathbb{Q}]=|Gal(L|\mathbb{Q})|$ ($L \supseteq \mathbb{Q}(\alpha_1)$)

מחבורה מסדר המתחלק ב-p יש איבר σ מסדר המתחלק ב-p (משפט קושי)

אם נחשוב על σ כתור פרמוטציה ונכתוב אותה כמכפלת ציקלוסים זרים היא חייבת להיות ציקלוס מאורך p (אחרת הסדר אינו p)

מצד שני ההצמדה המרוכבת שומרת על f ולכן על L. מההנחה (ההצמדה המרוכבת על L (שתסומן τ) מחליפה שני שרשים וקובעת את $q-2$ האחרים):

לכן τ טרנספוזיציה.

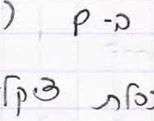
מהלמה הם יוצרים את S_p ולכן $Gal(L|\mathbb{Q})=S_p$.

דוגמא מספרית: נתבונן ב:

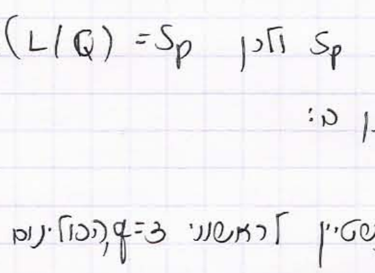
$$f(x)=x^5-6x+3$$

מקריטריון איינשטיין לראשוני $q=3$ הפולינום הנו אי-פריק

הנגזרת היא: $5x^4-6$



לכן הפולינום נראה כך



$f(0)>0$

$f(1)<0$

לכן יש ל-f בדיוק 3 שורשים ממשיים

תנאי הלמה מתקיימים ולכן:

$$Gal(f)=Gal(L|\mathbb{Q})=S_5$$

הערה: השורשים של הפולינום הזה שונים כי הוא אי-פריק.

(אפשר גם לראות שאין לו 0 משותף עם הנגזרת)

טענה: יש קשר הדוק בין אפשרות לפתור פולינום ע"י הוספת שורשים לבין היות חבורת הגלואה שלו פתירה. (מכאן בא השם חבורה פתירה)

(נראה זאת מחר)

נראה את המשפט הבא:

הרחבת שדות L/K נקראת רדיקלית אם L מוכלת ב- K_n

$$K_n \supset K_{n-1} \supset \dots \supset K_1 = K$$
$$K_n \supseteq L$$

רדיקלית

K_{i+1} מתקבלת מ- K_i ע"י הוספת שורש מספר n_i של איבר $a_i \in K_i$

המשפט יהיה: הרחבה רדיקלית מוכלת בהרחבת גלואה פתירה.

(כי הרחבת גלואה פתירה היא רדיקלית)

מסקנה מרכזית: שדה הפיצול של פולינום הוא רדיקלי (שאפשר למצוא את כל הפתרונות ע"י הוספת שורשים) $\Longleftrightarrow$ חבורת הגלואה של שדה הפיצול היא פתירה.

מבנים אלגבריים 2 - שעור מס' 19

בשבוע הבא יש שעור ביום ראשון.

הרחבות רדיקליות והרחבות פתירות

למשוואה ריבועית יש נוסחה: $ax^2+bx+c=0$

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

יש נוסחאות דומות למשוואות מדרגה 3 ומדרגה 4.
(מופיעים שורשים מסדר 3, 4)

מה לגבי דרגה 5?

בלתי אפשרי - זאת זה הוכיח גלואה.

נרצה להראות זאת ולשם כך ניתן מס' הגדרות.

נניח לשם פשטות ש-K שדה ממציין 0.

הגדרה: הרחבה L של K תקרא רדיקלית אם $L=K(\alpha_1,\ldots,\alpha_2)$
ומתקיים $K(\alpha_1,\ldots,\alpha_{i-1})\ni\alpha_i^{n_i}$
לכל $1\le i\le n-1$
$n_i - 1$: שלם ≥ 1 מתאים.

דוגמא: $\mathbb{Q}(\sqrt{-1},\sqrt[4]{1+\sqrt{-1}})$ היא הרחבה רדיקלית של $\mathbb{Q}$.

הגדרה: פולינום $f(x)\in K[x]$ פתיר ע"י רדיקלים אם קיימת הרחבה רדיקלית L של K
כך ש-f מתפרק לחלוטין (שדה הפיצול של f מוכל ב-L)

משפט (גלואה): אם ניתן לפתור את המשוואה $f(x)=0$ ע"י רדיקלים אזי לשדה הפיצול של f
יש חבורת גלואה פתירה.

הוכחה: נתחיל בלמה:

למה: אם f פתיר ע"י רדיקלים אזי שדה הפיצול שלו J מוכל בהרחבה L של K
שהיא רדיקלית וגלואה מעל K.

הוכחת הלמה: תהי L_0 הרחבה רדיקלית

$L_0 = K(\alpha_1,\ldots,\alpha_k)$

המכילה את J $\qquad K(\alpha_1,\ldots,\alpha_{i-1}) \ni \alpha_i^{n_i}$

(המשפט נכון) התכולה, לכן יש הרבה מחלקות.

יהי m_i הפולינום המינימלי של α_i מעל K

$m = \prod m_i$

ויהי L שדה הפיצול של הפולינום m (מעל K).

ברור כי L הוא גלואה מעל K, נראה כי הוא גם רדיקלי מעל K

נסיים את הוכחת הלמה:

אם $\sigma \in Gal(L/K)$ כלשהו אזי $\sigma\alpha_i$ גם הוא שורש ל- m_i

ולכן נקבל מאינדוקציה כי שדות הפיצול של $m_1,\ldots,m_i$ הם גלואה ורדיקלים מעל K.

שדה הפיצול של $m_1,\ldots,m_i$ נוצר ע"י $\alpha_1,\ldots,\alpha_i$ וכל הצמודים $\sigma\alpha_j$ $1\le j\le i$ שלהם. נטען כי זו הרחבה רדיקלית של K

בפרט ל $i=k$ וסיימנו.

נמשיך מהוכחת המשפט:

הוכחת המשפט:

תזכורת: אם $G \triangleright H$ אזי G פתירה $\iff$ H ו- G/H פתירות.

יהי f פתיר ע"י רדיקלים.

-קיימת הרחבת גלואה פתירה L של K המכילה את שדה הפיצול J של f.

L
|
J $\qquad Gal(L/K) \triangleright Gal(L/J)$
|
K

יספיק להראות $Gal(L/K)$ פתירה לכל שורשית את f ונורמלית L

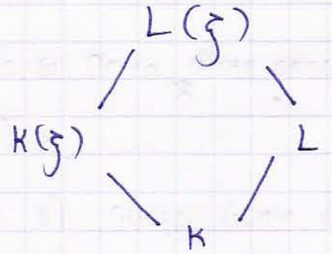
<u>ט3</u>: הרחבת גלואה רדיקלית היא <u>פתירה</u>.

$$L=K(\alpha_1,\dots,\alpha_r)$$

$$\alpha_i^{n_i}\in K(\alpha_1,\dots,\alpha_{i-1})$$

$$n=\prod n_i$$

נשפר את K ע"י הוספת שורש יחידה ζ מסדר n



(כי זה משדה מספיק גדול)

בוודאי $L(\zeta)$ <u>גלואה</u> מעל K כהרכבה של הרחבות גלואה L + $K(\zeta)$ שלו.

לכן יספיק להראות $Gal(L(\zeta)/K)$ פתירה.

אבל מכיון ש- $K(\zeta)/K$ אבלית (ζ שורש יחידה) היא בוודאי פתירה ולכן יספיק להראות כי $Gal(L(\zeta)/K(\zeta))$ פתירה.

<u>מסקנה</u>: מותר להניח ששורשי היחידה מסדר n_i בשדה K (מחליפים אותו ב- $K(\zeta)$ אם צריך)

$$L=K_k=K(\alpha_1,\dots,\alpha_k)$$

$$K_{k-1}=K(\alpha_1,\dots,\alpha_{k-1})$$

$$\vdots$$

$$K_i=K(\alpha_1,\dots,\alpha_i)$$

$$\vdots$$

$$K=K_0$$

ההרחבה K_{i+1}/K_i מתקבלת ע"י הוספת שורש מ- n_{i+1} כאשר שורשי היחידה ה- n_{i+1} ב- K_i

לכן (מהטענה הקודמת) ההרחבה הנ"ל היא גלואה וחבורת הגלואה שלה אבלית (שוב, ראינו בטענה הקודמת)

$$Gal(L/K) \supset Gal(L/K_1) \ldots \supset Gal(L/K_{R-1})$$

כל תת-חבורה נורמלית בקודמת, המנות העוקבות אבליות $\Leftarrow Gal(L/K)$ פתירה.

