① 12.05.08
מבנים

בוקר טוב!

המרצה: שחר מוזס

הקורס נקרא מבנים אלגבריים ב אבל ראוי היה שייקרא תורת השדות או תורת גלואה.

ספרות:
- Artin, Galois Theory
- Rotman, Galois Theory
- Stewart
- Milne (www.jmilne.org/math/coursenotes)

המוטיבציה מתחילה בניסיון לפתור משוואות. שתי הדמויות המרכזיות הן גלואה ואבל. גלואה היה הראשון שהשתמש במושג החבורה. כך שהיסטורית תורת גלואה נוסדה לפני תורת החבורות.

את מושג השדה אנחנו כולנו מכירים עוד משנה א'.
דוגמאות: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ (p ראשוני).

אבל יש עוד המון שדות, ואנחנו נדבר על איך אפשר לבנות שדות שונים ומשונים.

חוג פולינומים: יהי F שדה. $F[X]$ חוג הפולינומים מעל F
איבריו $p(X) = a_m X^m + a_{m-1} X^{m-1} + \dots + a_1 X + a_0$
כאשר $a_i \in F$ ו- $m \in \mathbb{N}$ על איברים אלה מוגדרים חיבור וכפל כפי שאנו מבינים 1, והפעולות האלה יוצרות מבנה של חוג.

טענה: חוג הפולינומים מעל שדה הוא חוג אוקלידי.

תזכורת: חוג R נקרא חוג אוקלידי אם:
- R חוג שלמות (חוג קומוטטיבי ללא מחלקי אפס)
- R חוג עם יחידה

- קיימת פונקציה $d: R\setminus\{0\} \longrightarrow \mathbb{Z}^{\geq 0}$ כך ש:

(א) $a,b \in R\setminus\{0\}$ $d(a) \leq d(ab)$

(ב) $a,b\in R$, $a\neq 0$ $\Leftarrow$ קיימים $q,r\in R$ כך ש- $b=aq+r$ ואם $r\neq 0$ אז $d(r)<d(a)$

תזכורת: חוג אוקלידי R הוא חוג ראשי, כלומר כל אידיאל $I\lhd R$ הוא מהצורה $I=(a)=aR$.

בקורס זה תמיד נדבר על חוגים קומוטטיביים

הגדרה: יהי R תחום שלמות

① איבר $a\in R$ ^לא הפיך^ ייקרא **ראשוני** אם לכל $b,c\in R$, אם $a|bc$ אז $a|b$ או $a|c$.

② איבר $a\in R$ ייקרא **הפיך** אם קיים $b\in R$ כך ש- $ab=1$

③ $a\in R$ ייקרא **פריק** אם ניתן להציגו כמכפלה $a=bc$ כאשר b,c אינם הפיכים. אחרת, הוא ייקרא **אי-פריק**.

משפט: בחוג אוקלידי איבר הוא אי-פריק אמ"מ הוא ראשוני.

משפט הפריקות היחידה: יהי R חוג אוקלידי ויהי $0\neq a\in R$ איבר לא הפיך. אז ניתן להציגו כמכפלה $a=r_1 r_2 \cdot\ldots\cdot r_k$ $(k\in\mathbb{N})$ $r_i\in R$ אי פריקים. יתר על כן, הצגה זו יחידה עד כדי סדר ויחס יחידות: אם $a=t_1 t_2\ldots t_m$ עבור $t_i\in R$ אז $k=m$ וקיימת תמורה $\pi\in S_k$ כך שלכל $1\leq i\leq k$ $r_i=\varepsilon_i t_{\pi(i)}$ כאשר $\varepsilon_i\in R$ הפיך.

מסקנה: בהינתן פולינום $p(x)\in F[X]$ כך ש- $\deg p(x)\geq 1$ (כלומר, הוא לא הפיך) אזי ניתן להציגו כמכפלת פולינומים אי-פריקים. אם $p(x)$ פולינום מתוקן $p(x)=x^m+a_{m-1}x^{m-1}+\ldots+a_0$ אזי ניתן להציגו כמכפלת פולינומים אי פריקים מתוקנים באופן יחיד עד כדי סדר.

הדבר ב- $\mathbb{C}$ הגיע מהרצון לפתור את הפולינום $x^2+1=0$ לפולינום הזה אין פיתרון ב- $\mathbb{R}$.

הפולינום $p(x)=x^2+1$ הוא פולינום אי-פריק. למה? אם הוא היה פריק בהכרח היה $p(x)=(x-\alpha_1)(x-\alpha_2)$ אבל זה אומר ש- $p(\alpha_2)=p(\alpha_1)=0$. אבל אין לפולינום הזה שורשים ב- $\mathbb{R}$!

באופן כללי, זה לא נכון שאם לפולינום אין שורשים אז הוא אי-פריק. למשל, אם ל- $p(x)=(x^2+1)^2$ אין שורשים ב- $\mathbb{R}$, אבל הוא בוודאי פריק.

עוד דוגמה היא x^2+x+1. קל להראות שהוא אי-פריק. אבל אם $x^{16}+x^{15}+\dots+x+1$ הוא אי-פריק אבל את זה מאוד קשה לנו כרגע להוכיח. נרצה לפתח שיטות שיאפשרו לנו להתמודד עם הבעיה הזו.

פריקות פולינומים ב- $\mathbb{Z}[X]$

הלמה של גאוס: יהי $f\in\mathbb{Z}[X]$ פולינום ממעלה ≥ 1 $f(x)=a_mx^m+a_{m-1}x^{m-1}+\dots+a_0$. אזי אם f פריק ב- $\mathbb{Q}[X]$ אזי הוא פריק גם ב- $\mathbb{Z}[X]$.

הוכחה: נניח ש- $f=gh$ כאשר $g,h\in\mathbb{Q}[X]$:

$$a_mx^m+a_{m-1}x^{m-1}+\dots+a_0=\left(\sum_{i=0}^{k}b_ix^i\right)\left(\sum_{j=0}^{m-k}c_jx^j\right)$$

כאשר $b_i,c_j\in\mathbb{Q}$. הרעיון הוא להפטר ממכנה משותף.
יהיו $r,s\in\mathbb{N}$ כך ש- $g_1=rg\in\mathbb{Z}[X]$, $h_1=sh\in\mathbb{Z}[X]$
לכן $rs\,f(x)=g_1(x)h_1(x)$ (*).
אם $rs=1$ סיימנו. אחרת, יהי p ראשוני כך ש- $p\mid rs$.
נתבונן בשוויון (*) מודולו p. נקבל שוויון

$$\overline{rs\,f(x)}=\overline{g_1(x)}\cdot\overline{h_1(x)}$$

כאשר עבור פולינום $q(x)=\sum_{i=0}^{n}d_ix^i\in\mathbb{Z}[X]$ נסמן $\overline{q(x)}=\sum_{i=0}^{n}\overline{d_i}x^i\in F_p[X]$ כאשר $\overline{d_i}\in\mathbb{Z}/p\mathbb{Z}$ תמונת d_i מודולו p.

נשים לב שההעתקה $\mathbb{Z}[X] \longrightarrow F_p[X]$

$g(x) \longmapsto \overline{g(x)}$

היא הומומורפיזם של חוגים ולכן $\overline{g_1(x)h_1(x)} = \overline{g_1(x)}\,\overline{h_1(x)}$

אז קיבלנו $0 = \overline{g_1(x)}\,\overline{h_1(x)}$. ואמנם זה תחום שלמות

$\Leftarrow$ $\overline{g_1(x)}=0$ או $\overline{h_1(x)}=0$. נניח לשם $\overline{g_1(x)}=0$

כלומר כל מקדמי $g_1(x)$ מתחלקים ב- p. לכן $g_1(x)=pg_2(x)$

עבור $g_2(x)\in\mathbb{Z}[X]$. לכן $\frac{rs}{p}f(x)=g_2(x)h_1(x)$

אם $\frac{rs}{p}=1$ סיימנו ומצאנו פירוק של $f(x)$ כמכפלת פולינומים

ב- $\mathbb{Z}[X]$. אחרת נבחר שוב ראשוני שמחלק את $\frac{rs}{p}$ ונחזור

על התהליך עד שנקבל $f(x)=g_j(x)h_j(x)$.

התהליך הזה בהכרח "ייגמר" כי בכל שלב $\frac{rs}{p}$ קטן יותר... ☺

<u>קריטריון אייזנשטיין</u>: יהי $f(x)=\sum_{i=0}^{m}a_i x^i\in\mathbb{Z}[X]$ ונניח שקיים

ראשוני p כך ש-

① $p\nmid a_m$

② $p\mid a_i$ עבור $0\le i\le m-1$

③ $p^2\nmid a_0$

אז $f(x)$ אי-פריק.

<u>הוכחה</u>: נניח ש- $f=gh$ כאשר $g,h\in\mathbb{Z}[X]$. נתבונן

בשוויון זה מודולו p - $\bar f=\bar g\,\bar h$ כאשר $f\mapsto\bar f$ ההעתקה

מההוכחה הקודמת. אבל $\bar f=\bar a_m X^m$ ו- $0\ne\bar a_m\in F_p$.

$\Leftarrow$ $\bar g=\bar c_k X^k$ ו- $\bar h=\bar d_{m-k}X^{m-k}$ כאשר $\bar c_k\bar d_{m-k}=\bar a_m$.

$\Leftarrow$ $c_i\in\mathbb{Z}$ $\quad g=c_kX^k+c_{k-1}X^{k-1}+\dots+c_0$

$d_i\in\mathbb{Z}$ $\quad h=d_{m-k}X^{m-k}+\dots+d_0$

כאשר $p\mid c_i$ ל- $0\le i\le k-1$ ו- $p\mid d_i$ ל- $0\le i\le m-k-1$

בפרט $p\mid c_0$ ו- $p\mid d_0$.

$\Leftarrow$ $f=gh=a_mX^m+\dots+a_0$

ו- $a_0=c_0d_0$ $\Leftarrow$ $p^2\mid a_0$ וזו סתירה. ☺

③

<u>טענה</u>: קיים אלגוריתם אפשר בהינתן פולינום $f\in\mathbb{Z}[X]$ מוצא פירוק שלו לגורמים אי פריקים.

<u>הוכחה</u>: נראה קיים חסם (ניתן לחישוב בזמן סופי) M (שתלוי ב-f) כך שאם $g=\sum h_i x^i\in\mathbb{Z}[X]$ מחלק את f אז $|h_i|\le M$ לכל i; ואז אפשר פשוט לחפש באופן שיטתי את כל המחלקים של f.

ידוע המשפט היסודי של האלגברה: כל פולינום מתוקן שמעלתו ≥ 1 מעל $\mathbb{C}$ $f\in\mathbb{C}[X]$ ניתן לפירוק כמכפלת גורמים ליניאריים $f(x)=\prod_{i=1}^{m}(x-\alpha_i)$ $\alpha_i\in\mathbb{C}$.

אז נניח שהפולינום f שלנו הוא (מספיק להוכיח לפולינום מתוקן)

$$x^m+a_{m-1}x^{m-1}+\dots+a_0=f(x)=\prod_{i=1}^{m}(x-\alpha_i)$$

נטען שכל שורש של הפולינום המתוקן $f(x)$ מקיים $|\alpha_i|\le\max\{1,mB\}$ כאשר $B=\max\{|a_i|:0\le i\le m-1\}$. נניח ש- $\max\{1,mB\}<|\alpha|$ ונראה ש- $f(\alpha)\neq 0$:

$$\left|\frac{f(\alpha)}{\alpha^{m-1}}\right|=\left|\frac{\alpha^m+a_{m-1}\alpha^{m-1}+\dots+a_0}{\alpha^{m-1}}\right|=$$

$$=\left|\alpha+a_{m-1}+\dots+\frac{a_0}{\alpha^{m-1}}\right|\geq$$

$$\geq\left||\alpha|-\left|a_{m-1}+\dots+\frac{a_0}{\alpha^{m-1}}\right|\right|\geq$$

$$\geq|\alpha|-\left|a_{m-1}+\dots+\frac{a_0}{\alpha^{m-1}}\right|\geq$$

$$\geq|\alpha|-\sum_{i=0}^{m-1}\left|\frac{a_i}{\alpha^{m-i-1}}\right|\geq$$

$$\underset{|\alpha|>1}{\geq}|\alpha|-\sum_{i=0}^{m-1}|a_i|\underset{|a_i|<B}{\geq}|\alpha|-mB>0$$

$$f(\alpha)\neq 0\Leftarrow|f(\alpha)|>|\alpha^{m-1}|>1\Leftarrow$$

⇐ אם נתון $f(x)$ פולינום מ-$\mathbb{Z}[X]$ מתוקן אזי ניתן למצוא חסם לכל אחד מהשורשים של f. נניח שיש פירוק $f=gh$

$I\subseteq\{1,\dots,m\}$ $f=\prod_{i=1}^{m}(x-\alpha_i)$, $h=\prod_{k\notin I}(x-\alpha_k)$, $g=\prod_{j\in I}(x-\alpha_j)$

בה"כ (כי אפשר לשנות את הסדר)

$$g=\prod_{i=1}^{r}(x-\alpha_i)=x^r+c_{r-1}x^{r-1}+\dots+c_0$$

$$c_0=\prod_{i=1}^{r}(-\alpha_i)\qquad c_{r+1}=-\sum_{i=1}^{r}\alpha_i$$

באופן כללי, $c_j = s_j(\alpha_1,\dots,\alpha_r)$ כאשר s_j הן הפונקציות הסימטריות שהן קבועות וידועות. לכן, מהיות חסם על גודל ה- $|\alpha_i|$ יש חסם על גודל כל אחד מהמקדמים c_i. $\Rightarrow$ מספיק לבדוק מספר סופי של פולינומים המועמדים לחלק את f.

כעת, בהינתן פולינום $f(x)\in\mathbb{Z}[X]$ שהוא לאו דווקא מתוקן, נעבור ראשית לפולינום מתוקן $\mathbb{Q}[X] \ni f_1(x)=\frac{1}{a_m}f(x)$.

$$f(x) = a_m X^m + a_{m-1}X^{m-1} + \dots + a_0$$

$$f_1(x) = X^m + \frac{a_{m-1}}{a_m}X^{m-1} + \dots + \frac{a_0}{a_m}$$

$$\tilde{f}(x) = a_m^m f_1\left(\frac{X}{a_m}\right) = a_m^m\left[\frac{X^m}{a_m^m} + \frac{a_{m-1}}{a_m}\cdot\frac{X^{m-1}}{a_m^{m-1}} + \frac{a_{m-2}}{a_m}\cdot\frac{X^{m-2}}{a_m^{m-2}} + \dots + \frac{a_0}{a_m}\right] =$$

$$= X^m + a_{m-1}X^{m-1} + a_m a_{m-2}X^{m-2} + \dots + a_m^{m-1}a_0$$

$\tilde{f}(x)\in\mathbb{Z}[X]$ פולינום מתוקן ואותו אנחנו יודעים לפרק. לכן אנחנו יודעים לפרק גם את $f(x)$ (תרגיל!)