מסקנה: את הפולינום מהמעלה החמישית: $x^5-6x+3=0$

מעל $\mathbb{Q}$ לא ניתן לפתור ע"י הוספת שורשים כי S_5 = חבורת הגלואה שלו
אינה פתירה.

ננסח את המשפט ההפוך (ללא הוכחה):

משפט: נניח כי L/K הרחבת גלואה עם חבורת גלואה פתירה אזי ניתן לשכן את L
בהרחבה רדיקלית (גלואה) של K.

(ההוכחה נדרשת אינדוקציה על המנה הפתיר של החבורה + הלמה של
קומר: אם שורשי יחידה מסדר n בשדה, אז הרחבה ציקלית מסדר n היא רדיקלית).

24-6-2007

מבנים אלגבריים 2 - שיעור מס' 20 (שיעור השלמה 6 יום ראשון)

(1)

* הוכחנו עם המרצה (המחליף) שפולינום מסויים מעל הרציונליים פתיר ברדיקלים.

נחזור על זה היום:

הבעיה שלנו היא:

ישנו K שהוא שדה וישנו פולינום $f \in K[x]$ ממעלה n מתוקן

(K – שדה הבסיס שלנו)

האם יש "נוסחה" לשורשים של f המשתמשת במקדמי f, בפעולות החשבון הרגילות $+, -, \cdot, /$ (שלא מוציאות אותנו מתחומי השדה) ובהוצאת שורש $\sqrt{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }$...

* נראה כיצד נראית ה"נוסחה" לשורשים של פולינום ממעלה 3.

<u>תזכורת מהשיעור הקודם:</u>

(הגדרה) L הרחבה רדיקלית של K אם $K \subset L \subset K(\alpha_1, \dots, \alpha_n)$, $K(\alpha_i^{(j)}) = M$

הוכחנו למה שאומרת:

כל הרחבה רדיקלית של K מוכלת בהרחבת גלואה רדיקלית של K.

אם f פולינום אי-פריק ו-β שורש שלו ! $L = K(\beta)$

ב-M f מתפצל ולכן לכל שורש אחר β' של f $K(\beta') \subset M$.

(תשובה לשאלה שנשאלה בהרצאה הקודמת בנוגע לשיעור.)

(אם יש הרחבה רדיקלית אז היא מוכלת בהרחבה עם יותר איברים שהיא כבר גלואה מעל K)

לא נכון לומר שלפולינום ממעלה 5 ומעלה אין פתרון כי אנחנו כן יודעים למצוא שורשים, אבל אנחנו לא יודעים להביע את השורשים כנוסחה מפורשת.

∞

פולינום ממעלה 3:

נניח שיש שדה K והשדה הוא ממציין 0 $\text{Char} K = 0$ (אפילו מספיק להניח $\text{Char} K \neq 2, 3$)

נתון פולינום: $x^3 + a_1 x^2 + a_2 x + a_3 = 0$

אם $x = u - \frac{1}{3}a_1$ אז האיבר הריבועי נעלם.

במקרה שלנו:

$$(u - \tfrac{1}{3}a_1)^3 + a_1(u - \tfrac{1}{3}a_1)^2 + \dots =$$

$$(A-B)^3 = A^3 - 3A^2B + 3AB^2 - B^3$$

$$u^3 - 3 \cdot \tfrac{1}{3} a_1 u^2 + a_1 u^2 + \dots = \dots \boxed{u^3 + au + b = 0}$$

והעלמנו את האיבר הריבועי
לכן מספיק לפתור פולינום מהצורה הבאה: $u^3+au+b=(u-\alpha_1)(u-\alpha_2)(u-\alpha_3)$

(המקדם של u^2): $0=\alpha_1+\alpha_2+\alpha_3$

המקדם של u: $a=\alpha_2\alpha_3+\alpha_1\alpha_3+\alpha_1\alpha_2$

(המקדם החופשי) $b=-\alpha_1\alpha_2\alpha_3$

אלו הם פולינומים סימטריים ב- $\alpha_1,\alpha_2,\alpha_3$ כלומר אם נעשה איזושהי תמורה של $\alpha_1,\alpha_2,\alpha_3$ הפולינומים הנ"ל יחזרו לעצמם.

נתבונן ב- $\underline{\alpha_1^2+\alpha_2^2+\alpha_3^2}=(\alpha_1+\alpha_2+\alpha_3)^2-2(\alpha_2\alpha_3+\alpha_1\alpha_3+\alpha_1\alpha_2)=\underline{-2a}$

$$\underline{\alpha_1^3+\alpha_2^3+\alpha_3^3}=(\alpha_1+\alpha_2+\alpha_3)(\alpha_1^2+\alpha_2^2+\alpha_3^2)-\alpha_1\alpha_2^2-\alpha_1\alpha_3^2-\alpha_2\alpha_1^2-\alpha_2\alpha_3^2-$$
$$-\alpha_3\alpha_1^2-\alpha_3\alpha_2^2=$$
$$=-\alpha_1\alpha_2(\alpha_1+\alpha_2)-\alpha_1\alpha_3(\alpha_1+\alpha_3)-\alpha_2\alpha_3(\alpha_2+\alpha_3)=3\alpha_1\alpha_2\alpha_3=\underline{-3b}$$

נזכר בתורת גלואה: אם $L=K(\alpha_1,\alpha_2,\alpha_3)$ אז ההרחבת גלואה כשדה פיצול - הרחבה נורמלית וספרבילית וראינו שחבורת גלואה פועלת כחבורה נאמנה כחבורת תמורות של שורשים, אנו יכולים לשכן את G ב- S_3 כאשר S_3 היא כל התמורות על $\alpha_1,\alpha_2,\alpha_3$. $A_3\subset S_3$ כאשר A_3 הינה כל התמורות הזוגיות. G יכולה להיות חבורה מסדר 2, 3 או כל S_3 אך אמור להיות שדה מדרגה 1 או 2 שהוא שדה השבת של החיתוך של G עם A_3 כאשר $A_3\triangleleft S_3$ יחידה. אם נסמן $F=\mathcal{F}(G\cap A_3)$ אז מתורת גלואה $[F:K]=1$ או 2 כי אם הסדר של G היה 3 אז $G=A_3$ אז שדה השבת היה K. אם הסדר של G יהיה 6 אז 1 או $(G\cap A_3)=3$

$L=K(\alpha_1,\alpha_2,\alpha_3)$
| $(G\cap A_3)=1$ או 3
$F=K(?)$
| 2 או 1
K
G

<u>השאלה היא מה יוצר את F?</u>

אנו צריכים למצוא ביטוי שיסומן ב- $\alpha_1,\alpha_2,\alpha_3$ שחבורת התמורות פועלת עליו דרך הסימן של התמורה, כלומר אם $\sigma\in G$ אז $\sigma(\delta)=\mathrm{sgn}\pi(\sigma)\delta$

סימן התמורה שמתאימה ל-σ כלומר תמורה של $(\alpha_1,\alpha_2,\alpha_3)$ המתאימה ל-σ

δ צריך שאותם איברים ב-G שהם ב-A_3 לא מזיזים אותו ואיברים ב-G שהם תמורות לא זוגיות צריכות להעביר את δ ל- $-\delta$.

24-6-2007 ②

מכפלת ההפרשים "מסדר עולה": $\delta=(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)$

אם נחליף את α_1 ב- α_2, δ ישנה סימן ונקבל $-\delta$

ומכאן כי תמורה אי-זוגית, לכן, קל לראות שמשפטי ה-δ הנה זה מתקיים.

הדיסקרימיננטה של הפולינום f: $\delta^2\in K$

המטרה שלנו היא למצוא את δ מעזרת הביטויים הנ"ל,

$$-\delta^2=f'(\alpha_1)\cdot f'(\alpha_2)\cdot f'(\alpha_3)$$

זה נכון כי נגזור את u^3+au+b ונקבל כאת כי:

$$=(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)$$

$$\Longrightarrow \delta^2=-(3\alpha_1^2+a)(3\alpha_2^2+a)(3\alpha_3^2+a)=$$

$$=-27(\alpha_1\alpha_2\alpha_3)^2-a^3-3a^2(\alpha_1^2+\alpha_2^2+\alpha_3^2)-9a(\alpha_1^2\alpha_2^2+\alpha_1^2\alpha_3^2+\alpha_2^2\alpha_3^2)=$$

$$=-27b^2-a^3-6a^3-9a^3=-27b^2-4a^3$$

$$\delta^2=-27b^2-4a^3 \Longrightarrow \delta=\sqrt{-27b^2-4a^3}$$

וזהו ביטוי של δ מעזרת רדיקלים.