☺

תרגיל: את אותו התהליך אפשר היה להתחיל גם מפולינום ב- $\mathbb{Q}[X]$

④ 13.05.08

מבנים

אתמול דיברנו על פולינומים. אם F שדה אז פולינום $f\in F[X]$ נקרא אי-פריק אם $\deg f \ge 1$ ולא ניתן להציגו כמכפלה $f=gh$ כאשר $g,h\in F[X]$ ו- $\deg g, \deg h \ge 1$.

בגלל ש- $F[X]$ תחום אוקלידי, אי פריקות שקולה לראשוניות ואידיאל $I \triangleleft F[X]$ הוא מקסימלי אמ"מ הוא מהצורה $I=(f)$ כאשר $f\in F[X]$ אי-פריק.

<u>משפט</u>: $f\in F[X]$ פולינום אי-פריק אמ"מ $F[X]/(f)$ שדה.

<u>למה</u>: $I \triangleleft F[X]$ הוא מקסימלי אמ"מ הוא מהצורה $I=(f)$ כאשר $f\in F[X]$ אי-פריק.

<u>הוכחה</u>: נניח ש- f פולינום פריק, כלומר $f=gh$ עבור $g,h\in F[X]$ עם דרגות לפחות 1. אז $(f)\subsetneq(g)\subsetneq F[X]$ שהרי $p\in(f)$ אמ"מ קיים $q\in F[X]$ כך ש- $p=qf$ כלומר $p=q(gh)=(qh)g\in(g)$ $\Leftarrow$ $(f)\subseteq(g)$ היות שכל איבר ב- (f) הוא פולינום מדרגה לפחות $\deg f$ נובע ש- $g\notin(f)$ $\Leftarrow$ $(f)\subsetneq(g)$ וברור גם $1\notin(g)$ לכן $(g)\subsetneq F[X]$ $\Leftarrow$ (f) לא מקסימלי.

מצד שני, נניח ש- f אי-פריק ונראה ש- (f) מקסימלי. נניח בשלילה ש- (f) אינו מקסימלי, כלומר קיים אידיאל $J\triangleleft F[X]$ כך ש- $(f)\subsetneq J\subsetneq F[X]$. אבל זה תחום ראשי לכן קיים פולינום $h\in F[X]$ מדרגה לפחות 1 כך ש- $J=(h)$. אז $(f)\subsetneq(h)$ $\Leftarrow$ קיים פולינום $g\in F[X]$ כך ש- $f=gh$. נשים לב ש- $g\notin F$ (כי אחרת $(f)=(h)$), כלומר $\deg g\ge 1$ $\Leftarrow$ f פריק.

☺

אז עכשיו אם יש לנו שדה ופולינום אי-פריק מעל השדה הזה יש לנו דרך לבנות שדה חדש.

__משפט:__ יהי F שדה ויהי $p \in F[X]$ פולינום ממעלה לפחות 1. אז קיים שדה $F \subseteq E$ וקיים $\alpha \in E$ שורש של p, כלומר $p(\alpha) = 0$.

__הוכחה:__ יהי $f \in F[X]$ גורם אי פריק של p. כלומר $f \in F[X]$ עם דרגה $\deg f \geq 1$ רק ש- $p = f \cdot g$ ו- f אי-פריק. ברור שנמצא שורש ל- f אז מצאנו שורש ל- p. לכן די להראות קיים שדה $F \subseteq E$ ואיבר $\alpha \in E$ רק ש- $f(\alpha) = 0$.

נתבונן ב- $E = F[X]/(f)$. מאחר ש- f אי פריק, E הוא שדה וברור ש- $F \subseteq E$.

$$\varphi : F \longrightarrow E = F[X]/(f)$$

$$\varphi = \pi|_F$$

כאשר $\pi : F[X] \to E$ ההטלה הקנונית $\pi(g) = g + (f)$

אפשר לבדוק ש- φ חח"ע (תרגיל!)

נגדיר $\alpha = \pi(x) = x + (f)$. נראה ש- $f(\alpha) = 0$. נזכיר:

נסמן $(f) = I$ ו- $f(x) = \sum_{i=0}^{n} a_i x^i$

$$\Rightarrow f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = \sum_{i=0}^{n} a_i (x+I)^i =$$

$$= \sum_{i=0}^{n} a_i x^i + I = f + I = I$$

$$= 0_E$$

☺

אם ל- p היה שורש ב- F אז $p(x) = (x-\alpha)q(x)$

אז $F \cong F[X]/(x-\alpha)$. יש העתקת המנה הרגילה

$$\pi : F[X] \longrightarrow F[X]/(x-\alpha)$$

ויש

$$\varphi : F \longrightarrow F[X]/(x-\alpha)$$

$$r \longmapsto r + (x-\alpha)$$

די רק להראות שההעתקה הזאת על (בתרגיל ראינו שהיא חח"ע).

נניח $h \in F[X]$ ונחפש את המקור של $h(x) + (x-\alpha)$. נחלק עם שארית את $h(x)$ ב- $x-\alpha$: $h(x) = f(x)(x-\alpha) + s(x)$

כאשר $S(x)=0$ או $S(x)$ פולינום רק ש- $\deg s < 1$

$\Leftarrow$ $s \in F$. $\Leftarrow$ $\pi(h(x)) = h(x) + (x-\alpha) = f(x)(x-\alpha) + s + (x-\alpha) = s$
$= \varphi(s)$

$\Leftarrow$ φ הוא על.

__מסקנה__: יהי $p \in F[X]$ פולינום. אם $\alpha \in F$ שורש של p אמ"מ $p \mid (x-\alpha)$.

__הוכחה__: תרגיל בעזרת חלוקה עם שארית ב- $x-\alpha$

__מסקנה__: יהי F שדה ; $p \in F[X]$ $p = \sum_{i=0}^{n} a_i x^i$, $n \geq 1$.
אזי קיים שדה $F \subseteq L$ רק שב- $L[X]$ $p(x) = a_n \prod_{i=1}^{n} (x-\alpha_i)$

__הוכחה__: חוזרים על המשפט בדבר קיום הרחבה בה יש שורש שוב ושוב. נרשום $p = \prod_{i=1}^{m} f_i$ כאשר $f_i \in F[X]$ אי-פריקים. אם כולם לינאריים סיימנו. אחרת, יהי $f_1(x)$ אחד הגורמים שאינם לינאריים ונמצא שדה $F \subsetneq E$ רק שקיים $\alpha \in E$; $f_1(\alpha) = 0$. $\Leftarrow$ ב- $E[X]$ $f_1(x) = (x-\alpha)\tilde{f}_1$. נתבונן בפירוק לגורמים אי-פריקים של p ב- $E[X]$ $p = \prod_{i=1}^{k} g_i$. נשים לב ש- $m<k$. נחזור על התהליך כל עוד הפירוק שלנו אינו רק למכפלת פולינומים אי-פריקים לינאריים ונשים לב שמספר הגורמים במכפלה גדל. היות שמספר הגורמים לא יכול לעלות על n התהליך חייב להיעצר ומקבלים פירוק של p למכפלת גורמים לינאריים. ☺

__הגדרה__: אם F שדה ; $p \in F[X]$ אזי השדה המינימלי $F \subseteq E$ רק שב- $E[X]$ p מתפרק למכפלת גורמים לינאריים נקרא __שדה הפיצול__ של p.

__הערה__: שדה הפיצול קיים והוא יחיד עד כדי איזומורפיזם. דיבקדת עבודה רבה להוכיח את זה.

⑥ 19.05.08
מבנים

שעת קבלה: יום ג' 13-14 חדר 1 (מתמטיקה)

◆

בשיעור הקודם הגדרנו שדה פיצול.

F שדה. שדה E המכיל את F יקרא שדה הרחבה של F.
במקרה זה כמובן $E[X] \supseteq F[X]$. נאמר שפולינום $f \in F[X]$
כאשר $\deg f \geq 1$ מתפצל ב-$E[X]$ אם $f = a\prod_{i=1}^{d}(X-\alpha_i)$
כאשר $\alpha_i \in E$ ו- $d = \deg f$.
שדה $F \subseteq E$ הוא שדה פיצול עבור $f \in F[X]$ אם f מתפצל
ב-$E[X]$. שדה הפיצול של f הוא השדה המינימלי $F \subseteq E$
כך ש-f מתפצל ב-$E[X]$. (המינימליות ביחס להכלה)

<u>טענה</u>: בהינתן $f \in F[X]$ קיים שדה E כך ש-f מתפצל ב-$E[X]$

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

יהי $f \in F[X]$. יהי K שדה הרחבה של F כך ש-f מתפצל
ב-$K[X]$. בה"כ f פולינום מתוקן. אז $f(x) = \prod_{i=1}^{d}(x-\alpha_i)$ כאשר
$\alpha_i \in K$. תת השדה המינימלי של K המכיל את F ואת כל α_i
מסומן ב-$F(\alpha_1, \dots, \alpha_d)$ ושווה ל-$\bigcap_{\substack{L \subseteq K \text{ שדה} \\ F \subseteq L \\ \alpha_1, \dots, \alpha_k \in L}} L$ כמו
כן $F(\alpha_1, \dots, \alpha_d) = \left\{ \frac{p(\alpha_1, \dots, \alpha_d)}{q(\alpha_1, \dots, \alpha_d)} : \begin{array}{l} p, q \in F[X_1, \dots, X_d], \\ q(\alpha_1, \dots, \alpha_d) \neq 0 \end{array} \right\}$
(זה אנלוגי למרחב וקטורי שנפרש ע"י קבוצת וקטורים - כל הצירופים
הליניאריים שלהם).
נסמן $E = F(\alpha_1, \dots, \alpha_d) \subseteq K$. ברור שזהו שדה מינימלי ביחס להכלה
המוכל ב-K כך ש-f מתפצל מעליו.
אז ברגע שאנחנו חיים בתוך שדה כלשהו K, אפשר לדבר
על שדה <u>ה</u>פיצול בתוך K. אבל אנחנו נרצה משהו חזק יותר.

משפט: יהיו F שדה, $f\in F[X]$, $d=\deg f\geq 1$. יהיו $F\subseteq E$, $F\subseteq E'$ שדות כך ש- f מתפצל מעליהם והם מינימליים ביחס להכלה. אזי קיים F-איזומורפיזם (לא בהכרח יחיד ואפילו לא קנוני) $\varphi:E\to E'$.

למה: יהי F שדה ויהי $g\in F[X]$ פולינום אי-פריק. נניח ש- $F\subseteq L$ שדה כך שקיים $\alpha\in L$ כך ש- $g(\alpha)=0$ ו- $L=F(\alpha)$. אזי $L=F(\alpha)$ F-איזומורפי ל- $F[X]/(g)$ ע"י $\alpha\mapsto\bar{x}=x+(g)$.

מסקנה: אם $F\subseteq L'$ שדה כך ש- $L'=F(\beta)$ ו- $g(\beta)=0$ אזי L ו- L' F-איזומורפיים ע"י $\psi(\alpha)=\beta$.

דוגמה: הפולינום $1+x+x^2+x^3+x^4\in\mathbb{Q}[X]$ הוא אי פריק. נסמן ב- $w_0,\dots,w_4$ את שורשי היחידה ה-5. אזי $\mathbb{Q}(w_0)\cong\mathbb{Q}(w_3)$

הוכחת הלמה: נגדיר הומומורפיזם של חוגים $\varphi:F[X]\to F(\alpha)$

$$\left.\begin{array}{l} a\in F \Rightarrow \varphi(a)=a\\ \varphi(x)=\alpha\end{array}\right\}\Rightarrow h\mapsto h(\alpha)$$

נראה ש- φ על וש- $\ker\varphi=(g)$ ואז ינבע ש- $F[X]/(g)\cong F(\alpha)$

אפשר לראות ש- $h\in\ker\varphi$ אמ"מ $h(\alpha)=0$. צריך להראות ש- $(g)=\{h\in F[X]: h(\alpha)=0\}$. אם $h\in(g)$ אז $h=gp$ עבור $p\in F[X]$ ואז $h(\alpha)=g(\alpha)p(\alpha)=0\cdot p(\alpha)=0$

מצד שני, אם $h\in F[X]$ כך ש- $h(\alpha)=0$ אז היות ש- $F[X]$ חוג אוקלידי אפשר לחלק עם שארית ולקבל $h=gp+r$ כאשר $p,r\in F[X]$. אם $r=0$ סיימנו. אחרת $\deg r<\deg g$ ואז $0=h(\alpha)=\overset{0}{g}(\alpha)p(\alpha)+r(\alpha)=r(\alpha)$. קיבלנו שקיים פולינום $r\in F[X]$ ממעלה קטנה מאשר g כך ש- $r(\alpha)=0$. זה לא ייתכן: יהי $s\in F[X]$ המחלק המשותף המקסימלי של r ו- g. אז $\deg s\leq\deg r<\deg g$. מתקיים $s|g$ וזו סתירה לאי פריקות של g שכן $s=q_1g+q_2r$ ולכן $s(\alpha)=q_1(\alpha)g(\alpha)+q_2(\alpha)\underset{0}{r(\alpha)}=0$ $\Leftarrow$ $\deg s\geq 1$.

נותר להראות ש- φ על. אבל זה ברור כי $\varphi(F[X])=\{\sum_{i=0}^{n}a_i\alpha^i: a_i\in F\}$

נתבונן ב- $\bar{\varphi}:F[X]/(g)\to F(\alpha)$ המושרית ע"י φ. היות ש- $F[X]/(g)$ שדה ו- $\bar{\varphi}$

הומומורפיזם חח"ע, תמונתו $\bar{\varphi}(F[X]/(g))$ הוא שדה. זהו תת שדה
של $F(\alpha)$ המכיל את F כי $\bar{\varphi}(a)=a$ לכל $a\in F$.
וכן $\alpha=\varphi(\bar{x})\in\bar{\varphi}(F[X]/(g))$ כאשר $\bar{x}=x+(g)$
לכן נובע ש- $F[X]=\bar{\varphi}(F[X]/(g))$ ומתקיים
$\varphi(F[X])=\bar{\varphi}(F[X]/(g))$ ☺

המסקנה אומרת שאם F שדה; $g\in F[X]$ פולינום אי-פריק
אז אם $F\subseteq L$ שדה בו קיים שורש α ל- g; $L=F(\alpha)$
אז $F(\alpha)\cong F[X]/(g)$ והאיזומורפיזם משאיר את F במקום.
סקיצה של ההוכחה: מגדירים הומומורפיזם $F[X]\to F(\alpha)$

$$F\ni a\longmapsto a$$
$$x\longmapsto\alpha$$
$$h\longmapsto h(\alpha)$$

מוכיחים: • $\ker\varphi=(g)$:

(⊇) $h(\alpha)=p(\alpha)g(\alpha)=0 \Leftarrow h=pg \Leftarrow g(\alpha)=0$

(⊆) $h(\alpha)=0 \Leftarrow h\in\ker\varphi$. נחלק h ב-g עם שארית
$h=qg+r$ אם $r\neq 0$ אז $r\in F[X]$; $\deg r<\deg g$
וקיים $r(\alpha)=0$. נתבונן ב $s=\gcd(r,g)$.
זה פולינום המקיים $s|g$, $s|r$; $\deg s\leq\deg r<\deg g$
ו- $s(\alpha)=q_1(\alpha)r(\alpha)+q_2(\alpha)g(\alpha)=0 \Leftarrow s=q_1r+q_2g$
$\deg s\geq 1 \Leftarrow$ וזו סתירה לאי-פריקות של g

• ההעתקה היא על: $\varphi(F[X])=\bar{\varphi}(F[X]/(g))$
כאשר $\bar{\varphi}:F[X]/(g)\to F[X]$ מושרית מ- φ. $F[X]/(g)$
שדה לכן $\bar{\varphi}(F[X]/(g))$ שדה. $\bar{\varphi}|_F=id|_F$;
$\bar{\varphi}(\bar{x})=\alpha$ לכן תמונת $\bar{\varphi}$ היא תת שדה של $F(\alpha)$ המכיל
את F ואת α לכן תמונת φ היא תמונת $\bar{\varphi}$
היא $F(\alpha)$.

משפט: F שדה. $f\in F[X]$ פולינום מתוקן ממעלה ≥ 1 $F\subseteq E$ שדה פיצול
מינימלי עבור f; $F\subseteq E'$ שדה פיצול מינימלי עבור F. אז
קיים F- איזומורפיזם $\psi:E\to E'$.

הוכחה: נוכיח את הטענה באינדוקציה על מעלת הפולינום f.
יהי f פולינום (מתוקן) ממעלה $1 \leq d$. אם $d=1$ אזי $F=E=E'$
והטענה ברורה.

נניח באינדוקציה שאם L שדה ו- $h \in L[X]$ פולינום ממעלה $< d$
אז אם $L \subseteq E$ ו- $L \subseteq E'$ שדות פיצול מינימליים של h אזי
קיים L-איזומורפיזם $E \to E'$. (הנחת האינדוקציה היא לכל שדה
L ולא רק לשדה F שהתחלנו איתו).

נפרק את f לגורמים אי-פריקים ב- $F[X]$ $f=f_1 f_2 \dots f_m$
(הנחה) לגבי E פירושה $f=\prod_{i=1}^{d}(x-\alpha_i)$ ב- $E[X]$ ו-
$E=F(\alpha_1, \dots, \alpha_d)$. באותו אופן $f=\prod_{j=1}^{d}(x-\beta_j)$ ב- $E'[X]$
ו- $E'=F(\beta_1, \dots, \beta_d)$

נטען שקיים α_i כלשהו $1 \leq i \leq d$ כך ש- $f_1(\alpha_i)=0$. בה"כ $f_1(\alpha_1)=0$.
הרי $0=f(\alpha_1)=f_1(\alpha_1)\dots f_d(\alpha_1)$ $\Leftarrow$ $f_{i_0}(\alpha_1)=0$ לאיזה
i_0 $\Leftarrow$ $f_{i_0}=(x-\alpha_1)\tilde{f}_{i_0}$ $\Leftarrow$ $f=f_1 f_2 \dots \tilde{f}_{i_0}(x-\alpha_1) f_{i_0+1} \dots f_m$
נחלק ב- $x-\alpha_1$ ונקבל $\prod_{i=2}^{d}(x-\alpha_i)=f_1 f_2 \dots \tilde{f}_{i_0} \dots f_m$. נמשיך תהליך זה
שוב ושוב ונקבל חלוקה $\{1, \dots, d\}=R_1 \cup \dots \cup R_m$ כך ש-
$f_j=\prod_{i \in R_j}(x-\alpha_i)$

באותו אופן ולאחר שינוי שמות של β $f_1(\beta_1)=0$.
$F \subseteq F(\alpha_1) \subset E$, $F \subseteq F(\beta_1) \subseteq E'$. לפי הלמה שהוכחנו
קיים F-איזומורפיזם $\varphi_1 : F(\alpha_1) \to F(\beta_1)$

נעדן קצת את הנחת האינדוקציה. יהיו L ו- L' שדות הרחבה של
F. $F \subseteq L$ ו- $F \subseteq L'$ כך ש- L, L' הם F-איזומורפיים ע"
$\psi : L \to L'$. יהי $h \in L[X]$ פולינום ממעלה $< d$. ψ
משרה F-איזומורפיזם $\psi : L[X] \to L'[X]$ ונסמן $h'=\psi(h)$
יהי $L \subseteq E$ שדה פיצול מינימלי של h, $L' \subseteq E'$ שדה פיצול
מינימלי של h'. אזי קיים F-איזומורפיזם $\varphi : E \to E'$.
(תרגיל: לבדוק ש $d=1$ מקיימת הדרוש.

עכשיו נסמן $L=F(\alpha_1)$, $L'=F(\beta_1)$. נשים לב שב- $L[X]$ קיים $f(x)=(x-\alpha_1)h(x)$ וגם בדקנו ש
$f(x)=(x-\beta_1)h'$ ב- $L'[X]$ לכן מהנחת האינדוקציה נובע ש- E ו- E' הם F-איזומורפיים.

⑧ 20.05.2008
מבנים

משפט 8 יהיו L, L' שדות; $\sigma: L \to L'$ איזומורפיזם.
יהי $f \in L[X]$ ונסמן $f' = \sigma(f)$ (σ משרה הומומורפיזם $\sigma: L[X] \to L'[X]$).
יהיו $L \subseteq E$ שדה פיצול מינימלי עבור f; ו- $L' \subseteq E'$ שדה פיצול מינימלי עבור f'. אזי קיים איזומורפיזם $\varphi: E \to E'$ כך ש- $\varphi|_L = \sigma$.

הוכחה: נוכיח באינדוקציה על דרגת f. עבור f מדרגה 1 מתקיים $L = E$ ו- $L' = E'$ וניקח $\varphi = \sigma$.
נניח שהטענה מתקיימת עבור פולינום ממעלה קטנה ממעלת f.
נפרק את f למכפלת פולינומים אי-פריקים ב- $L[X]$ $f = f_1 f_2 \dots f_m$. יהי $\alpha_1 \in E$ שורש של f_1.
נתבונן ב- $f_1' = \sigma(f_1) \in L'[X]$ ויהי $\beta_1 \in E'$ שורש של f_1'. קיים איזומורפיזם $\Psi: L(\alpha_1) \to L'(\beta_1)$ כאשר $\Psi|_L = \sigma$.
כעת נסמן $M = L(\alpha_1)$, $M' = L'(\beta_1)$. יהיו $g \in M[X]$ $g' \in M'[X]$ כך ש- $f = (x-\alpha_1)g$, $f' = (x-\beta_1)g'$.
נשים ♡ שמתקיים $g' = \Psi(g)$. ואז כן, $M \subseteq E$ הוא שדה פיצול מינימלי עבור g; ו- $M' \subseteq E'$ הוא שדה פיצול מינימלי עבור g'. וכמובן- $\deg g = \deg f - 1 < \deg f$. לכן, לפי הנחת האינדוקציה קיים איזומורפיזם $\varphi: E \to E'$ כך ש- $\varphi|_M = \Psi$
אבל $L \subseteq M$ ולכן $\varphi|_L = (\varphi|_M)|_L = \Psi|_L = \sigma$.
☺

הסברים והערות: E שדה פיצול מינימלי עבור f פירושו
ב- $E[X]$ מתקיים $f(x) = \prod_{i=1}^{d}(x-\alpha_i)$ כאשר $d = \deg f$
; $E = L(\alpha_1, \dots, \alpha_d)$ שדה מינימלי ביחס להכלה שמקיים ״
כעת נתבונן בפולינום $g \in M[X] \subseteq E[X]$ המוגדר ע״
$g = (X-\alpha_2)(X-\alpha_3)\dots(X-\alpha_d)$ אז $f = (X-\alpha_1)g$ וכן
$E = L(\alpha_1)(\alpha_2, \dots, \alpha_d) = M(\alpha_2, \dots, \alpha_d)$.

נניח ש- $F \subseteq E$ שדות (לפעמים כותבים E/F). אז אפשר לחשוב על E כמרחב וקטורי מעל F. הרחבת שדות $F \subseteq E$ תיקרא <u>הרחבה סופית</u> אם E מרחב וקטורי ממימד סופי מעל F.
נסמן $[E:F] = \dim_F E$.

<u>משפט</u>: נניח שנתונים שדות $F \subseteq L \subseteq E$ וההרחבות סופיות.
אזי $[E:F] = [E:L][L:F]$

<u>הוכחה</u>: יהי $\alpha_1, \dots, \alpha_n$ בסיס ל- E מעל L ויהי $\beta_1, \dots, \beta_m$ בסיס ל- L מעל F.
נטען שהאוסף $\Omega = \{\alpha_i \beta_j\}_{i,j}$ בסיס ל- E מעל F וזה כמובן מוכיח את המשפט.

נראה ש- $\text{span}_F \Omega = E$ וש- Ω בת"ל מעל F.
יהי $\varepsilon \in E$. קיימים $\lambda_1, \dots, \lambda_n \in L$ כך ש- $\varepsilon = \sum_{i=1}^n \lambda_i \alpha_i$ (כי $\{\alpha_i\}$ בסיס מעל L). אבל $\{\beta_j\}$ בסיס של L מעל F) לכן לכל $1 \le i \le n$ קיימים $a_{ij} \in F$ $1 \le j \le m$ כך ש- $\lambda_i = \sum_{j=1}^m a_{ij} \beta_j$.

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

$\Leftarrow$ Ω פורשת את E מעל F.

נותר להראות אי תלות. נניח שקיימת תלות

$$\sum_{i=1}^n \sum_{j=1}^m b_{ij} \alpha_i \beta_j = 0 \qquad b_{ij} \in F$$

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

אבל $\sum_{j=1}^m b_{ij} \beta_j \in L$! $\{\alpha_i\}$ בסיס לכן לכל j $\sum b_{ij} \beta_j = 0$. אבל $\{\beta_j\}$ בסיס. $\Leftarrow$ $b_{ij} = 0$.

ההוכחה של המשפט טריוויאלית אבל היא ממש חשובה ונובעים ממנו דברים מופלאים.

דוגמה: ברור ש- $\sqrt{2}$ ו- $\sqrt[9]{3}$ הם שורשים של פולינומים.
אבל מה לגבי $\sqrt{2}-\sqrt[9]{3}$? עבודה מייגעת ורגילה להביא
אותו לפולינום שזה השורש שלו, אבל זה נובע מהמשפט שלנו
באופן מיידי.

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

משפט: הרחבה $F\subseteq E$ היא הרחבה סופית אמ"מ ההרחבה אלגברית ו- $F\subseteq E$ נוצרת סופית (כלומר $E=F(\alpha_1,\dots,\alpha_k)$ ו- $k\in\mathbb{N}$ ו- $\alpha_1,\dots,\alpha_k\in E$).

הוכחה: נניח ש- $F\subseteq E$ הרחבה סופית. יהי $\alpha\in E$.
נתבונן ב- $1,\alpha,\alpha^2,\alpha^3,\dots,\alpha^n$ כאשר $n=[E:F]$
אלה $n+1$ וקטורים במרחב וקטורי E n-ממדי מעל F.
⇐ קיימת תלות לינארית לא טריוויאלית:

$$a_0+a_1\alpha+\dots+a_n\alpha^n=0$$

⇐ α שורש של הפולינום $a_nX^n+\dots+a_1X+a_0\in F[X]$.
⇐ ההרחבה אלגברית. נראה שהיא נוצרת סופית. אם
$n=[E:F]<\infty$ אז נבחר בסיס $\beta_1,\dots,\beta_n$ עבור
E מעל F ומתקיים $E=F(\beta_1,\dots,\beta_n)$. (האמת היא שאפשר
להסתפק גם בתוספת קטנה יותר - $\log n$ איברים).
נניח כעת שההרחבה אלגברית ונוצרת סופית, כלומר
$E=F(\alpha_1,\dots,\alpha_k)$ ו- $\alpha_i\in E$. צריך להראות ש- $[E:F]<\infty$
מתקיים $F\subseteq F(\alpha_1)\subseteq\dots\subseteq F(\alpha_1,\dots,\alpha_k)=E$
⇐ $[E:F]=\prod_{i=0}^{n-1}[F(\alpha_1,\dots,\alpha_{i+1}):F(\alpha_1,\dots,\alpha_i)]$. לכן מספיק להראות שאם
$L\subseteq K$ הרחבת שדות ו- $\alpha\in K$ אלגברי מעל L אזי
$[L(\alpha):L]<\infty$. המשך בשבוע הבא...

⑩ 26.05.08

מבנים

משפט: הרחבת שדות $F \subseteq E$ היא סופית אמ"מ היא אלגברית (כלומר כל איבר ב-E אלגברי מעל F) ונוצרת סופית (כלומר $E = F(\alpha_1, \dots, \alpha_k)$)

הוכחה:

הראנו שאם $n=[F:F] < \infty$ אזי היא אלגברית ונוצרת סופית. זה היה פשוט. בהינתן $\alpha \in E$ הסתכלנו ב- $1, \alpha, \alpha^2, \dots, \alpha^n$. אלה $n+1$ וקטורים תלויים לינארית מעל F. $\Leftarrow$ קיימים $a_0, \dots, a_n \in F$ לא כולם 0 כך ש- $p(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = 0$. אז α שורש של $0 \neq p(x) = \sum_{i=0}^{n} a_i x^i \in F[X]$. רצי להוכיח שהיא נוצר סופי זה גם פשוט:

אם $E = F$ סיימנו. אחרת, נבחר איזה $\alpha_1 \in E \setminus F$. נסמן $E_1 = F(\alpha_1)$. אם $E_1 = E$ סיימנו. אחרת, נבחר $\alpha_2 \in E \setminus E_1$ ונסמן $E_2 = E_1(\alpha_2) = F(\alpha_1, \alpha_2)$ וכן הלאה. היות ש- $E \subsetneq E_1 \subsetneq E_2 \subsetneq \dots \subsetneq E$ מקבלים סדרה עולה ממש (!) של תתי מרחבים לינאריים מעל F במרחב וקטורי ממימד סופי. סדרה כזו חייבת להיות סופית.

נוכיח את הכיוון השני. נראה שאם $L \subseteq E$ שדה ו- $\alpha \in E$ אלגברי מעל L אזי $[L(\alpha) : L] < \infty$. ברור שזה מספיק כי נתון $E = F(\alpha_1, \dots, \alpha_k)$ ולכן נקבל $\infty > d_{i+1} = [F(\alpha_1, \dots, \alpha_{i+1}) : F(\alpha_1, \dots, \alpha_i)]$ ואז $[E:F] = \prod_{i=0}^{n-1} d_i < \infty$

למה: אם α אלגברי מעל L אזי $L(\alpha) = L[\alpha]$

$$\left\{ \frac{f(\alpha)}{g(\alpha)} : f,g \in L[X], g(\alpha) \neq 0 \right\} = \left\{ \sum_{i=0}^{n} a_i \alpha^i ; n \in \mathbb{N} \cup \{0\}, a_i \in L \right\}$$

בנוסף $L[\alpha] = \{ \sum_{i=0}^{m-1} a_i \alpha^i : a_i \in L \}$ כאשר $m = \deg f$ עבור $0 \neq f \in L[X]$ מתוקן כך ש- $f(\alpha) = 0$. (m הזה הוא לא יחיד, אבל נוח להיות שיש ראשון מלמטה).