כעת נרצה למצוא את ה-ω-ים מעזרת רדיקלים.

ההרחבה F/K אי-אפשר לסגל כלי סיבוח $\sqrt[3]{1}=\omega=e^{\frac{2\pi i}{3}}$

נרצה להסתכל מהרחבה $L(\omega)=K(\omega,\alpha_1,\alpha_2,\alpha_3)$ ולמצוא את אחד (ה-α

עם רדיקלים תוך שימוש ב- ω ו- δ

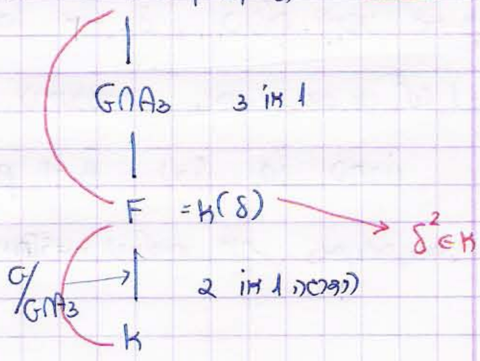
$F(\omega)=K(\omega,\delta)$ שני רדיקלים

<u>תזכורת</u> - $L=K(\alpha_1,\alpha_2,\alpha_3)$ האפשרויות הן: $G=S_3$

* $|G|=3 \Longrightarrow G=A_3$ (A_3 היא התמורה היחידה מסדר 3 ב- S_3)

$|G|=2$ - יש שלוש כאלה.

$G=\{e\}$



אם 3 מחלק את $|G|$ אז $G=S_3$ או $G=A_3$ לכן נתבונן בחיתוך

$G\cap A_3$ ובשדה השבת שלו $F=\mathcal{F}(G\cap A_3)$ - שדה השבת של כל התמורות

הזוגיות.

<u>המטרה - לבטא את α_i ע"י רדיקלים.</u>

$G|_F=id$ אם ורק אם $\sigma(\delta)=\delta$ וזה אם ורק אם $G\in G\cap A_3$

אם ורק אם $sgn(\pi(\sigma))=-1$

$$\sigma(\delta)=sgn(\pi(\sigma))\delta$$

נתבונן באיבר $\beta=\alpha_1+\omega\alpha_2+\omega^2\alpha_3 \in L(\omega)$

אם הייתה לנו תמורה (ציקלוס) $(\alpha_1\ \alpha_2\ \alpha_3)$ ומשאירה את ω במקומו $\sigma(\omega)=\omega$

$\sigma(\alpha_i)=\alpha_{(i+1)\bmod 3}$

היא הייתה בעצם מכפילה את β ב-ω.

$$\Longrightarrow \sigma(\beta)=\alpha_2+\omega\alpha_3+\omega^2\alpha_1=\omega^2\cdot\beta \Longrightarrow \sigma(\beta^3)=\beta^3$$

$$\beta^3=(\alpha_1+\omega\alpha_2+\omega^2\alpha_3)(\alpha_1+\omega\alpha_2+\omega^2\alpha_3)(\alpha_1+\omega\alpha_2+\omega^2\alpha_3)=$$

$$=\alpha_1^3+\alpha_2^3+\alpha_3^3+6\alpha_1\alpha_2\alpha_3+3\omega(\alpha_1^2\alpha_2+\alpha_2^2\alpha_3+\alpha_3^2\alpha_1)+\omega^2 3(\alpha_2^2\alpha_1+\alpha_3^2\alpha_2+\alpha_1^2\alpha_3)=$$

$$=-9b+3\omega\left(\frac{3b+\delta}{2}\right)+3\omega^2\left(\frac{3b-\delta}{2}\right)=\beta^3\in F(\omega)$$

$$\beta\in L(\omega)=K(\omega,\alpha_1,\alpha_2,\alpha_3)$$

$$\beta^3\in F(\omega)=K(\omega,\delta)$$

$$\bar{\beta}=\alpha_1+\omega^2\alpha_2+\omega\alpha_3$$

$$\bar{\beta}^3=-9b+3\omega^2\left(\frac{3b+\delta}{2}\right)+3\omega\left(\frac{3b-\delta}{2}\right)$$

בעזרת רדיקלים בשלב הראשון אנו יכולים לקבל את δ, בשלב השני גם את

האיבר β ואת $\bar{\beta}$ וכל איבר אחר המבוטא באמצעות $\alpha_1,\alpha_2,\alpha_3,\omega,\omega^2,1$.

כלומר מתוך ידיעת כל הצירופים מהסוג של β ו-$\bar{\beta}$ וכו' ע"י פתרון

של 3 משוואות לינאריות בשלושה נעלמים, מחלצים את $\alpha_1,\alpha_2,\alpha_3$.

24-6-2007

לסכם:

שלב I: חישוב δ $\delta=\sqrt{-27b^2-4a^3}$ ויוצרים את $F=K(\delta)$ ע"י רדיקלים.

שלב II: מספחים את $\omega=\sqrt[3]{1}$ ויוצרים את $L(\omega)$ כהרחבה רדיקלית של $F(\omega)$ ע"י $F(\omega)(\beta)=L(\omega)$

שלב III: (לא סימני) מבטאים את $\alpha_1,\alpha_2,\alpha_3$ בעזרת הנתונים.

זוהי לא הדרך הקצרה ביותר (בסנכ יש דרך יותר אלגנטית) אך זו הדרך הכי "שקופה".

באותה דרך, אם $deg(F)=4$ אז $G\subseteq S_4$ ו- $\overset{1}{1}\triangleleft \overset{4}{V}\triangleleft \overset{12}{A_4}\triangleleft \overset{24}{S_4}$

כאשר $V=\{1,(12)(34),(14)(23),(13)(24)\}$

ו: $\delta=(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)(\alpha_2-\alpha_4)(\alpha_3-\alpha_4)$

איפה כה יצור הרחבה מסדר 2.

מבנה לבחינה:

חלק ראשון: 1/2 הוכחת משפט מן החומר (30)

חלק שני: 2/3 תרגילים (הוכחות/חישובים) מתוך תרגילי חזרה שנתנו. (40)

חלק שלישי: נכון/לא נכון ללא הנמקה (30)

25-6-2007

מבנים אלגבריים -2- שעור מס' 21

(1)

* פתרונות / אי-פתירות של משוואה פולינומיאלית כללית.

* הרחבות טרנסצנדנטיות ודרגת טרנסצנדנטיות.

K שדה , $t_1, \dots, t_n$ סמלים, "משתנים".

__מונום__ הוא איבר מהצורה $M = c\,t_1^{e_1} t_2^{e_2} \cdots t_n^{e_n}$ $\quad 0 \le e_i \quad c \in K$

e_i = דרגת M במשתנה t_i והדרגה הכוללת $\sum_{i=1}^{n} e_i = \deg(M)$

__דוגמאות למונומים בשלושה משתנים:__

$t_1^2 t_3$, t_3^2 , $t_1^3 t_2 t_3^2$

דרגה 3 , דרגה 2 , דרגה 6.

__פולינום__ הינו סכום פורמלי של מונומים (במספר סופי)

$$\sum \underbrace{a_{e_1 e_2 \dots e_n}}_{\text{מקדמים מתוך } K} t_1^{e_1} t_2^{e_2} \dots t_n^{e_n}$$

$\deg(p)$ = הדרגה המקסימלית של מונום המופיע ב- p.

למשל דרגת הפולינום $t_1^2 t_2 + t_1 t_2^2 + 3t_1 t_2 + t_1 + t_2 + 1$

היא 3 , הדרגה ב- t_1 שווה ל- 2 כי

(*) $(t_2)\cdot t_1^2 + (t_2^2 + 3t_2 + 1)t_1 + (t_2 + 1)$

עם פולינומים אלו, כיצורים אלגבריים אפשר לעשות כל מיני פעולות:

* מכפלת מונומים הינה מונום ו- $\deg(M_1 \cdot M_2) = \deg M_1 + \deg M_2$

* סכום ומכפלת פולינומים הם פולינומים, אוסף הפולינומים ב- n משתנים מהווה חוג קומוטטיבי שיסומן $K[t_1, \dots, t_n]$.