הוכחה: די להראות ש- $M = \{ \sum_{i=0}^{m-1} a_i \alpha^i : a_i \in L \}$ הוא שדה. ברור ש- $L \cup \{\alpha\} \subseteq M \subseteq L(\alpha)$ ולכן אם M שדה מהגדרה מתקיים שוויון (מהמינימליות של $L(\alpha)$). [נשים ♡ ש- $\dim_L M \le m$ ממימד סופי ולכן מוכיח את המשפט].

כדי להראות ש- $\emptyset \neq M \subseteq E$ הוא תת שדה צריך להראות

סגירות לחיבור, כפל וקיום נגדי והופכי.

ברור מיד מההגדרה ש- M סגורה לחיבור:

$$\sum_{i=0}^{m-1} a_i \alpha^i + \sum_{i=0}^{m-1} c_i \alpha^i = \sum_{i=0}^{m-1} (a_i + c_i) \alpha^i \in M$$

ברורה גם סגירות לנגדי $-\sum_{i=0}^{m-1} a_i \alpha^i = \sum_{i=0}^{m-1} (-a_i) \alpha^i \in M$

נראה גם סגירות לכפל: $\sum_{i=0}^{m-1} a_i \alpha^i , \sum_{j=0}^{m-1} c_j \alpha^j \in M$ $\quad a_i, c_j \in L$

$$\left(\sum_{i=0}^{m-1} a_i \alpha^i\right)\left(\sum_{j=0}^{m-1} c_j \alpha^j\right) = \sum_{k=0}^{2m-2} \left(\sum_{i+j=k} a_i c_j\right) \alpha^k$$

נשים לב ש- $\alpha^m = \sum_{i=0}^{m-1} (-b_i) \alpha^i$ כאשר b_i המקדמים של

$f = x^m + \sum_{i=0}^{m-1} b_i x^i$ הפולינום שעבורו $f(\alpha) = 0$.

$$\Rightarrow \alpha^{m+1} = \alpha \cdot \alpha^m = \alpha\left(\sum_{i=0}^{m-1} (-b_i) \alpha^i\right) =$$

$$= -b_{m-1} \alpha^m + \left(\sum_{i=0}^{m-1} ? \alpha^i\right) =$$

$$= (-b_{m-1})\left(\sum_{i=0}^{m-1} (-b_i) \alpha^i\right) + \left(\sum_{i=0}^{m-1} ? \alpha^i\right) \in M$$

מראים באופן כזה שכל α^t $t \in \mathbb{N}$ הוא איבר ב- M ולכן גם

המכפלה ב- M.

בינתיים הראנו ש- $L \subseteq M \subseteq E$ תת מרחב ממימד סופי מעל L

סגור לכפל. נותר שנוכיח מכך שלכל $0 \neq \beta \in M$ קיים הופכי

ב- M. יהי $0 \neq \beta \in M$ ונגדיר $T : M \to M$ כפל ב- β.
$\quad u \mapsto \beta u$

T אכן העתקה מ- M ל- M כי M סגור לכפל; $\beta \in M$.

צריך להראות ש- $1 \in \operatorname{Im} T$. מספיק להראות שהיא על. אבל T

כמובן לינארית והיא גם חח"ע (כאשר ש- $M \subseteq E$; E שדה

אם $\beta u = 0$ מההכרח $u = 0$). $\Leftarrow$ (נובע ממשפט המימדים

(לינארית 1) ש- T היא על. לכן קיים $\gamma \in M$ כך ש- $\gamma\beta = \beta\gamma = 1$.

☺

<u>הגדרה</u>: הרחבה E/F תיקרא סגורה אלגברית אם מתקיים:

① E/F אלגברית

② אם E'/E הרחבה אלגברית אז $E' = E$.

(11)

משפט: הטענות הבאות שקולות עבור שדה Ω

① כל פולינום ממעלה ≥ 1 ב- $\Omega[X]$ מתפצל ב-$\Omega[X]$.

② לכל פולינום $f \in \Omega[X]$ ממעלה ≥ 1 יש שורש ב- Ω.

③ פולינום אי- פריק ב- $\Omega[X]$ הוא ממעלה 1

④ כל הרחבה סופית של Ω היא Ω.

הגדרה: Ω כמו במשפט נקרא שדה סגור אלגברית.

טענה: יהי F שדה ו- $L \subseteq E$ שדה הרחבה. אם $\alpha,\beta \in E$ אלגבריים מעל F אזי $\alpha+\beta,\ \alpha\cdot\beta \in F$ $-\alpha,\ \alpha^{-1}$ אלגבריים מעל F.

הוכחה: ממה שהוכחנו קודם $[F(\alpha,\beta):F]<\infty$. לכן $\alpha+\beta,\ \alpha\beta \in F(\alpha,\beta)$ אלגבריים מעל F. וזהו זה. ☺

נניח שנתון F שדה ושדה $F \subseteq E$ רק ש- E שדה סגור אלגברית.
נגדיר $M=\{\alpha \in E:\ \alpha \text{ אלגברי מעל } F\}$

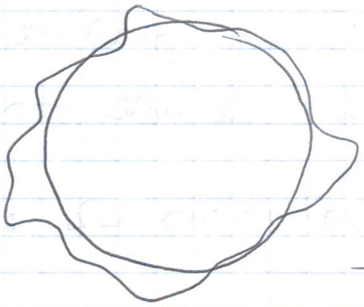
טענה: M שדה סגור אלגברית.

הוכחה: מהטענה הקודמת ברור ש- M שדה. נראה שהוא סגור אלגברית. נניח ש- $f \in M[X]$ פולינום ממעלה ≥ 1. צריך להראות של- f יש שורש ב- M. מההנחה, היות ש- $M[X] \subseteq E[X]$ ו- E סגור אלגברית נובע שיש ל- f שורש α ב- E. צריך להראות ש-α אלגברי מעל F. נסמן $f(x)=\sum_{i=0}^{n} a_i x^i$ כאשר $a_i \in M$. נסמן $L=F(a_1,\dots,a_n)$. $\{a_i\}$ אלגבריים מעל F, L/F הרחבה סופית, כלומר $[L:F]<\infty$ ו- $[L(\alpha):L]<\infty$ $\Leftarrow$ $[L(\alpha):F]<\infty$ $\Leftarrow$ α אלגברי מעל F לכן $\alpha \in M$. ☺

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

רעיונות לדרך הוכחה ש- $\mathbb{C}$ סגור אלגברית: נתון $f(z)=z^n+\dots+a_0$ עבור $n \geq 1$. נסתכל על הפולינום כהעתקה מ- $\mathbb{C}$ ל- $\mathbb{C}$. צריך להראות ש- 0 בתמונה של f.

נתבונן במעגל גדול סביב הראשית ברדיוס R. אם $f(z) = z^n$ אז תמונת המעגל היא מעגל ברדיוס R^n שמלופף סביב עצמו n פעמים. אם R ממש גדול אז האיברים האחרים של הפולינום זניחים ואז התמונה היא בערך מעגל



הפונקציה f רציפה והאינטואיציה אומרת שתמונת העיגול המלא איכשהו מכסה את כל הפנים של המסילה הזאת ולא מפספס דבר - בפרט לא את 0.

הוכחה פורמלית בפונקציות מרוכבות או בטופולוגיה אלגברית.

<u>דוגמה</u>: $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \mathbb{Q}$ אלגברי מעל $\alpha\}$. $\bar{\mathbb{Q}}$ היא שדה המספרים האלגבריים. (שדה סגור אלגברית לפי המשפט)

נשים לב ש-$\mathbb{Q}(i)$ לא סגור אלגברית כי $\sqrt{2} \notin \mathbb{Q}(i)$ ולכן לפולינום $x^2 - 2$ אין שורש.

אפשר לבנות את $\bar{\mathbb{Q}}$ באופן אינדוקטיבי. $\mathbb{Q}[X]$ היא בת-מניה.

תהי $f_1, f_2, \ldots \in \mathbb{Q}[X]$ סדרה של כל הפולינומים מדרגה ≥ 1.

נגדיר $F_0 = \mathbb{Q}$. $F_0 \subseteq F_1$ שדה הפיצול עבור f_1,

$F_1 \subseteq F_2$ שדה הפיצול עבור f_2

וכן הלאה.

מקבלים סדרה עולה של שדות $\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq \ldots$

נגדיר $E = \bigcup_{i=0}^{\infty} F_i$. קל לראות שזה שדה (ממש, אם $\alpha, \beta \in E$ יש i_0 כך ש- $\alpha, \beta \in F_{i_0} \Rightarrow \alpha + \beta \in F_{i_0} \Rightarrow \alpha + \beta \in E$).

קל לבדוק ש-E אלגברי מעל $\mathbb{Q}$ כי כל הרחבה F_n היא סופית מעל $\mathbb{Q}$ ולכן אם $\alpha \in E$ אז $\alpha \in F_{i_0}$ ולכן אלגברי מעל $\mathbb{Q}$. E סגור אלגברית. אם $g \in E[x]$, ו-$\deg g \geq 1$ אז $b_i \in E$ $g = \sum b_i x^i$. קיימים $k_i \in \mathbb{N}$ כך ש- $b_i \in F_{k_i}$ לכן קיים $k = \max\{k_i\}$ כך ש- $b_i \in F_k$ לכל i.

נתבונן בהרחבה סופית M של F_k בה יש ל-g שורש β.

β היא אלגברי מעל $\mathbb{Q}$. כלומר קיים פולינום $h \in \mathbb{Q}[X]$ ממעלה ≥ 1

כך ש- $h(\beta)=0$. קיים $s\in\mathbb{N}$ כך ש- $h=f_s$
(כי $\{f_i\}$ זו מנייה של כל הפולינומים מעל $\mathbb{Q}$) ולכן
בשדה F_t כאשר $t=\max\{k,s\}$ יש שורש לפולינום
h וגם לפולינום g.

אפשר לעשות דברים דומים גם לשדות לא בני מנייה ואז צריך
להשתמש באינדוקציה טרנס-פיניטית...

$\bar{\mathbb{Q}}$ הוא בן מנייה. $\Leftarrow$ $\bar{\mathbb{Q}}\neq\mathbb{C}$ $\Leftarrow$ יש מספרים שהם
לא אלגבריים. למשל $\beta=\sum_{n=0}^{\infty}\frac{1}{10^{10^n}}$

<u>תרגיל</u>: יהי $\alpha\in\bar{\mathbb{Q}}$ אי-רציונלי. אזי קיים $n\in\mathbb{N}$ ו- $0<c$
כך שלכל $\mathbb{N}\ni p,q\neq 0$ $|\alpha-\frac{p}{q}|>\frac{c}{q^n}$.

<u>מסקנה</u>: ברור ש- β לא מקיים תכונה זו ולכן אינו אלגברי.

⑬ 27.05.08

מבנים

<u>תרגיל</u>: יהי $\alpha \in \bar{\mathbb{Q}} \setminus \mathbb{Q}$. אזי קיימים $n \in \mathbb{N}$ ו- $0 < c$ כך שלכל $p, q \in \mathbb{N}$ $|\alpha - \frac{p}{q}| > \frac{c}{q^n}$

<u>הוכחה</u>: $\alpha \in \bar{\mathbb{Q}}$ אמ"מ קיים פולינום $f \in \mathbb{Q}[X]$ כך ש- $f(\alpha) = 0$. ולמעשה אפשר להניח ש- $f \in \mathbb{Z}[X]$ (ע"י מכפלה במכנה המשותף). נסמן $f(x) = \sum_{i=0}^{n} a_i x^i$. אז

$$f(\tfrac{p}{q}) = \sum_{i=0}^{n} a_i (\tfrac{p}{q})^i$$

$$\Rightarrow q^n f(\tfrac{p}{q}) = \sum_{i=0}^{n} a_i p^i q^{n-i}$$

יש סביבה של α שבה α השורש היחידי של הפולינום.
אם $\frac{p}{q}$ מספיק קרוב ל- α אז $q^n f(\frac{p}{q}) \neq 0$ שהרי $\mathbb{Q} \not\ni \alpha \neq \frac{p}{q}$. חוץ מזה, $q^n f(\frac{p}{q}) \in \mathbb{Z}$ שהרי $a_i \in \mathbb{Z}$.

$$|f(\alpha) - f(\tfrac{p}{q})| = |f(\tfrac{p}{q})| \geq \frac{1}{q^n} \Leftarrow |q^n f(\tfrac{p}{q})| \geq 1 \Leftarrow$$

לפי משפט שהוא מהסוף של אינפי 1 יש c כך ש-

$$\left| \frac{f(\frac{p}{q})}{\alpha - \frac{p}{q}} \right| = \left| \frac{f(\alpha) - f(\frac{p}{q})}{\alpha - \frac{p}{q}} \right| = |f'(c)| \underset{\downarrow}{<} M$$

$$M > \max_{x \in [\alpha-1, \alpha+1]} |f'(x)| < \infty$$

$$\Rightarrow |f(\tfrac{p}{q})| \leq M |\alpha - \tfrac{p}{q}|$$

$$\Rightarrow \frac{1}{q^n} \leq M |\alpha - \tfrac{p}{q}|$$

אם ניקח $c = \frac{1}{M}$ ונקבל $|\alpha - \frac{p}{q}| < \frac{c}{q^n}$.

<u>משפט</u>: Ω שדה. אז התנאים הבאים שקולים:

① כל פולינום מדרגה ≥ 1 ב- $\Omega[X]$ מתפצל ב- $\Omega[X]$
② לכל פולינום מדרגה ≥ 1 ב- $\Omega[X]$ יש שורש ב- Ω.
③ פולינום אי-פריק ב- $\Omega[X]$ הוא בהכרח מדרגה 1.
④ כל הרחבה סופית של Ω היא Ω.

הוכחה:

($1 \Rightarrow 2$) ברור. מתפצל פירושו מתפרק לגורמים לינאריים וכל גורם כזה נותן שורש.

($2 \Rightarrow 3$) ברור כי אם הדרגה גדולה מ-1 אז יש לו שורש ולכן פריק.

($3 \Rightarrow 1$) ברור מההגדרה.

($3 \Rightarrow 4$) תהי $\Omega \subseteq E$ הרחבה סופית. יהי $\alpha \in E$. אזי α אלגברי מעל Ω [מתקיים פולינום לא פריק $0 \neq f \in \Omega[X]$ כך ש- $f(\alpha)=0$. $\alpha \in E$] אלגברי. $\Rightarrow$ קיים $0 \neq g \in \Omega[X]$ כך ש- $g(\alpha)=0$. נפרק את g למכפלת פולינומים אי-פריקים $g=f_1 \cdots f_k$!.
$0=g(\alpha)=\prod f_i(\alpha) \Rightarrow f_j(\alpha)=0$ לאיזה k. לכן קיים פולינום אי-פריק f ר"ל}.
לפי ההנחה ב-(3) נובע שהפולינום f מדרגה 1 ולכן $\alpha \in \Omega \Rightarrow \Omega = E$.

($4 \Rightarrow 3$) יהי $f \in \Omega[X]$ פולינום אי-פריק. אזי $\Omega[X]/(f)$ שדה הרחבה של Ω ומתקיים $[\Omega[X]/(f) : \Omega] = \deg f$. לכ ההרחבה סופית ומההנחה $\Omega = \Omega[X]/(f) \Rightarrow$
$\deg f = 1$ ☺

הגדרה: הרחבה מהצורה $F \subseteq F(\alpha)$ נקראת הרחבה פשוטה.

נשאלת השאלה מהם ה-F-איזומורפיזמים מ-$F(\alpha)$ ל-$F(\alpha)$?

משפט: תהי $F(\alpha)$ הרחבה פשוטה, ותהי $F \subseteq \Omega$ הרחבה כלשהי.

① אם α לא אלגברי מעל F אזי עבור כל F-הומומורפיזם $\varphi : F(\alpha) \to \Omega$ מתקיים ש- $\varphi(\alpha) \in \Omega$ לא אלגברי.
בפרט, יש התאמה חח"ע ועל

$$\left\{ \begin{matrix} F\text{-הומומורפיזמים} \\ \varphi : F(\alpha) \to \Omega \end{matrix} \right\} \longleftrightarrow \left\{ \beta \in \Omega : \begin{matrix} \beta \text{ לא} \\ F \text{ אלגבריים} \end{matrix} \right\}$$

ב) אם α אלגברי מעל F אזי עבור כל F-הומומורפיזם $\varphi: F(\alpha)\to\Omega$, $\varphi(\alpha)$ הוא אלגברי והוא שורש של הפולינום המינימלי f של α. בפרט, יש התאמה חח"ע ועל

$$\left\{\begin{matrix}\text{שורשי הפולינום}\\ \text{המינימלי של } \alpha\\ \text{ב-}\Omega\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}F\text{-הומומורפיזמים}\\ \varphi: F(\alpha)\to\Omega\end{matrix}\right\}$$

הגדרה: יהי $F\subseteq E$ הרחבת שדות. ו-$\alpha\in E$ אלגברי. הפולינום המינימלי של α הוא הפולינום המתוקן מדרגה מינימלית $f\in F[X]$ כך ש- $f(\alpha)=0$.

הערה: צריך להוכיח שיש כזה. ושהוא יחיד.

יהי $\alpha\in E$ אלגברי מעל F. יהי $f\in F[X]$ פולינום מתוקן ממעלה מינימלית כך ש- $f(\alpha)=0$.

טענה: אם $g\in F[X]$, $g(\alpha)=0$ אז $f\mid g$.

מסקנה: הפולינום המינימלי הוא יחיד.

הוכחת הטענה: חלוקה עם שארית: אם $f\nmid g$ אז יש $r\in F[X]$ עם $\deg r<\deg f$ כך ש-

$$g=qf+r$$

$$0=g(\alpha)=q(\alpha)f(\alpha)+r(\alpha)=r(\alpha)$$

וזו סתירה למינימליות הדרגה של f.

הוכחת המשפט:

תזכורת: הומומורפיזם של שדות הוא מהגדרה חח"ע (חלק מהדרישה היא ש- $0\mapsto0$, $1\mapsto1$ ואז זה ברור).

א) נניח ש- $\varphi: F(\alpha)\to\Omega$ F-הומומורפיזם. נסמן $\beta=\varphi(\alpha)$ ב-Ω. יהי $f\in F[X]=\sum_{i=0}^{n} a_i x^i$. אז מתקיים $\varphi(f(\alpha))=f(\beta)$

שהרי

$$\varphi\left(\sum_{i=0}^{n} a_i\alpha^i\right)=\sum_{i=0}^{n}\varphi(a_i)\varphi(\alpha)^i=\sum_{i=0}^{n}\varphi(a_i)\beta^i=\sum_{i=0}^{n}a_i\beta^i=f(\beta)$$

$\leftarrow$ φ הוא F-הומומורפיזם

קיבלנו שאם $0 \neq f \in F[x]$ אז $f(\alpha) \neq 0$ כי α אינו אלגברי ולכן היות ש-φ חח"ע נובע ש-

$$0 \neq \varphi(f(\alpha)) = f(\beta)$$

ולכן גם β אינו אלגברי מעל F.

כמו כן, נשים לב ש-

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in F[x],\ g(\alpha) \neq 0 \right\}$$

לכן F-הומומורפיזם φ נקבע באופן יחיד ע"י $\varphi(\alpha) = \beta$

לכן ההעתקה

$$\left\{ \varphi : \varphi \text{ הומו'-}F \text{ מ-}F(\alpha) \text{ ל-}K \right\} \longrightarrow \left\{ \text{איברים טרנס' } K \right\}$$

$$\varphi \longmapsto \varphi(\alpha)$$

זו העתקה חח"ע. נותר להראות שהיא על. לכל $\beta \in K$ טרנס' נגדיר $\varphi\left(\frac{f(\alpha)}{g(\alpha)}\right) = \frac{f(\beta)}{g(\beta)}$. אז מקבלים F-הומומורפיזם מ-$F(\alpha)$ ל-K.

<u>תרגיל</u>: בדקו שאכן φ מוגדרת היטב והיא F-הומומורפיזם.

⑮ 3.6.08
מבנים

<u>משפט</u>: F שדה ; $F \subseteq F(\alpha)$; $F \subseteq \Omega$. נסמן

$\mathcal{L} = \{\varphi : F(\alpha) \to \Omega$; φ F-הומומורפיזם$\}$

① אם α טרנסצנדנטי מעל F אזי קיימת התאמה חח"ע ועל בין $\mathcal{L}$ לבין $\{\beta \in \Omega :$ β טרנס' מעל $F\}$ הניתנת ע"י $\varphi \longmapsto \varphi(\alpha) \in \Omega$.

② אם α אלגברי מעל F ; $f \in F[X]$ פולינום מינימלי של α אז קיימת התאמה חח"ע ועל בין $\mathcal{L}$ לבין $\{\beta \in \Omega :$ β שורש של $f\}$ הניתנת ע"י $\varphi \longmapsto \varphi(\alpha)$.

<u>הוכחה</u>:

① נזכור שהומומורפיזם של שדות הוא חח"ע. לכן, אם α טרנס' מעל F ונניח ש- $\varphi : F(\alpha) \to \Omega$ F-הומומורפיזם אזי תמונת α תחת φ $\beta = \varphi(\alpha)$ הינו טרנס' מעל F כי אם $0 \neq g \in F[X]$; $g(\beta) = 0$ אז

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

אבל היות ש-φ חח"ע נובע ש- $g(\alpha) = 0$ וזו סתירה להנחה ש-α טרנס' מעל F.

נותר להראות (במקרה א) שההתאמה המתאימה ל-φ את $\varphi(\alpha)$ היא אכן חח"ע ועל הקבוצה $\{\beta \in \Omega :$ β טרנס' מעל $F\}$

רק להראות חח"ע נשים לב שאם φ, ψ F-הומומורפיזמים מ-$F(\alpha)$ ל-Ω אזי היות שכל איבר $F(\alpha)$ הם מהצורה $\frac{g(\alpha)}{h(\alpha)}$ כאשר $g, h \in F[X]$ ו- $h(\alpha) \neq 0$ ונניח שכל איבר ב- $F(\alpha)$ צורתו הנ"ל $\gamma = \frac{g(\alpha)}{h(\alpha)}$ לכן אם $\beta = \varphi(\alpha) = \psi(\alpha)$

$$\varphi(\gamma) = \varphi\left(\frac{g(\alpha)}{h(\alpha)}\right) = \frac{\varphi(g(\alpha))}{\varphi(h(\alpha))} = \frac{g(\varphi(\alpha))}{h(\varphi(\alpha))} =$$

$$= \frac{g(\beta)}{h(\beta)} = \frac{g(\psi(\alpha))}{h(\psi(\alpha))} = \frac{\psi(g(\alpha))}{\psi(h(\alpha))} = \psi\left(\frac{g(\alpha)}{h(\alpha)}\right) = \psi(\gamma)$$

קיבלנו ש- φ ; ψ מסכימים על $F(\alpha)$ לכן הם שווים.

נותר להוכיח שההתאמה הינה על. נניח ש- $\beta \in \Omega$ טרנס' מעל

F. יהי $\gamma \in F(\alpha)$. אזי קיימים $g, h \in F[X]$ כך ש-

$h(\alpha) \neq 0$; $\gamma = \frac{g(\alpha)}{h(\alpha)}$ ונגדיר $\varphi(\gamma) = \frac{g(\beta)}{h(\beta)} \in \Omega$. נשים

לב ש- $h(\beta) \neq 0$ כי β טרנס' מעל F. צריך לוודא ש- φ

מוגדרת היטב. כלומר, אם $\frac{g(\alpha)}{h(\alpha)} = \frac{g_1(\alpha)}{h_1(\alpha)}$ כאשר $g, h, g_1, h_1 \in F[X]$;

$h(\alpha), h_1(\alpha) \neq 0$ אז גם $\frac{g(\beta)}{h(\beta)} = \frac{g_1(\beta)}{h_1(\beta)}$. אם נוכיח את זה יהיה

קל לראות שההעתקה שהגדרנו $\varphi : F(\alpha) \to \Omega$ היא אכן

F-הומומורפיזם.

אז נוכיח ש- φ מוגדרת היטב. נתון $\frac{g(\alpha)}{h(\alpha)} = \frac{g_1(\alpha)}{h_1(\alpha)}$

כאשר $h_1(\alpha), h(\alpha) \neq 0$. $\Leftarrow$ $h_1(\alpha)g(\alpha) = h(\alpha)g_1(\alpha)$

$$\Rightarrow p(\alpha) = h_1(\alpha)g(\alpha) - h(\alpha)g_1(\alpha) = 0$$

כאשר $p = h_1 g - h g_1$. היות ש- α טרנס' מעל F

נקבל ש- $p \equiv 0$, כלומר $h_1 g - h g_1 \equiv 0$, כלומר

$0 = h_1(\beta)g(\beta) - h(\beta)g_1(\beta)$ $\Leftarrow$ $\frac{g(\beta)}{h(\beta)} = \frac{g_1(\beta)}{h_1(\beta)}$ וההתאמה

היא על.

ⓑ α אלגברי ; $0 \neq f_0 \in F[X]$ פולינום מינימלי עבור α.

יהי $\varphi : F(\alpha) \to \Omega$ F-הומומורפיזם. היות ש- α אלגברי

$F(\alpha) = \{g(\alpha) : g \in F[X]\}$. נגדיר $\beta = \varphi(\alpha)$ ונשים לב ש-

$$f_0(\beta) = f_0(\varphi(\alpha)) = \varphi(f_0(\alpha)) = \varphi(0) = 0$$

$\Leftarrow$ β שורש ב- Ω של הפולינום המינימלי f_0 של α.

אז $\begin{array}{ccc} \mathcal{L} & \longrightarrow & \Omega \\ \varphi & \longmapsto & \varphi(\alpha) \end{array}$ היא למעשה $\mathcal{L} \longrightarrow \{\beta \in \Omega : f_0(\beta) = 0\}$

נותר להראות שהתאמה זו חח"ע ועל. חח"ע נובעת בקלות

מכך ש- $F(\alpha) = F[\alpha]$. נניח $\varphi, \psi \in \mathcal{L}$ ונניח ש-

$\varphi(\alpha) = \psi(\alpha) = \beta$. אזי לכל $\gamma \in F(\alpha)$ קיים $g \in F[X]$

כך ש- $\gamma = g(\alpha)$ ולכן $\varphi(\gamma) = \varphi(g(\alpha)) = g(\varphi(\alpha)) = g(\psi(\alpha)) = \psi(g(\alpha)) = \psi(\gamma)$

$\Leftarrow$ $\varphi = \psi$. נותר לוודא שההתאמה היא על. נניח $\beta \in \Omega$

; $f_0(\beta) = 0$. נגדיר עבור $\gamma \in F(\alpha)$ את $\varphi(\gamma)$ ע"י שנבחר

$g \in F[X]$ כך ש- $g(\alpha) = \gamma$ ונגדיר $\varphi(\gamma) = g(\beta)$.

נבדוק שזה מוגדר היטב. נניח $g, g_1 \in F[X]$ מקיימים

$g(\alpha) = \gamma = g_1(\alpha)$, אזי הפולינום $p = g - g_1$ מקיים

$p(\alpha)=g(\alpha)-g_1(\alpha)=0$ ולכן f מחלק את p ולכן
$g(\beta)-g_1(\beta)=p(\beta)=0$ ולכן $g(\beta)=g_1(\beta)$.

☺

משפט: יהי F שדה ; $F\subseteq E$ שדה הרחבה. $f\in F[X]$ פולינום המתפצל ב- $E[X]$ ונניח ש- E נוצרת מעל F ע"י שורשי הפולינום f. יהי $F\subseteq\Omega$ שדה כך ש- f מתפצל ב- Ω. אזי מספר ה- F-הומומורפיזמים $\varphi : E\to\Omega$ הוא לכל היותר $[E:F]$ ושוויון מתקיים אמ"מ ל- f יש $[E:F]$ שורשים שונים ב- Ω.

הוכחה: $E=F(\alpha_1,\dots,\alpha_d)$ כאשר $\alpha_1,\dots,\alpha_d$ שורשי הפולינום f. נפרק את f לגורמים אי-פריקים $f=f_1\cdots f_k$ מעל F. ונניח α_1 שורש של f_1. תמונת α_1 תחת F-הומומורפיזם היא מהכרח שורש של f_1. לכן מספר האפשרויות לבחירת תמונת α_1 הוא לכל היותר מספר שורשי f_1 ב- Ω, כלומר $\geq \deg f_1 = [F(\alpha_1):F]$
נתבונן כעת ב- $F(\alpha_1)\subseteq E$ ונחפש $F(\alpha_1)$ הומומורפיזמים ל- Ω. נמשיך באינדוקציה...

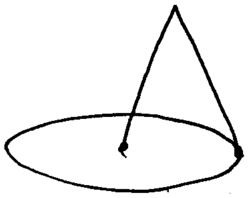
המשך שבוע הבא.

⑰ 10.6.08
מבנים

כחיק מחליף את שחר

בניות בעזרת מחוגה וסרגל

מחוגה זה משהו שאפשר לצייר איתו מעגלים



סרגל (לא מסומן) זה משהו שאפשר לצייר איתו ישרים
היוונים התעסקו בבניות האלה הרבה.