__למה:__ זהו תחום שלמות (חוג קומוטטיבי ללא מחלקי אפס).

__הערה:__ ניתן לחשוב על $K[t_1, \dots, t_n]$ כעל חוג הפולינומים במשתנה אחד מעל שאר המשתנים $\cong \underbrace{K[t_1, \dots, t_{n-1}]}[t_n]$

חוג הפולינומים ב- n-1 המשתנים הראשונים
(מקדמים בהצבות t_n, למשל כמו בדוגמא (*)).

ב- $R[t]$, אם R הינו תחום שלמות, גם $R[t]$ הינו תחום שלמות.

$(a_0+a_1t+\dots+a_nt^n)(b_0+\dots+b_mt^m)=\dots\dots a_nb_mt$

$(a_nb_m\neq 0)$

נ"שם הערה כי על המקרה שלנו והאינדוקציה הלמה נכונה.

(תכונה של תחום שלמות אין קשר למציין של השדה).

* ב- $\mathbb{F}_p$ הפולינום $X^p-X=0$ אך פולינום זה איננו פולינום האפס כי המונומים אינם מבטלים זה את זה.

* $K[t_1,\dots,t_n]$ הוא תחום שלמות קומוטטיבי (אם $2\le n$ זהו איננו חוג ראשי אבל כן חוג עם פריקות חד-ערכית - ללא הוכחה - מעבר לרמת הקורס)

נסמן ב- $K(t_1,\dots,t_n)$ = שדה השברים (השברים) של $K[t_1,\dots,t_n]$

ונקרא לו שדה הפונקציות הרציונליות ב-n משתנים.

$f=\frac{P}{Q}$ כאשר P,Q פולינומים. $\frac{P_1}{Q_1}=\frac{P_2}{Q_2} \Longleftrightarrow P_1Q_2=P_2Q_1$

יש משמעות להצבת פונקציה רציונלית הגדרה מצומצמת אך אנו לא ניגע בנושא זה.

<u>הגדרה:</u> הרחבה L/K נקראת עוצרת סופית אם $L=K(\alpha_1,\dots,\alpha_n)$ עבור $\alpha_i\in L$ כלשהם. (אנו לא מניחים שהם אלגבריים), המשמעות היא ש-L הוא השדה הקטן ביותר שמכיל גם את K וגם את $\alpha_1,\dots,\alpha_n$

נגדיר העתקה $\varphi:K[t_1,\dots,t_n]\longrightarrow L$ ע"י שנציב $t_i=\alpha_i$ ונעריך את הפולינום $\varphi(p)=P(\alpha_1,\dots,\alpha_n)$ (כמובן שנקבל איבר ב-L כי אנו משתמשים בפעולות השדה).

<u>הגדרה:</u> (האיברים) $\alpha_1,\dots,\alpha_n$ הם בלתי תלויים אלגברית מעל K אם $\ker\varphi=0$ (כלומר φ חח"ע). זה אומר שאין שום פולינום $\neq 0$ עם איברים מ-K שמאפס את $\alpha_1,\dots,\alpha_n$.

* $\{\alpha_1\}$ בלתי תלוי אלגברית מעל K זה אותו הדבר כמו להגיד ש-α_1 טרנסצנדנטי מעל K.

25-6-2007

הערה: $\alpha_1,\dots,\alpha_n$ בלתי תלויים אלגברית מעל K $\Longleftarrow$ כל אחד מהם טרנסצנדנטי מעל K.

אבל זה הרבה יותר חזק: גם e וגם π ידועים כמספרים טרנסצנדנטים מעל $\mathbb{Q}$ (כלומר הם לא אלגבריים) אבל השאלה שהם בלתי תלויים אלגברית היא עוד יותר עמוקה (ואת זה יודעים מתורת המספרים הטרנס')

* אם $\alpha_1,\dots,\alpha_n$ בלתי תלויים אלגברית, φ הינו שיכון של $\varphi: K[t_1,\dots,t_n] \hookrightarrow L$ ולכן הוא ניתן להרחבה להומומורפיזם של שדה השברים לתוך L.

$\varphi: K(t_1,\dots,t_n) \hookrightarrow L$ הומומורפיזם כזה הוא על כי $Im(\varphi)$ הינו תת-שדה של L המכיל את K ולכן כל α_i כי $\alpha_i=\varphi(t_i)$ (מונום מדרגה 1), ואולם L נוצר ע"י $\alpha_1,\dots,\alpha_n$ ולכן φ גם על (כי השדה הקטן ביותר שמכיל גם את K וגם את $\alpha_1,\dots,\alpha_n$ הוא כבר כל L) ולכן φ הוא בעצם איזומורפיזם.

* יהיה L שדה הרחבה נוצר סופית של K $L=K(\alpha_1,\dots,\alpha_n)$

יהיה d המספר המקסימלי של איברים מתוך $\{\alpha_1,\dots,\alpha_n\}$ שהינם בלתי תלויים אלגברית מעל K. בה"כ ע"י שינוי סדר ה-α-ות נניח ש-$\alpha_1,\dots,\alpha_d$ בלתי תלויים אלגברית, נקבל

$$K\subseteq M=L(k_1,\dots,k_d)\subseteq L=M(\alpha_{d+1},\dots,\alpha_n)$$

כל α_i $i\geq d+1$ הוא אלגברי מעל M כי $\{\alpha_1,\dots,\alpha_d,\alpha_i\}$ כבר תלויים אלגברית מעל K ולכן יש פולינום ב- d+1 משתנים המאפס אותם.

הפולינום הנ"ל חייב להכיל את המשתנה האחרון (כי $\alpha_1,\dots,\alpha_d$ בלתי תלויים אלגברית) ולכן הוא פולינום במשתנה האחרון עבור α_i מעל M.

L/M נוצרת סופית ע"י n-d איברים אלגבריים ולכן היא הרחבה סופית. $[L:M]<\infty$. $M\cong K(t_1,\dots,t_d)$ זה מראה שכל הרחבה נוצרת סופית ניתן "לשבור" מאמצע. קודם כהרחבה טרנס' טהורה (הוא שדה הפונקציות הרציונליות ב- d משתנים) ומעליה אנו בונים הרחבה אלגברית סופית.

הערה 1: אין שום דרך קנונית לבחור את $\alpha_1,\dots,\alpha_d$.

הערה 2: מבחירות שונות של $\alpha_1,\dots,\alpha_d$ ההרחבות של L/M יכולות להיות דרגות שונות.

דוגמא: $L=K(x)$ אם ניקח $\alpha_1=x$ אז $L=K(\alpha_1)$ (הדרגה מעליו היא 1)

אך אם ניקח $\alpha_1=x^2+1$ אז כתוך L נמצא שדה M שהוא $K(x^2+1)$

זה כל פונקציה רציונלית ניתנת לביטוי ב- x^2+1

$$K\subset M=K(x^2+1)\subset L$$

זה נוכל לקבל את כל הפונקציות הרציונליות מכיוון $x\notin K(x^2+1)$

והפולינום המינימלי של x מעל M הוא $T^2-(x^2+1)+1=0$

(x מקיים משוואה זו) משוואה זו היא אי-פריקה מעל M.

במקרה כזה L/M דרגתו 2. $[L:M]=2$ (כי $K(x^2+1)\subsetneq L$)

לכן אין כ"כ משמעות לדרגה של L/M. ואין כל כך משמעות לאיברים שבחרנו, הדבר היחיד שיש לו משמעות הוא d.

הגדרה:

ה- d שהתקבל נקרא דרגת הטרנסצנדנטיות של L מעל K.

כל $\alpha_1,\dots,\alpha_d$ המקיימים: (א) $\alpha_1,\dots,\alpha_d$ בלתי תלויים אלגברית מעל K

(ב) L אלגברי מעל $K(\alpha_1,\dots,\alpha_d)$

נקראים בסיס טרנסצנדנטי של L מעל K L/K.

כאמור הבסיס הטרנסצנדנטי אינו יחיד וכמו דרגת האלגבריות מעליו איננה מוגדרת כ"כ טוב והיא תלויה בבסיס אך נראה שההגדרה כן טובה:

משפט: דרגת הטרנסצנדנטיות מוגדרת היטב.

הוכחה: צריך להוכיח שאם $L=K(\alpha_1,\dots,\alpha_d)$ כאשר $\alpha_1,\dots,\alpha_d$ תת-קבוצה בלתי תלויה אלגברית מקסימלית וגם $L=K(\beta_1,\dots,\beta_m)$ כאשר $\beta_1,\dots,\beta_e$ תת הקבוצה בלתי תלויה אלגברית מקסימלית $\Longrightarrow e=d$.