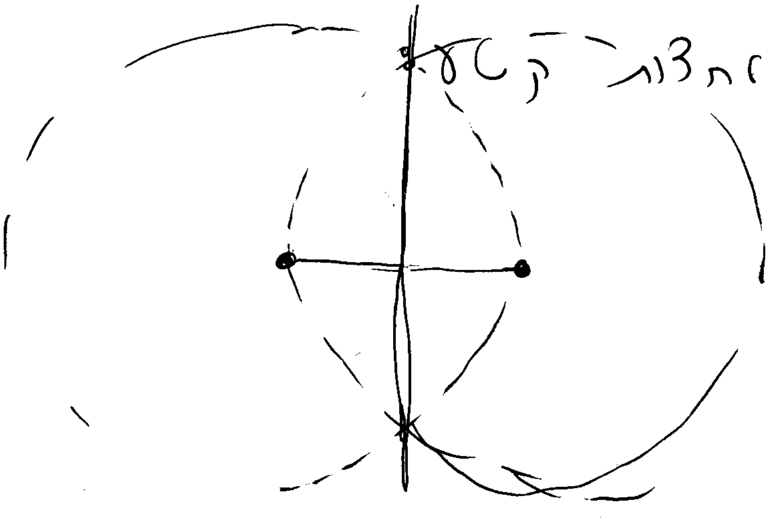
נניח שנתונה קבוצת נקודות במישור. מה אפשר לקבל בעזרת סרגל ומחוגה?
צריך להגיד מהם החוקים של המשחק:

- אפשר להעביר ישר דרך כל שתי נקודות מקבוצה
- אפשר להעביר מעגל שמרכזו בקבוצה והרדיוס שלו שווה למרחק בין שתי נקודות מקבוצה.

רק מתקבלות נקודות חדשות - נקודות חיתוך של ישרים ומעגלים ואפשר להשתמש גם בהן.

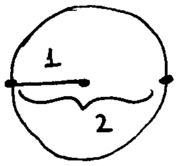
<u>הגדרה</u>: בהינתן קבוצה A של נקודות במישור נאמר כי נקודה p במישור ניתנת לבנייה מ-A בצעד אחד אם p נקודת חיתוך של ישר או מעגל עם ישר או מעגל המוגדרים ע"י A (כלומר אפשר לבנות שתי צורות שהן בצעד).

<u>דוגמה</u>: אפשר לחצות קטע



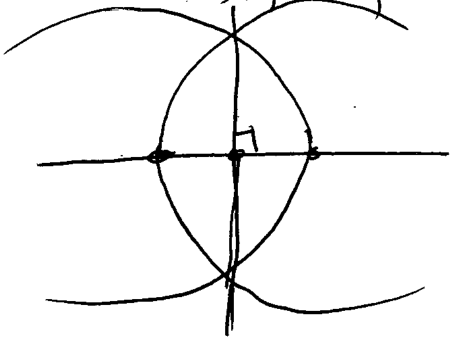
דוגמה: אפשר להכפיל בכל מספר שלם.

למשל, עבור 2 :

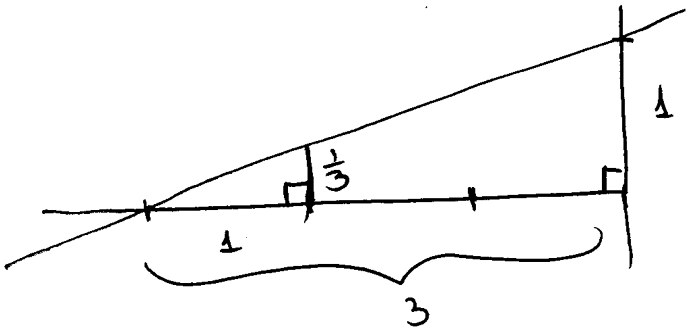


--- והשאר באינדוקציה...

דוגמה: אפשר להעביר אנך לנקודה
(ולכן אפשר לבנות
מערכת צירים)



דוגמה: אפשר לחלק בכל מספר שלם (בעזרת שימוש בדמיון משולשים):

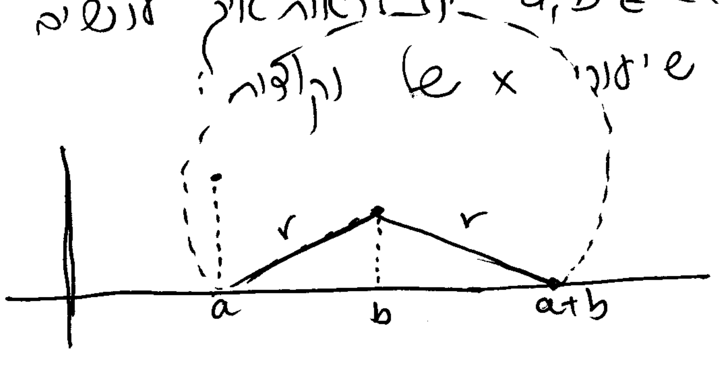


בהינתן קבוצה $A \subseteq \mathbb{R}^2$ נבנה מערכת צירים עם ראשית ב-A:
ציר x עובר דרך שתי נקודות מ-A וציר y ניצב לציר x
נקבע את יחידת האורך במישור לפי המרחק בין שתי נקודות כלשהן ב-A.

הגדרה: $C(A)$ הוא קבוצת שיעורי x, y של כל הנקודות שניתן לבנות מ-A במספר סופי של צעדים.

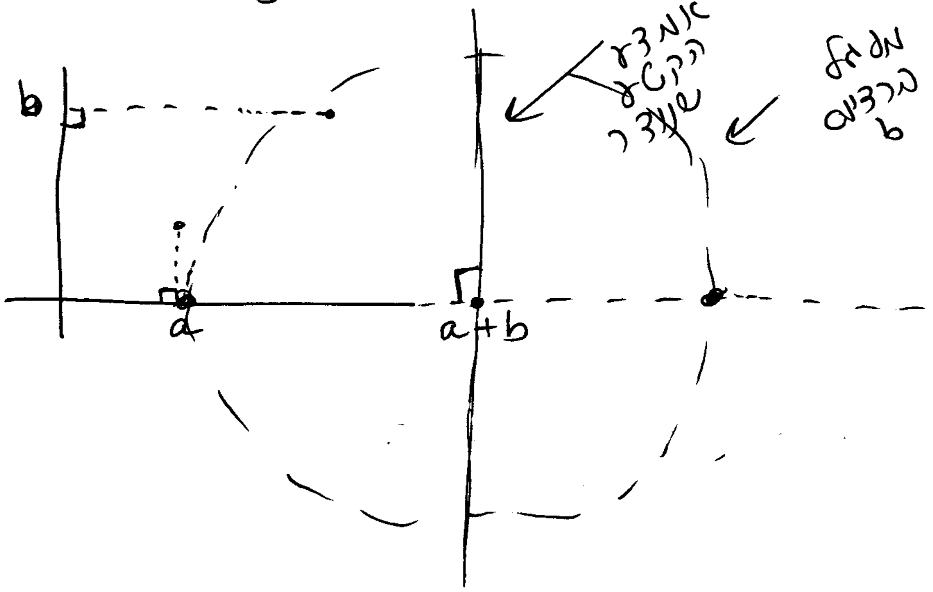
טענה: $C(A)$ הוא שדה, ולמעשה תת שדה של $\mathbb{R}$.

הוכחה: אם $a,b \in C(A)$ ~~ק~~ נראה איך עושים חיבור.
למשל, אם שניהם שיעורי x של נקודות:

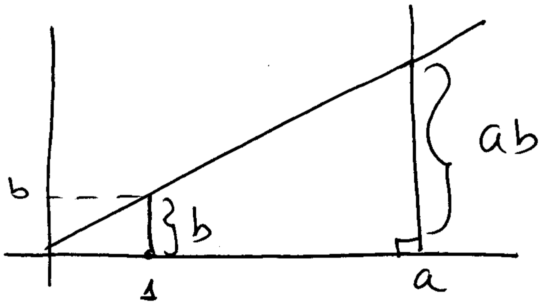


באופן דומה
אם a,b
שיעורי y של
נקודות.

אם a שיעור x ו-b שיעור y אז



כפל בעזרת דימיון משולשים:

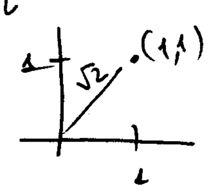


חילוק באופן דומה.
אז אפשר לעשות חיבור, כפל וחילוק אז זה שדה.

☺

שאלה: מהו השדה $C(A)$? מהו שדה ההרחבה של $\mathbb{Q}$.
אבל אנחנו נטען שזו הרחבה אלגברית!

למשל אפשר לקבל את $\sqrt{2}$:



נסמן ב- $F=F(A)$ את השדה הנפרש משיעורי x,y של נקודות A. (השדה המינימלי שמכיל את A. למשל אם יש שתי נקודות ב-A שמרחקן 1 אז $F(A)=\mathbb{Q}$).
אז $F(A)$ תת שדה של $C(A)$.

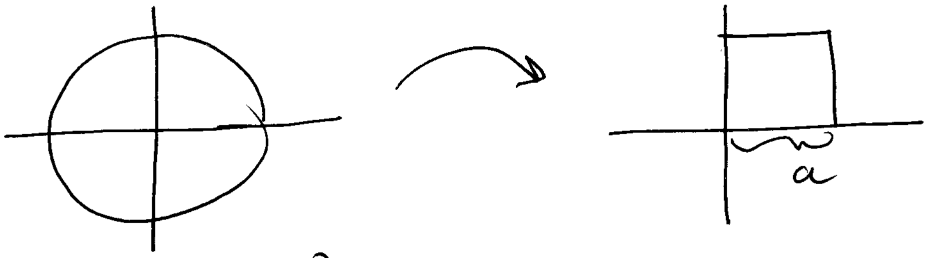
משפט: אם $\alpha \in C(A)$ אז α אלגברי מעל $F(A)$!
$|F(\alpha)/F|$ חזקה של 2. בנוסף, אם $\alpha \in \mathbb{R}$ מקיים

ש- $\left|F(\alpha)/F\right|$ חזקה של 2 אז $\alpha \in C(A)$.

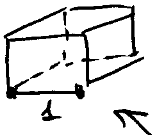
אז המשפט אומר שאנחנו יודעים בדיוק מהן הנקודות שאפשר לבנות ואי אפשר לבנות.

דוגמאות:

① ריבוע מעגל: נניח שנתון מעגל ברדיוס 1. האם ניתן לבנות ריבוע ששטחו כשטח המעגל. (משהו שנתונים המרכז והרדיוס)



האם ניתן לבנות a כך ש- $a^2=\pi$, כלומר $a=\sqrt{\pi}$?
אי אפשר כי π לא אלגברי!



② האם ניתן להכפיל נפח קוביה?
קטע באורך 1 מגדיר קוביה בנפח 1. האם אפשר למצוא קטע שמגדיר קוביה בנפח 2? כלומר השאלה היא אם $\sqrt[3]{2}\in C(\{0,1\})$. התשובה היא לא כי $\sqrt[3]{2}$ הוא שורש של $p(x)=x^3-2$ והוא אי פריק ולכן $\left|\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right|=3$ שאינה חזקה של 2.

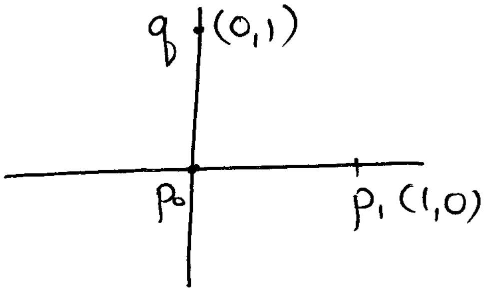
③ האם אפשר לחלק זווית ל-3? באופן כללי, לא.
למשל אם $\theta=\frac{\pi}{3}$ אז $\cos\theta=\frac{1}{2}$ לכן אפשר לבנות זווית θ. אבל לעומת זאת את $\alpha=\frac{\theta}{3}=\frac{\pi}{9}$ אי אפשר לבנות. ידועה הזהות $\cos 3\alpha=4\cos^3\alpha-3\cos\alpha$ אז $\cos\alpha$ צריך לקיים $\frac{1}{2}=4x^3-3x$, כלומר $\cos\alpha$ שורש של $p(x)=8x^3-6x-1$ אבל זה פולינום אי-פריק ממעלה 3 ולא חזקה של 2!

⑲ 16.6.08

מבנים

בניה בסרגל ומחוגה

מתחילים מקבוצה $A \subseteq \mathbb{R}^2$ שבה יש לפחות שתי נקודות. בוחרים $p_0, p_1 \in A$ ומגדירים מערכת צירים במישור כאשר הראשית היא p_0, ציר ה-x עובר דרך p_0 ו- p_1 כאשר p_1 מתאימה ל- $(1,0)$. נבחר וקטור ניצב לישר $\overline{p_0p_1}$ דרך p_0 באורך שווה לאורך של $\overline{p_0p_1}$



על נקודה במישור יש זוג קואורדינטות $p = (x_p, y_p)$

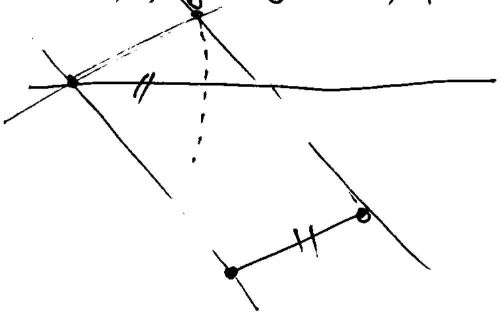
נסמן $F(A) = \{$ השדה הנוצר ע"י $\{x_p, y_p : (x_p, y_p) \in A\}\}$

$C(A) = \{$ השדה הנוצר ע"י קואורדינטות של הנקודות הניתנות לבנייה מ- A $\}$

$\mathcal{C}(A) =$ אוסף הנקודות הניתנות לבניה בעזרת סרגל ומחוגה מ- A.

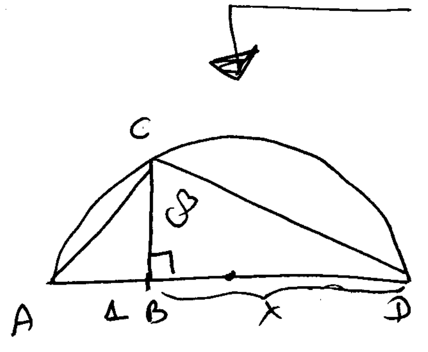
אז למעשה $C(A) = F(\mathcal{C}(A))$

היום אנחנו משנים את החוקים: אי אפשר להרים את המחוגה מהדף ולהעביר אותה למקום אחר. לפי ההגדרה בהינתן שתי נקודות אפשר להעביר מעגל סביב אחת מהן שרדיוסו המרחק ביניהן. אבל אפשר להוכיח שלמעשה אפשר גם "להעביר" אורכים:



מהיותן מן קטעים ב- A באורכים x,y ניתן לבנות קטע באורך:

- $x+y$
- $x-y$
- xy
- x/y
- $\sqrt{x}$



$$\Delta ABC \sim \Delta CBD$$

$$\frac{1}{\beta} = \frac{\beta}{x} \Leftarrow\Rightarrow x = \beta^2$$

$$\beta = \sqrt{x}$$

משפט: (תיקון של המשפט מהפעם הקודמת!)

תהי נתונה קבוצה A במישור (עם 2 נקודות לפחות).

נסמן $F = F(A)$. אז $\alpha \in C(A)$ אמ"מ

$\alpha \in F[\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_k}]$ כאשר לכל $1 \le i \le k$

$a_i \in F[\sqrt{a_1}, \dots, \sqrt{a_{i-1}}]$.

מסקנה: $\mathcal{C}(A) = \{(x,y) : x,y \in C(A)\}$

הוכחת המשפט:

($\Rightarrow$) נניח $\alpha \in F[\sqrt{a_1}, \dots, \sqrt{a_k}]$ $(*)$ כאשר $a_i \in F[\sqrt{a_1}, \dots, \sqrt{a_{i-1}}]$

נוכיח באינדוקציה על k שאם מתקיים $(*)$ אזי ניתן לבנות קטע באורך α. עבור $k=0$ זה ברור כי אם $\alpha \in F = F(A)$ וראינו שניתן ליצור קטעים שאורכם סכום, הפרש, מכפלה או מנת אורכי קטעים נתונים. נניח באינדוקציה עבור $k-1$.

לכן, היות ש- $a_k \in F[\sqrt{a_1}, \dots, \sqrt{a_{k-1}}]$ ניתן לבנות קטע באורך a_k $\Leftarrow$ ניתן לבנות קטע באורך $\sqrt{a_k}$ $\Leftarrow$ ניתן לבנות קטע באורך α.

($\Leftarrow$) נניח ש- $\alpha \in C(A)$. טוען α בשדה הנוצר ע"י קואורדינטות של נקודות ניתנות לבנייה מ- A. צריך להראות שקיים k

$a_1,\dots,a_k \in \mathbb{R}$ כך ש- $\alpha \in F[\sqrt{a_1},\dots,\sqrt{a_k}]$

$a_i \in F[\sqrt{a_1},\dots,\sqrt{a_{i-1}}]$.

נסמן ב- Ω את הקואורדינטות של נקודות הנתונות לבנייה מ- A. אז $C(A)$ הוא השדה שנוצר ע"י Ω:

אם $\alpha \in C(A)$ אז $\alpha = \frac{\sum_{i=1} a_{j_1}\cdots a_{j_{k_i}}}{\sum_{l=1}^{m} b_{n_j}\cdots b_{n_{k_l}}}$ כאשר $a_i, b_j \in \Omega$.

כלומר, α שייך לשדה הנוצר ע"י קואורדינטות של מספר סופי של נקודות ב- $C(A)$. נותר עוד להראות כי: לכל נקודה ב- $C(A)$ הקואורדינטות שלה מקיימות את התנאי (*). די להראות שבתהליך בנייה בכל שלב הקואורדינטות המתקבלות מקיימות את תנאי (*). הקואורדינטות של נקודה חדשה הן פתרון של מערכת משוואות שהיא

① לינארית אם הנקודה היא חיתוך זוג ישרים

② ריבועית אם הנקודה היא חיתוך מעגל עם ישר או מעגל.

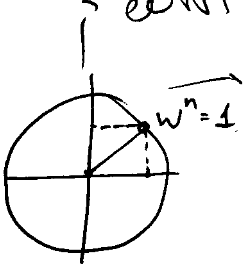
במקרה (1) הקואורדינטות הן בשדה בו אנו נמצאים ובמקרה (2) ייתכן שיש צורך להרחיב את השדה בעזרת שורשים של איברים מהשדה.

נשים לב ש- $[F[\sqrt{a_1},\dots,\sqrt{a_k}]:F] = 2^m$ עבור $m \le k$ כלשהו.

מסקנה: בהינתן A כך ש- $F(A) = \mathbb{Q}$ לא ניתן לבנות את $\sqrt[3]{2}$ כי $[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}] = 3$ כי $\sqrt[3]{2}$ שורש של x^3-2 שהוא אי-פריק. לכן לא קיימים $a_1,\dots,a_n$ כך ש- $\sqrt[3]{2} \in \mathbb{Q}[\sqrt{a_1},\dots,\sqrt{a_k}] = M^{(**)}$ כאשר $a_i \in \mathbb{Q}[\sqrt{a_1},\dots,\sqrt{a_{i-1}}]$ כי מ- (**) נקבל $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}] \subseteq M$ אבל אז $3 = [\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}] \mid [M:\mathbb{Q}] = 2^m$ בסתירה.

שאלה: אילו מצולעים משוכללים ניתן לבנות בעזרת סרגל ומחוגה?

תשובה: משכול לבנות מצולע משוכלל עם n צלעות צריך למעשה לבנות את $\omega = e^{\frac{2\pi i}{n}}$ ובמשכול זה צריך את $(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$. אז תנאי הכרחי ומספיק לכך שאפשר לבנות מצולע משוכלל בן n צלעות הוא שהקואורדינטות $(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$ מקיימות את (*) מהמשפט.



תרגיל: להוכיח שאי אפשר לבנות משובע. (7-גון).

משפט: אם p ראשוני מהצורה $2^{2^n}+1$ אז ניתן לבנות מצולע משוכלל בן p צלעות.

משפט: F שדה, $F \subseteq E$ שדה הרחבה ונניח $f \in F[X]$ פולינום המתפצל ב-$E[X]$ ונניח ש-E נוצר ע"י שורשי הפולינום f כלומר $E = F[\alpha_1, \dots, \alpha_d]$ כאשר $f(x) = \prod_{i=1}^{d}(x-\alpha_i)$ ב-$E[X]$.
ויהי $F \subseteq \Omega$ שדה כך ש-f מתפצל ב-$\Omega[X]$.
אזי מספר ה-F-הומומורפיזמים $\varphi: E \to \Omega$ הוא לכל היותר $[E:F]$ ושוויון מתקיים אמ"מ ל-f יש $[E:F]$ שורשים שונים ב-Ω.

הוכחה: α_1 הוא שורש של f אבל α_1 שורש של איזשהו גורם אי-פריק ב-$F[X]$, g_1 של f.
תמונות α_1 ב-Ω הוא שורש של g_1 אבל מספר האפשרויות לבחירת תמונה ל-α_1 הוא לכל היותר $\deg g_1 = [F[\alpha_1]:F]$ ושוויון בדיוק כאשר ל-g_1 יש $\deg g_1$ שורשים שונים ב-Ω.

לאחר בחירת $\varphi(\alpha_1)$ מבין שורשי g_1 ב-Ω נזהה את $F[\alpha_1] \subseteq E$ עם $F[\varphi(\alpha_1)] \subseteq \Omega$. כלומר מתפשטים $F[\alpha_1]$-הומומורפיזם מ-$F[\alpha_1, \alpha_2]$ ל-Ω.
α_2 הוא שורש של f אבל הוא שורש של גורם אי-פריק g_2 של f.

ב- $F[\alpha_1]$. תמונת α_2 היא שורש של g_2 ב- Ω

לכן מספר האפשרויות ל- α_2 הוא לכל היותר $[F[\alpha_1,\alpha_2]:F[\alpha_1]] = \deg g_2$

ושוויון בדיוק כאשר ב- Ω יש ל- g_2 $\deg g_2$ שורשים שונים.

נמשיך את התהליך שוב ושוב עד לבחירת תמונת α_d.

$\underset{\text{אפשרויות}}{[F[\alpha_1]:F]} \geq \alpha_1 \longmapsto$ {שורשים של g_1}

$\underset{\text{אפשרויות}}{[F[\alpha_1,\alpha_2]:F[\alpha_1]]} \geq \alpha_2 \longmapsto$ {שורשים של g_2}

$\vdots$

$\underset{\text{אפשרויות}}{[F[\alpha_1,\dots\alpha_j]:F[\alpha_1\dots\alpha_{j-1}]]} \geq \alpha_j \longmapsto$ {שורשים של g_j}

$\vdots$

$\underset{\text{אפשרויות}}{[F[\alpha_1,\dots,\alpha_d]:F[\alpha_1\dots\alpha_{d-1}]]} \geq \alpha_d \longmapsto$ {שורשים של g_d}

סה"כ מספר האפשרויות הוא לכל היותר מכפלת האפשרויות בכל שלב:

$$[F[\alpha_1,\dots,\alpha_d]:F[\alpha_1,\dots,\alpha_{d-1}]]\cdot\ldots\cdot[F[\alpha_1]:F] =$$
$$= [F[\alpha_1,\dots,\alpha_d]:F] = [E:F]$$

ושוויון בדיוק כשיש מספר שורשים מירבי - כאשר ב- Ω יש ל- f $[E:F]$ שורשים.

שורשים רבים

$f,g\in F[X]$, $\neq 0$. מחלק משותף מקסימלי q הוא פולינום ממעלה גבוהה ביותר אשר מחלק את f ואת g. אפשר לרשום $q = rf+sg$ $\quad r,s\in F[X]$

המחלק המשותף של f,g אינו משתנה אם לוקחים הרחבה של F

אפשר לראות את זה מהסתכלות באלגוריתם אוקלידס - אבל לא חשוב באיזה שדה משתמשים: אם $F\subseteq\Omega$ ונניח $h\in\Omega[X]$ מחלק את f,g. אז $h\,|\,q=rf+sg \Leftarrow \deg h\leq\deg g$

ואם $\deg h<\deg g$ כי סתירה למקסימליות ...)

יהי $f\in F[X]$ ויהי $F\subseteq\Omega$ שדה הרחבה כך ש-

$$f(x)=\prod_{i=1}^{k}(x-\alpha_i)^{m_i}\qquad \alpha_i\neq\alpha_j$$

אם $m_i=1$, α_i נקרא שורש פשוט

אם $m_i>1$, α_i נקרא שורש כפול.

$\{m_1,\dots,m_k\}$ אינה תלויה בשדה Ω . $F[\alpha_1,\dots,\alpha_d]$ שדה
הפיצול של f מעל F ולכן $m_1,\dots,m_k$ (עד כדי סדר)
אינם תלויים ב- Ω.

בהינתן פולינום f כיצד ניתן לבדוק האם ל- f יש שורש כפול?

<u>טענה</u>: ל- f יש שורש כפול אמ"מ $gcd(f,f')\neq 1$
(f' - הנגזרת של f)

<u>הוכחה</u>: ראשית, צריך להגדיר פעולת גזירה של $F[X]$ (עבור
שדה כלשהו), אם $f(x)=\sum_{i=0}^{n} a_i x^i$ אז
$f'(x)=\sum_{i=1}^{n} i\cdot a_i x^{i-1}$

מראים שכל התכונות של גזירה המוכרות לנו מתקיימות:

כלומר $f'+g'=(f+g)'$

$f'g+g'f=(fg)'$

ואז נניח שאם $f(x)=\prod(x-\alpha_i)^{m_i}=(x-\alpha)^m g$

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

ולכן אם $m>1$ נקבל ש- $(x-\alpha)^{m-1}$ מחלק את
f ואת f' ולכן אינם זרים.

המשך מחר...

(22) 17.6.08
מבנ״ית

שורשים מרובים

F שדה ; $f\in F[X]$. קיים שדה הרחבה בה כך ש- $f=\prod_{i=1}^{k}(X-\alpha_i)^{m_i}$ כאשר $\alpha_i\neq\alpha_j$ עבור $i\neq j$. אם $m_i=1$ אומרים ש- α_i שורש פשוט ואם $m_i>1$ אומרים ש- α_i שורש מרובה (כפול).

משפט: יהי f פולינום אי-פריק ב- $F[X]$. אזי התנאים הבאים שקולים:

① יש ל- f שורש מרובה

② $\gcd(f,f')\neq 1$

③ $\mathrm{char}F=p>0$, $f'=0$; $f(x)=g(x^p)$ ולאיזה $g\in F[X]$.

④ כל שורשי f הם מרובים.

הגדרה: (א) פולינום $f\in F[X]$ ייקרא ספרבילי אם לכל גורמיו האי-פריקים ב- $F[X]$ יש רק שורשים פשוטים (בשדה פיצול).

(ב) שדה ייקרא מושלם אם כל הפולינומים בו הם ספרבילים.

מסקנה:

(א) שדה ממציין 0 הוא שדה מושלם

(ב) שדה F ממציין $p>0$ הוא מושלם אמ״מ לכל איבר $a\in F$ קיים $b\in F$ כך ש- $b^p=a$.

הוכחת המשפט:

$(1\Rightarrow 2)$ הערנו כבר בפעם הקודמת כי אם ל- f יש שורש מרובה α אזי f ו- f' מתחלקים ב- $X-\alpha$ ולכן אינם זרים. לכן מ- (1) נובע ש- $\gcd(f,f')\neq 1$.

$(2\Rightarrow 3)$ נסמן $g=\gcd(f,f')$. לפי ההנחה $\deg g\geq 1$ ו אזי היות ש- f אי-פריק נובע ש- $f=g$ (עד כפול בסקלר) וקיבלנו ש- f' פולינום ממעלה קטנה ממעלת f המתחלק

בפולינום ממעלת f. ⇐ $f'=0$.

נניח $f=\sum_{i=0}^{n}a_ix^i$ אז $0=f'=\sum_{i=1}^{n}ia_ix^{i-1}$

⇐ לכל $1\le i\le n$ $ia_i=0$. היות ש- $a_n\neq 0$

ו- $na_n=0$ נובע שמציין F ראשוני $0<p$!

$n=pm$ ו- m טבעי. לכל $1\le i<n$ אם $a_i\neq 0$

אז $p|i$. כלומר $f=\sum_{j=0}^{n/p}a_{pj}x^{pj}$

⇐ $f(x)=g(x^p)$ כאשר $g=\sum_{j=0}^{n/p}a_{pj}x^j$

(3 ⇐ 4) נתון $\mathrm{char}F=p>0$ ו- $f(x)=g(x^p)$

קיים שדה הרחבה Ω כך ש- $g(x)=\prod_{j=1}^{m}(x-\beta_j)$ $m=\frac{n}{p}$

אז $f(x)=g(x^p)=\prod_{j=1}^{m}(x^p-\beta_j)$. קיימת הרחבה

$F\subseteq\Omega\subseteq\Lambda$ כך שקיימים $\gamma_j\in\Lambda$ כך ש- $\gamma_j^p=\beta_j$

ואז $f(x)=g(x^p)=\prod_{j=1}^{m}(x^p-\beta_j)=\prod_{j=1}^{m}(x^p-\gamma_j^p)=$

$$=\prod_{i=1}^{m}(x-\gamma_j)^p$$ כי המציין p

ואז הריבוי של השורשים מ-Λ הוא לפחות p.

(4 ⇐ 1) זהו!