דוגמא: $L=K(x)[y]/(x^3+y^3-1)$, (x^3+y^3-1) הינו אי-פריק ראשוני ב $K(x)[y]$

L שדה $\alpha=x\bmod(x^3+y^3-1)$, $\beta=y\bmod(x^3+y^3-1)$ אז: $L=K(\alpha,\beta)$ $\alpha^3+\beta^3=1$

25-6-2007 (3)

ע"י "למת החלפה" די להוכיח ש $d \ge e$ ו $d \le e$

(ולכן יתקיים שוויון).

נתחיל עם β_1:

$\beta_1 \in L$ ולכן הוא אלגברי מעל $K(\alpha_1,\dots,\alpha_d)$, זה אומר שיש

פולינום $p \in K[t_1,\dots,t_d,X]$ כך ש- $p(\alpha_1,\dots,\alpha_d,\beta_1)=0$

β_1 אלגברי מעל שדה הפונקציות הרציונליות ולכן פותר פולינום ב-X

שמקדמיו מתוך $K(\alpha_1,\dots,\alpha_d)$ כלומר מהצורה: $\frac{u_i(\alpha_1,\dots,\alpha_d)}{v_i(\alpha_1,\dots,\alpha_d)}$

כאשר $u_i,v_i \in K[t_1,\dots,t_d]$

ע"י הכפלה במכנה משותף ניתן לנקות את המכנים ולהניח שמקדמי

הפולינום ש- β_1 פותר הינם ב- $K[\alpha_1,\dots,\alpha_d]$

הפולינום הזה חייב לערב את אחד ה- t_i-ים, בה"כ ע"י שינוי סדר את t_1

(כי אחרת הוא פולינום ב-X, ולכן אלגברי מעל K, בסתירה לכך ש- β_1 בלתי

תלוי אלגברית), אם נחשוב על p כעל פולינום ב-t_1 שמקדמיו פולינומים

ב- $t_2,\dots,t_d,X$ $\Longleftarrow$ α_1 אלגברי מעל $K(\beta_1,\alpha_2,\dots,\alpha_d)$ (החלפנו את α_1 ב-β)

כי L אלגברי מעל $K(\beta_1,\alpha_1,\dots,\alpha_d)$ (מפרקים את α_1 למה שישלנו ומקבלים

הרחבה אלגברית וכעת פשוט הגדלנו אותה עוד יותר ולכן L אלגברי מעליה).

בשלב השני, קיים $p \in K[t_1,t_2,\dots,t_d,X]$ כך ש- β_2 מקיים אותו, כלומר כך ש:

$p(\beta_1,\alpha_2,\dots,\alpha_d,\beta_2)=0$ עכשיו p חייב לערב את אחד מתוך $t_2,\dots,t_d$

כי אחרת β_1,β_2 תלויים אלגברית, בה"כ p מערב את t_2 ולכן α_2 אלגברי

מעל $(\beta_1,\beta_2,\alpha_3,\dots,\alpha_d)$ $\Longleftarrow$ L אלגברי מעל $K(\beta_1,\beta_2,\alpha_3,\dots,\alpha_d)$.

כך ממשיכים באינדוקציה עד שמראים ש-L אלגברי מעל $K(\beta_1,\dots,\beta_d)$

זה אומר ש $\beta_{d+1},\dots,\beta_e$ (אם $d<e$) כבר תלויים אלגברית

מעל קודמיהם, בסתירה למקסימליות e ולכן $d \ge e$ ובאותו אופן

מהפיך מראים $d \le e$ $\Longleftarrow$ $e=d$.

26-6-2007

מבנים אלגבריים 2 - שיעור מס' 22

הבהרה לגבי אתמול: (בעקבות שאלה שנשאלה)

$L=K(\alpha_1,\dots,\alpha_n)$

הגדרה: דרגת הטרנסצנדנטיות (L/K) $tr.deg$ הינו המספר המקסימלי d כך שמתוך $\alpha_1,\dots,\alpha_n$ ישנם d איברים בלתי תלויים אלגברית מעל K

משפט (שטייניץ): המספר הנ"ל מוגדר היטב: כלומר אם $L=K(\beta_1,\dots,\beta_m)$ ו- e המס' המקסימלי מתוכם שהם בלתי תלויים אלגברית, אז $e=d$.

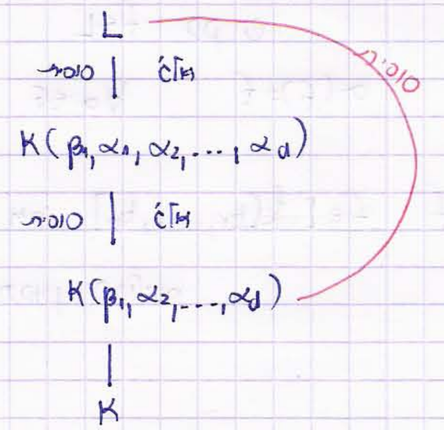
הוכחה: (עשינו אתמול) הסתמכה על "החלפה" של איברים

$\underbrace{K(\alpha_1,\dots,\alpha_d)}_{\text{בלתי תלויים אלגברית}} \subset L$ (אלגברית סופית)

$K(\beta_1,\dots,\beta_e) \subset L$ (אלגברית סופית)

נניח על דרך השלילה $d<e$

בה"כ α_1 אלגברי מעל $K(\beta_1,\alpha_2,\dots,\alpha_d)$



אם ניתן למצוא בסיס טרנסצנדנטלי $\alpha_1,\dots,\alpha_d$ כך ש:

$L=K(\alpha_1,\dots,\alpha_d)$

$\cong K(t_1,\dots,t_d)$

אומרים ש L/K הרחבה טרנסצנדנטלית טהורה.

המשוואה הפולינומיאלית הכללית ממעלה n

נתחיל משדה בסיס k (נשתמש בו כשדה סקלרים)

k = שדה הבסיס (למשל $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$)

$$L = k(t_1, \ldots, t_n)$$

$t_1, \ldots, t_n$ משתנים בלתי תלויים אלגברית

$G = S_n$ חבורת התמורות על $\{1, 2, \ldots, n\}$

$\sigma \in G$ נגדיר פעולה על L ע"י $\sigma|_k = id$

$$\sigma(t_i) = t_{\sigma(i)}$$

למשל: $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\quad n=3$

$$\sigma\left(\frac{t_1^2 - t_2 + t_3^2}{1 - t_2 t_3}\right) = \frac{t_2^2 - t_1 + t_3^2}{1 - t_1 t_3}$$

$$\sigma \in Aut(L)$$

איבר של L שהינו אינוריאנטי תחת פעולת G

$f \in L$ כך ש

$\forall \sigma \in G \quad \sigma(f) = f$ נקרא פונקציה (רציונלית) סימטרית

אם $f \in k[t_1, \ldots, t_n]$ f נקרא פולינום סימטרי

נתבונן בפולינום

$$f = (x - t_1)(x - t_2) \ldots (x - t_n)$$

$$f \in L[x]$$

$$= x^n - (t_1 + \ldots + t_n)x^{n-1} + \left(\sum_{i<j} t_i t_j\right) x^{n-2} - \ldots + (-1)^n t_1 t_2 \ldots t_n$$

$$= x^n - s_1 x^{n-1} + s_2 x^{n-2} - \ldots + (-1)^n s_n$$

$$s_i = \sum_{j_1 < j_2 < \ldots < j_i} t_{j_1} t_{j_2} \ldots t_{j_i}$$

אם $\sigma \in G$ $\quad \sigma f = f$ (כי σ רק משנה את סדר הגורמים) ולכן $\sigma(s_i) = s_i$

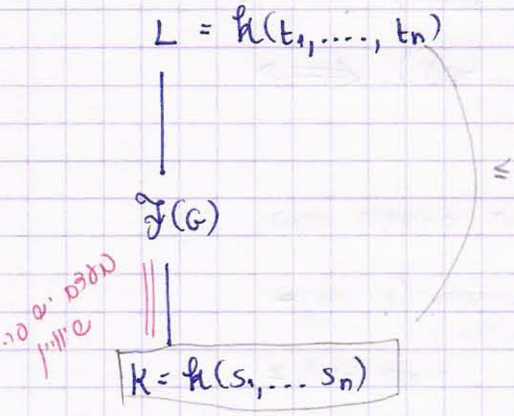
ולכן ה-s_i הינם פולינומים סימטריים - הפולינומים הסימטריים היסודיים

26-6-2007

משפט: (א) השדה $K = k(s_1,\dots,s_n) \subset L$ הינו שדה השבת של G.

(ב) $G \cong Gal(L/K)$ ו- $[L:K]=n!$

(ג) K הינו הרחבה טרנסצנדנטית טהורה של k מדרגת טרנסצנדנטיות n ו- $s_1,\dots,s_n$ בלתי תלויים אלגברית.



הוכחה: ברור ש- $K \subset \mathcal{F}(G)$ כי s_i אינווריאנטי תחת פעולת G.

מצד אחד עפ"י המשפט היסודי של תורת גלואה

$G \subseteq Aut(L)$

$$G \cong Gal(L/\mathcal{F}(G))$$

$L/\mathcal{F}(G)$ הרחבת גלואה סופית ולכן $[L:\mathcal{F}(G)]=n!$

מצד שני, הפולינום $f \in K[x]$ כי מקדמיו הם בדיוק $s_1,\dots,s_n$

$$f=(x-t_1)\cdots\cdots(x-t_n)$$

שורשיו $t_1,\dots,t_n$ פורשים את L ולכן L שדה פיצול של f מעל K.

ראינו משפט שאומר שדרגת שדה הפיצול של פולינום ממעלה n הינה לכל היותר $n!$

כלומר $[L:K]\le n!$

$\Longleftarrow$ $[L:K]=n!$ ו- $k=\mathcal{F}(G)$

עד כה הוכחנו (א) ו-(ב)

עבור להוכחת חלק (ג):

ראינו כי $tr.deg\ L/K=n$. אם $\exists$ מתוך $s_1,\dots,s_n$

רק d מת"א והשאר אלגבריים מעליהם אזי L היתה הרחבה אלגברית של הרחבה טרנסצנדנטית טהורה מדרגה טרנסצ' d $\deg(L/k)=d$ $\Longleftarrow$ $d=n$

מאחר ו- $s_1,\dots,s_n$ בלתי תלויים אלגברית מעל k הם יכולים להחשב כפרמטרים בלתי תלויים והפולינום

$$f=x^n-s_1x^{n-1}+s_2x^{n-2}-\dots+(-1)^n s_n$$

הינו הפולינום הכללי ממעלה n.

ולכן **מסקנה:** אם L הינו שדה הפיצול של f מעל $K = k(s_1, \dots, s_n)$ אזי

L/K הרחבת גלואה עם $Gal(L/K) = S_n$

מסקנה מן המסקנה: אם $n \geq 5$ הפולינום הכללי ממעלה n אינו פתיר בעזרת רדיקלים (מעל $k(s_1, \dots, s_n)$)

הוכחה: עפ"י ההגדרה, f פתיר בעזרת רדיקלים $\Longleftrightarrow$ L הרחבה רדיקלית של K $\Longleftrightarrow$ (על סמך המשפט היסודי משפט שעבר) $Gal(L/K)$ חבורה פתירה.

$\Longleftrightarrow$ (עבור S_n) $4 \geq n$.

בשני השיעורים הבאים שנותרו נעשה כמה השלמות:

* (נדבר על) סגור אלגברי של שדה
* שדות סופיים
* בניית מצולעים משוכללים בעזרת סרגל ומחוגה.

2-7-2007

מבנים אלגבריים 2 - שיעור מס' 23

שימושים והשלמות

נדבר היום על:

- שדות סופיים
- משפט האיבר הפרימיטיבי
- סגור אלגברי
- מצולעים משוכללים.

שדות סופיים

נניח כי F שדה סופי

המציין שלו חיובי ממש והוא מס' ראשוני $0<p=\text{char}F$

F מכיל את השדה $\mathbb{F}_p$: $\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p\subseteq F$

(השדה הראשוני בן p איברים.)

טענה: (1) קיים n טבעי $|F|=p^n$ $\quad n=[F:\mathbb{F}_p]$

(2) F^* חבורה ציקלית מסדר p^n-1

(3) F הינו שדה הפיצול של $f(x)=x^{p^n}-x$ מעל $\mathbb{F}_p$, יתרה מזאת $F=\{f \text{ שורשי}\}$. הפולינום הנ"ל ספרבילי - כל שורשיו שונים.

(4) $F/\mathbb{F}_p$ הרחבת גלואה והחבורה שלה $Gal(F/\mathbb{F}_p)$ חבורה ציקלית מסדר n הנוצרת ע"י האוטומורפיזם של פרובניוס $\varphi(x)=x^p$.

הוכחה: (1) יהיו $w_1,\dots,w_n$ בסיס של F כמרחב וקטורי מעל $\mathbb{F}_p$.

כל איבר של F ניתן לכתיבה יחידה מהצורה:

$a_1w_1+a_2w_2+\dots+a_nw_n$

$a_i\in\mathbb{F}_p$ ולכן $|F|=p^n$

(2) F^* היא כמובן חבורה סופית בשדה (סופית כיוון שכך) והוכחנו משפט שבכל שדה, כל תת-חבורה סופית של F^* הינה ציקלית $\Leftarrow F^*$ ציקלית.

(3) כל איבר $x\in F^*$ מקיים $x^{p^n-1}=1$ (כל איבר בחזקת סדר החבורה $=1$)

פרט ל-אפס כל האיברים מקיימים זאת.

נכפול את שני האגפים ב-x $\quad x^{p^n}=x$ (וזה כבר מתקיים לכל האיברים כולל אפס)

$f(x)=x^{p^n}-x$ פולינום ממעלה p^n שמצאנו לו p^n שורשים שונים ב- F

$$x^{p^n}-x=\prod_{\alpha\in F}(x-\alpha) \Longleftarrow f(x)$$ ספרבילי, מתפצל ב- F

F -ו שדה הפיצול שלו ומתקבל עם אוסף שורשיו.

הערה: ש-$f(x)$ ספרבילי נובע מכך ש $f'=-1$

$\Longleftarrow \gcd(f,f')=1 \Longleftarrow f$ ספרבילי.

(4) $F/\mathbb{F}_p$ הרחבת גלואה ממעלה n בתור שדה פיצול של פולינום ספרבילי.

נתבונן ב: $\varphi(x)=x^p$

לכל שדה ממציין p זהו אנדומורפיזם ≡ הומומורפיזם של השדה) עצמו (טרבי לא על)

$$(x\cdot y)^p=x^p\cdot y^p$$

$$(x+y)^p=x^p+y^p$$

הוא F סופי במקרה שלנו, φ גם על ולכן

$\varphi\in Gal(F/\mathbb{F}_p)$

המשפט הקטן של פרמה.
$$\begin{cases} x^p=x & \forall x\in\mathbb{F}_p \\ a^p\equiv a \bmod p & \forall a\in\mathbb{Z}\end{cases}$$

$$\varphi^m(x)=x^{p^m}$$

$$\varphi^2(x)=\varphi(\varphi(x))=\varphi(x^p)=\varphi(x)^p=(x^p)^p=x^{p^2}$$

וכן הלאה..

הסדר של φ = ה- m המינימלי עבורו $\varphi^m=e$ (הזהות)

= ה- m המינימלי עבורו $x^{p^m}=x$ לכל x.

למשוואה הנ"ל לכל היותר p^m פתרונות ב- F ולכן ה- m המינימלי הינו $m=n$.

= הסדר של φ הינו n.

2-7-2007

$$|Gal(F/\mathbb{F}_p)| = [F:\mathbb{F}_p] = n$$

ולכן $Gal(F/\mathbb{F}_p) = \langle \varphi \rangle$ ציקלית.

מסקנה: שני שדות סופיים בעלי אותו מספר איברים איזומורפיים

הוכחה: p^m איברים

q^n איברים

p, q ראשוניים

$p^m = q^n \Longleftarrow$ $\left.\begin{matrix} p=q \\ m=n \end{matrix}\right\}$ $\Longleftarrow$ שני השדות הינם שדות פיצול של אותו פולינום מעל $\mathbb{F}_p$.

(נסגור עכשיו להוכחת קיום)

טענה 2: לכל n יש שדה אחד ויחיד עד כדי איזומורפיזם בן p^n איברים

שיסומן $\mathbb{F}_{p^n}$ (≡ שדה גלואה בן p^n איברים).

$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \Longleftrightarrow m|n$ ותתי השדות של $\mathbb{F}_{p^n}$ הינם בהתאמה

חח"ע עם המחלקים של n.

הוכחה: (א) יהיה F שדה הפיצול של $x^{p^n}-x$ מעל $\mathbb{F}_p$.

שורשי $x^{p^n}-x$ מהווים קבוצה סגורה תחת פעולות השדה. כי הם אוסף האיברים

ה x-ים שמקיימים

$\varphi^n(x) = x^{p^n} = x$ (נקודות השבת של φ^n)

$(x+y)^{p^n} = x^{p^n} + y^{p^n}$

$(xy)^{p^n} = x^{p^n} y^{p^n}$

$F =$ השדה הקטן ביותר, המינימלי המכיל את שורשי $f(x)$ ולכן הוא מתלכד עם אוסף השורשים

ולכן f ספרבילי $\Longleftarrow$ $|F| = p^n$

(ב) אם $\mathbb{F}_p \subset \mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ (כאשר $[\mathbb{F}_{p^n}:\mathbb{F}_p]=n$ ו-$[\mathbb{F}_{p^m}:\mathbb{F}_p]=m$)

$[\mathbb{F}_{p^m}:\mathbb{F}_p] \,|\, [\mathbb{F}_{p^n}:\mathbb{F}_p]$ (מכפליות הדרגות במגדלים)

$\Longleftarrow m|n$

להיפך, אם $m|n$ יש ל $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ שהיא ציקלית מסדר n,

תת-חבורה יחידה מסדר $d=\frac{n}{m}$ הנוצרת ע"י φ^m.

שדה השבת של תת-חבורה זאת הינו מדרגה $m=\frac{n}{d}$ מעל $\mathbb{F}_p$ ולכן הוא

איזומורפי ל $\mathbb{F}_{p^m}$.

מסקנה:

$$x^{p^m}-x \mid x^{p^n}-x$$

$$\iff m|n.$$

הוכחת המסקנה:

$$x^{p^m}-x \mid x^{p^n}-x$$

$$\iff \mathbb{F}_{p^m}\subset\mathbb{F}_{p^n}$$

$$\iff m|n.$$

פה: סתם עובדה על חלוקת פולינומים

ניתן להוכיח אותה ישירות ללא תורת

גלואה (וכן תרגיל: תנו הוכחה ישירה

למסקנה!

∞

הבהרה לגבי הגדרות:

אמרנו:

(הגדרנו הרחבה רדיקלית כ:

$$\overset{\text{רדיקלית}}{K\subset L}\subset K(\alpha_1,\dots,\alpha_n)$$

$$\alpha_i^{N_i}\in K(\alpha_1,\dots,\alpha_{i-1})$$

מתרגל:

$K\subset M\subset L$ ($K\subset L$ רדיקלית, $K\subset M$ לא רדיקלית)

מתרגל ④ בדף 10 שקיבלנו מחפשים בעצם להרחבה $K(\alpha_1,\dots,\alpha_n)$

$\alpha_i^{N_i}\in K(\alpha_1,\dots,\alpha_{i-1})$ ושדה ביניים M שאינו מהצורה: $K(\beta_1,\dots,\beta_m)$ $\beta_i^{M_i}\in K(\beta_1,\dots,\beta_{i-1})$

∞

2-7-2007

אם מסתכלים על הפולינום $x^3+ax+b=0$

$K=\mathbb{C}(a,b)$

$K \subset K(\theta) \subset K(\alpha_1,\alpha_2)$

S_3 ביטויים רדיקלים

(עזרה בנושא לתרגיל) מ"ת

משפט האיבר הפרימיטיבי

$$L=K(\alpha_1,\dots,\alpha_m)$$
$$|$$
$$\vdots$$
$$K(\alpha_1,\alpha_2)$$
$$|$$
$$K(\alpha_1)$$
$$|$$
$$K$$

משפט האיבר הפרימיטיבי:

אם L/K הרחבה ספרבילית סופית. אזי, $L=K(\theta)$ עבור θ מסוים (הרחבה פשוטה)

(בפרט כל הרחבה סופית ממציין 0 הינה פשוטה)

הוכחה: אם K סופי, גם L שדה סופי, ולכן F^* החבורה הכפלית ציקלית (מתקיים השמו)

ואם θ יוצר שלה $L=K(\theta)$.

מעכשיו נניח כי K שדה אינסופי

למה: כל הרחבה ספרבילית סופית L/K ניתנת לשיכון בהרחבה סופית ספרבילית ונורמלית M/K ($\equiv$ גלואה)

הוכחת הלמה: יהיו $\alpha_1,\dots,\alpha_r$ יוצרים של L מעל K.

יהיו $f_1,\dots,f_r \in K[x]$ הפולינומים המינימליים שלהם. (הנחת הספרבילית היא שהפולינומים הנ"ל ספרבילים)

על פי ההנחה, f_i ספרבילים.

f_i אי-פריקים ולכן $f_i=f_j$ או $(f_i,f_j)=1$ (זרים)

לכן מכפלת ה-f_i-ים (בלי חזרות) הינה פולינום ספרבילי - כי משפה פיצול שלו כל שני גורמים לינאריים שלו שונים - כי אם הם מאותו f_j עם $i\neq j$ אז $(f_i,f_j)=1$ ואם הם מאותו f_i, אז f_i ספרבילי.

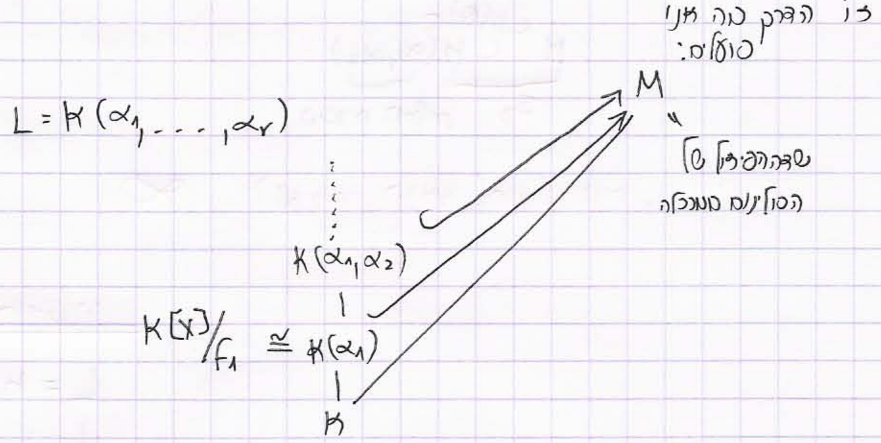
ולכן המכפלה הינה פולינום ספרבילי.

שדה הפיצול של הפולינום הזה היא הרחבת גלואה ($\equiv$ שדה פיצול של פולינום ספרבילי)

הוכחנו בשיעורים קודמים

ועל סמך משפט הרחבת השיכונים ניתן לשכן את L.

☒ הוכחת הלמה.



נחזור להוכחת המשפט:

L/K ספרבילית $\xLeftarrow{\text{למה}}$ ניתנת לשיכון ב M/K גלואה.

שדות ביניים $K \subseteq ? \subseteq M$ הם בהתאמה חח"ע עם $H \le Gal(M/K)$ (תת-חבורה)

ויש רק מס' סופי של H $\Longleftarrow$ מס' סופי של אפשרויות לשדות ביניים "?"

מכאן יש רק מס' סופי של שדות ביניים $K \subseteq F \subseteq L$

(הערה: יש דוגמה של הרחבה אי-ספרבילית $[L:K]=p^2$ עם אינסוף שדות ביניים

$$\underbrace{K \subset F}_{p}\underbrace{\subset L}_{p}$$
)

נשתמש בהוכחת משפט האיבר הפרימיטיבי רק ב-2 הדברים הבאים:

(1) K אינסופי

(2) יש מס' סופי של שדות ביניים $K \subseteq F \subseteq L$

נניח על דרך השלילה L איננה פשוטה ותהי $K \subset K(\alpha) \subset L$ הרחבה פשוטה מקסימלית. (ביחס להכלה)

יהיה β $\beta \in L \setminus K(\alpha)$ (לא נמצא ב-$K(\alpha)$) ונתבונן בשדות $F_t = K(\alpha + t\beta)$ כאשר $t \in K$

יש אינסוף אפשרויות ל-t (בגלל (1)) אבל רק מס' סופי של שדות ביניים (בגלל (2))

מכאן שיש $t_1 \neq t_2$ ב-K שבהם מתקיים ש $F_{t_1} = F_{t_2}$

כלומר $F = K(\alpha + t_1\beta) = K(\alpha + t_2\beta)$ (נסמן אותו פשוט ב-F)

$$\alpha + t_1\beta \in F$$

$$\alpha + t_2\beta \in F$$

נחסר ונחלק

$$\alpha = (\alpha + t_1\beta) - t_1\beta \in F \quad \Longleftarrow \quad \frac{(\alpha+t_1\beta)-(\alpha+t_2\beta)}{t_1 - t_2} = \beta \in F$$

$\Longleftarrow$ F מכיל את $K(\alpha)$ ממש

$K(\alpha) \subsetneq F$ כי $\beta \in F$ וזו סתירה לכך ש-$K(\alpha)$

הרחבה פשוטה מקסימלית.

$\Longleftarrow$ $L = K(\alpha)$

$\blacksquare$

מחר נמשיך עם הנושאים שהזכרנו בתחילת השעור.

3-7-2007

מבנים אלגבריים ב- שעור אחרון

(1)

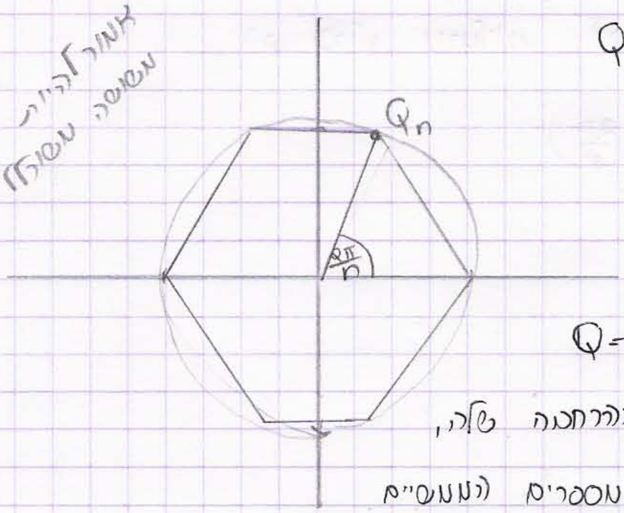
שעור חזרה לקראת המבחן:

24/7/2007 בשעה 9:00

לוין 8

מצולעים משוכללים -

בניה בסרגל ומחוגה.



אמור להיות משושה משוכלל

$S=\{(0,0),(1,0)\}$ $Q_n=(\cos\frac{2\pi}{n},\sin\frac{2\pi}{n})$

גאוס תאר בניה עבור $n=17$

נדבר רק על $n=p$ ראשוני.

שדה הבסיס = $\mathbb{Q}$, אם נקודה $Q=(x_Q,y_Q)$ ניתנת לבניה בסרגל ומחוגה אזי דרגת ההרחבה שלה, כלומר, הדרגה של השדה שנוצר מסיפוח המספרים הממשיים x ו- y של הנקודה הינה חזקת 2 (הוכחנו)

$[\mathbb{Q}(x_Q,y_Q):\mathbb{Q}]=$ חזקת 2

חישובי דרגה:

$\zeta=e^{\frac{2\pi i}{p}}$

$\zeta^{-1}=\bar{\zeta}$ (הצמוד המרוכב)

$\frac{\zeta+\bar{\zeta}}{2}=\cos\frac{2\pi}{p}$

$\frac{\zeta-\bar{\zeta}}{2i}=\sin\frac{2\pi}{p}$

$\mathbb{Q}(\zeta,i)=\mathbb{Q}(\cos\frac{2\pi}{p},\sin\frac{2\pi}{p},i)$

- $\mathbb{Q}(\zeta,i)$ — 1 או 2 — $\mathbb{Q}(\zeta)$
- $\mathbb{Q}(\zeta,i)$ — 2 — $\mathbb{Q}(\cos\frac{2\pi}{p},\sin\frac{2\pi}{p})$
- $\mathbb{Q}(\zeta)$ — $p-1$ (הרחבה ציקלוטומית) — $\mathbb{Q}$
- $\mathbb{Q}(\cos\frac{2\pi}{p},\sin\frac{2\pi}{p})$ — $\frac{p-1}{2}$ או $p-1$ ← מחישובי דרגות — $\mathbb{Q}$

חבורה ציקלית מסדר p-1

* **מסקנה 1**: אם p-1 אינו חזקת 2 אזי אי-אפשר לבנות מצולע משוכלל בן p צלעות בסרגל ומחוגה.

* נניח $p=2^r+1$ (ראשוני של פרמה) לדוגמא $17=2^4+1$ $5=2^2+1$

ההרחבה הנ"ל $\left\{\begin{array}{l}\mathbb{Q}(\zeta)\\ |\\ \mathbb{Q}\end{array}\right.$ חבורה ציקלית מסדר $p-1=2^r$ והיא איזומורפית ל $(\mathbb{Z}/p\mathbb{Z})^*$

הראינו ש- $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})\cong\mathbb{Z}/p\mathbb{Z}$ (דרגה p-1)

$\sigma\mapsto\chi(\sigma)$

המשך ←

ההרחבה $K=\mathbb{Q}(\cos\frac{2\pi}{p},\sin\frac{2\pi}{p})$ הינה הרחבה אבלית

$$K \;|\; \mathbb{Q}$$

מסדר 2^r או 2^{r-1}

נסמן:

$G=Gal(\mathbb{Q}(\cos\frac{2\pi}{p},\sin\frac{2\pi}{p})/\mathbb{Q})$ אז ∃ $G=H_0\supset H_1\supset\dots\supset H_r=\{e\}$

רק שכולן נורמליות (כי G אבלית) $[H_i:H_{i+1}]=2$

$$p-1=2^r \left\{ \begin{array}{l} K_r=K=\mathbb{Q}(\cos\frac{2\pi}{p},\sin\frac{2\pi}{p}) \\ \quad | \\ \quad \vdots \\ K_2 \\ 2\,| \\ K_1=\mathcal{F}(H_1) \\ 2\,| \\ \mathbb{Q}=K_0 \end{array} \right.$$

* ניתן לבנות את ההרחבות ריבועיות.

נאמר שמספר α ניתן לבניה מתוך שדה F אם הנקודה $(\alpha,0)$ ניתנת לבניה מכל הנקודות $(x,0)$ כאשר $x\in F$.

למה: (1) אם קבוצת מספרים S ניתנת לבניה אז גם השדה שהם יוצרים ניתן לבניה.

(2) אם $a>0$ ניתן לבניה אז גם $\sqrt{a}$ ניתן לבניה.

מסקנה $\Leftarrow$ $(\cos\frac{2\pi}{p},\sin\frac{2\pi}{p})$ ניתנת לבניה (כאשר p הינו ראשוני של פרמה)

$(\mathbb{Z}/p\mathbb{Z})^*$ היא ציקלית ובפרט אבלית.

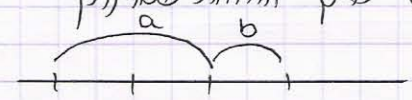
המשפט הנ"ל הוא מקרה של שדות השמת של החבורות כאשר כל הרחבה היא ריבועית, הרחבות ריבועיות תמיד מתקבלות ע"י פיתוח שורש, במקרה הנ"ל סגרה.

3-7-2007

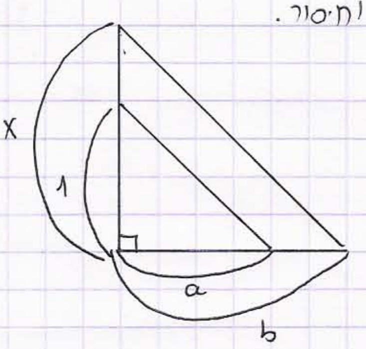
②

הוכחת הלמה:

(1) צריך להראות שבהינתן a,b ניתן לבנות את $a \pm b$, $a \cdot b$ ו $\frac{a}{b}$:



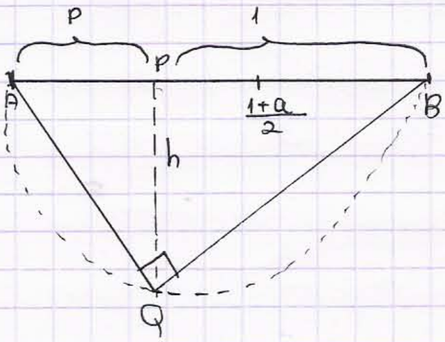
וכך מתקבל חיבור וחיסור.



כפל וחילוק נראה בעזרת דמיון משולשים

$$\frac{1}{x} = \frac{a}{b} \Longrightarrow x = \frac{b}{a}$$

(2)



$$\frac{h}{1} = \frac{a}{h} \Longrightarrow h = \sqrt{a}$$

מדמיון $\triangle PQB \sim \triangle PAQ$

משפט: מצולע משוכלל בן n צלעות ניתן לבניה בסרגל ומחוגה $\Longleftrightarrow$ $n = 2^e p_1 \cdots p_r$ כאשר p_i ראשונים של פרמה מהצורה $p_i = 2^{r_i}+1$ שונים זה מזה, אם 2^r+1 הינו ראשוני אזי $r = 2^s$ $\quad p_i = 2^{2^{s_i}}+1$