☺

מסקנה:

(א) שדה ממציין אפס הוא מושלם

(ב) שדה ממציין $0<p$ הוא מושלם אמ"מ לכל $a\in F$ קיים $b\in F$ כך ש- $b^p=a$.

הוכחה:

(א) נובע מהשקילות $3 \Leftrightarrow 1$

(ב) נניח שקיים $a\in F$ כך שלא קיים $b\in F$ כך ש- $b^p=a$. נתבונן בפולינום $f=x^p-a$. נשים לב שאין ל-f שורש ב- F. יהי $F\subseteq\Omega$ שדה הרחבה כך שקיים $\beta\in\Omega$ כך ש- $\beta^p=a$. ב- $\Omega[X]$ קיים

$$(x-\beta)^p=x^p-\beta^p=x^p-a=f$$

⇐ f אינו ספרבילי. יהי $h\in F[X]$ גורם אי-פריק של

f. אזי $h=(x-\alpha)^r$ כאשר $2\le r\le p$

לכן קיבלנו שהשדה אינו מושלם.

בכיוון שני, נניח שלכל $a\in F$ קיים $b\in F$ כך ש- $b^p=a$. ונראה שהשדה מושלם. נניח f ב- $F[x]$ פולינום אי-פריק עם שורשים כפולים. ⇐ קיים פולינום $g\in F[x]$ כך ש- $f=g(x^p)$ כאשר $g=\sum_{i=0}^{m}a_i x^i$

אז $f(x)=g(x^p)=\sum_{i=0}^{m}a_i x^{pi}$

מההנחה נובע שקיימים $b_i\in F$ כך ש- $b_i^p=a_i$. קיבלנו ש- $f(x)=\sum_{i=0}^{m}a_i x^{pi}=\sum_{i=0}^{m}b_i^p x^{pi}=\sum(b_i x^i)^p=(\underbrace{\sum b_i x^i}_{\in F[x]})^p$

נסמן $h(x)=\sum b_i x^i \in F[x]$ וקיבלנו $f=h^p$

וסתירה להנחה ש- f אי פריק

㉔ 23.06.08
מבנים

שיעור עם דחיק.

(2.7) <u>טענה</u>: נניח $f \in F[X]$. נוצר $E \supseteq F$ ע"י שורשים של f. ויהי $\Omega \supseteq F$ שדה שבו f מתפצל. אזי

ⓐ יש הומומורפיזם $f: E \to \Omega$

ⓑ מספר ההומומורפיזמים $E \to \Omega$ הוא לכל היותר $[E:F]$ ומתקיים שוויון רק אם ל-f יש $\deg f$ שורשים שונים ב-Ω.

(2.8) <u>מסקנה</u>: E, L הרחבות של F כאשר $|E/F| < \infty$. אזי

ⓐ מספר ההומומורפיזמים $E \to L$ הוא לכל היותר $[E:F]$

ⓑ קיימת הרחבה סופית Ω/L ו-F-הומומורפיזם $E \to \Omega$.

 <u>תורת גלואה</u>

$F \subseteq E$ שדות. F-איזומורפיזם מ-E ל-E נקרא F-אוטומורפיזם.
כל ה-F-אוטומורפיזמים של E מהווים חבורה שמסומנת $\mathrm{Aut}(E/F)$.

<u>דוגמאות</u>: ① $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \cong C_2$ חבורה ציקלית מסדר 2 עם יוצר $z \mapsto \bar{z}$. לא קשה להראות שזה ה-F-אוטומורפיזם היחיד שאינו הזהות. [מספיק להראות שהאפשרויות היחידות הן $i \mapsto i$ או $i \mapsto -i$ ובגלל שהממשיים עוברים לעצמם יש רק $x+iy \mapsto x+iy$ או $x+iy \mapsto x-iy$]

② $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ חבורה מעוצמת הרצף

③ $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{id\}$ (כמה מפתיע!). אמנם כל אוטומורפיזם צריך לשמור על סדר אז מהצפיפות של $\mathbb{Q}$ ב-$\mathbb{R}$ ינבע שהוא טריוויאלי – כי הוא שומר על $\mathbb{Q}$ ולכן שומר על $\mathbb{R}$. איך נראה שהוא שומר על סדר? מספיק להראות שהחיוביים עוברים לעצמם. אבל מספר הוא חיובי אמ"מ הוא ריבוע. ואיברים ריבועיים עוברים לאיברים ריבועיים שהם חיוביים... אז כל אוטומורפיזם של $\mathbb{R}$ שומר על $\mathbb{R}^{\geq 0}$ ולכן כל אוטומורפיזם שומר על הסדר ב-$\mathbb{R}$ ומכיוון ש-$\mathbb{Q}$ צפופה ב-$\mathbb{R}$ אינווריאנטית תחת אוטומורפיזם נובע שכל

אוטומורפיזם הוא טריוויאלי.

④ $\text{Aut}(\mathbb{C}(x)/\mathbb{C}) \cong PGL_2(\mathbb{C})$ (ללא הוכחה)

שדה הפונקציות הרציונליות מעל $\mathbb{C}$.

<u>טענה</u>: E שדה פיצול של פולינום ספרבילי מתוקן $f \in F[X]$. אזי

$$[E:F] = |\text{Aut}(E/F)|$$

<u>הוכחה</u>: אפשר להניח $f = \prod f_i^{m_i}$ כאשר f_i מתוקנים אי-פריקים שונים. אפשר להניח ש- $m_i = 1$ לכל i כי השורשים אותם שורשים וזה אותו שדה פיצול.

מה טענה (2.7) נובע שיש $[E:F]$ F-הומומורפיזמים שונים $E \to E$ ומכיוון ש-E הרחבה סופית כל F-הומומורפיזם $E \to E$ הוא F-אוטומורפיזם (מכיוון ש-E שדה הן מוכרח העתקה חח"ע ומכיוון שזה סוף ממדי העתקה חח"ע היא מוכרח על).

☺

<u>דוגמאות</u>:

א) $E = F[\alpha]$ כאשר α אלגברי. והפולינום המינימלי $f \in F[X]$ אם אין ל-f שורשים נוספים ב-E אז $\text{Aut}(E/F) = \{1\}$. למשל, $F = \mathbb{Q}$, $E = \mathbb{Q}[\sqrt[3]{2}]$. ב-$E$ יש ל-2 שורש שלישי יחיד. למשל, אפשר לקחת את $\sqrt[3]{2} \in \mathbb{R}$ אז $E \subseteq \mathbb{R}$. $|\text{Aut}(E/F)| = 1$, $|E/F| = 3$.

זאת דוגמה לכך שאם הפולינום לא מתפצל הטענה לא נכונה.

ב) הטענה גם לא נכונה אם הפולינום לא ספרבילי: F ממציין $p \neq 0$. $f(x) = x^p - a$ כאשר ל-$a \in F$ אין שורש p. (המצב הזה אפשרי!) למשל ניקח α אבר טרנס' מעל $\mathbb{F}_p$; ו- $\beta = \alpha^p$. נתבונן ב- $F = \mathbb{F}_p(\beta)$; $E = \mathbb{F}_p(\alpha) = F(\alpha)$ אז α שורש של $x^\beta - \alpha$ ומתקיים $x^p - \beta = (x-\alpha)^p$. אז α שורש יחיד של $x^p - \beta$ ב-E. לכן $|\text{Aut}(E/F)| = 1$ וזו הרחבה לא טריוויאלית ו-$1 < |E/F|$. שוב הטענה לא מתקיימת...

(25)

<u>טענה</u>: E/F הרחבה סופית, אז כל F-הומומורפיזם $\sigma: E\to E$ הוא F-אוטומורפיזם.

<u>הוכחה</u>: σ תח"ע כי E שדה ו- $\ker\sigma$ אידיאל, אבל בשדה אין אידיאלים פרט לטריויאליים - $\{0\}$, ו- E. וברור ש- $\ker\sigma\neq E$ כי ($F\not\subseteq\ker\sigma$). $\sigma: E\to E$ טרנספורמציה לינארית של E כמרחב וקטורי מעל F. אבל $\dim_F(E)=[E:F]<\infty$ אז כל ט"ל תח"ע הוא על. $\Leftarrow$ σ על. $\Leftarrow$ σ F-אוטומורפיזם. ☺

תהא E/F הרחבה. $G\subseteq \mathrm{Aut}(E/F)$ תת חבורה. מסמנים: $E^G=\{a\in E: \forall\sigma\in G\ \sigma(a)=a\}$ = שדה השבת של G (קל לראות שזה אכן שדה). אזי $F\subseteq E^G\subseteq E$.

לכל $G\subseteq \mathrm{Aut}(E/F)$ מתאים שדה ביניים E^G. מאידך, לכל שדה ביניים $F\subseteq K\subseteq E$ מתאימה תת החבורה

$$\mathrm{Aut}(E/F)\supseteq \mathrm{Aut}(E/K)$$

תחת תנאים מסויימים ההתאמות האלה חח"ע ועל ואז ההרחבה נקראת הרחבת גלואה ויש לה מיני תכונות מעניינות.

<u>הערה</u>: כשכותבים $\mathrm{Aut}(E)$ מתכוונים לכל האוטומורפיזמים של E (שלא קשורים לשדה כלשהו) אבל למעשה זה הרי שווה ל- $\mathrm{Aut}(E/F)$ כאשר F השדה הראשוני המתאים (כמו $\mathbb{Q}$ או $\mathbb{F}_p$).

<u>משפט ארטין</u>: $G\leq \mathrm{Aut}(E)$ תת חבורה סופית וכך ש- $F=E^G$. אזי $|G|=[E:F]$.

<u>הוכחה</u>: ממסקנה 2.8 $|G|\leq|\mathrm{Aut}(E/F)|\leq[E:F]$. נראה את אי-השוויון ההפוך. די להראות ש- $\dim_F E\leq|G|$. נניח בשלילה ש- $|G|=m$ ו- $\infty\geq\dim_F E\geq n>m$. יהיו $\alpha_1,\dots,\alpha_n\in E$ איברים בלתי תלויים לינארית מעל F. נסמן $G=\{\sigma_1,\dots,\sigma_m\}$. נביט במערכת המשוואות

$$\text{m משוואות ב-n נעלמים } n>m\quad \begin{cases}\sigma_1(\alpha_1)X_1+\dots+\sigma_1(\alpha_n)X_n=0\\ \vdots\\ \sigma_m(\alpha_1)X_1+\dots+\sigma_m(\alpha_n)X_n=0\end{cases}$$

מכיוון ש- $m < n$ יש פתרון. נבחר פתרון לא טריוויאלי $(c_1,\dots,c_n)$ עם מספר מינימלי של פרמטרים שונים מ- 0. בה"כ $c_1 \neq 0$. ע"י הכפלה בסקלר אפשר להניח $c_1 \in F$. יש i_0 שעבורו $c_{i_0} \notin F$ כי אנחנו מניחים ש- $\alpha_1,\dots,\alpha_n$ בת"ל מעל F. מכיוון ש- $F = E^G$ יש σ_k מסוים שעבורו $\sigma_k(c_{i_0}) \neq c_{i_0}$.

נתבונן במשוואות שלנו:

$$0 = c_1\sigma_1(\alpha_1) + \dots + c_i\sigma_1(\alpha_i) + \dots + c_n\sigma_1(\alpha_n)$$

$$\vdots$$

$$0 = c_1\sigma_m(\alpha_1) + \dots + c_i\sigma_k(\alpha_i) + \dots + c_m\sigma_m(\alpha_n)$$

נפעיל על כל המשוואות את σ_k ונקבל

$$0 = c_1\sigma_k\sigma_j(\alpha_1) + \dots + \sigma_k(c_i)\sigma_k\sigma_j(\alpha_i) + \dots + \sigma_k(c_n)\sigma_k\sigma_j(\alpha_n)$$

σ חבורה ולכן $\{\sigma_k\sigma_j : j=1,\dots,m\} = \sigma_k G = G = \{\sigma_j : j=1,\dots,m\}$ לכן נקבל שהקבוצה השמאלית היא תמורה ולכן שווה לקבוצה הימנית ולכן אחרי הפעלת σ_k קיבלנו את אותן משוואות מבעין אך בסדר שונה. לכן $(c_1,\sigma_k(c_2),\dots,\sigma_k(c_i),\dots,\sigma_k(c_n))$ פתרון למערכת המשוואות המקורית ולכן גם ההפרש בין שני הפתרונות הוא פתרון, כלומר $(0, c_2-\sigma_k(c_2),\dots,c_m-\sigma_k(c_m))$ פתרון ~~אבל לפתרון זה~~ לא טריוויאלי כי $c_{i_0} \neq \sigma_k(c_{i_0})$ אבל יש לו יותר אפסים מלפתרון המקורי וזו סתירה. ☺

(26) 24/6/08
מבנים

שיעור עם צחיק

<u>משפט ארטין</u>: $G \le Aut(E)$ חבורה סופית רק ש- $F = E^G$ אז $[E:F] = |G|$.

<u>מסקנה</u>: $G \le Aut(E)$ סופית אזי $G = Aut(E/E^G)$

<u>הוכחה</u>: נסמן $A = Aut(E/E^G)$. אז $F = E^A \supseteq E^G$

לפי מסקנה (2.8) $|A| \le [E:F] < \infty$.

ממשפט ארטין $|A| = [E:F]$ ו $|G| = [E:E^G]$.

מהגדרה $G \subseteq Aut(E/E^G) = A$. ⇐

$$|G| \le |A| = [E:F] \le [E:E^G] = |G|$$

$$\downarrow$$

$$F \supseteq E^G$$

⇐ $|G| = |A|$. אבל $G \subseteq A$ ⇐ $G = A$. ☺

<u>הגדרה</u>: הרחבה אלגברית E/F היא <u>ספרבילית</u> אם הפולינום המינימלי מעל F של כל איבר ב-E הוא ספרבילי. E/F נקראת <u>נורמלית</u> אם הפולינום המינימלי של כל איבר מתפצל.

אם E/F אלגברית לא ספרבילית אז F לא מושלם ולכן $char F = p \neq 0$ ובנוסף יש $a \in E$ שהפולינום המינימלי שלו הוא מהצורה $f(x^p) = p(x)$.

<u>דוגמה</u>: $\mathbb{F}_p(T)/\mathbb{F}_p(T^p)$ כאשר T טרנס' מעל $\mathbb{F}_p$ היא הרחבה לא ספרבילית כי הפולינום המינימלי של T הוא $p(x) = x^p - T^p$.

אם E/F נורמלית אז לכל איבר $a \in E$ הפולינום המינימלי f של a מעל F מתפצל ב-E. אם בנוסף E/F ספרבילית אז יש ב-E $\deg(f)$ שורשים שונים ל-f. השורשים של f ב-E נקראים <u>הצמודים</u> של a ב-E/F

למשל ב-$\mathbb{C}/\mathbb{R}$ הפולינום המינימלי של z הוא $p(x) = (x-z)(x-\bar{z}) =$
$= x^2 - (z+\bar{z})x + |z|^2$

הערה: F-אוטומורפיזם של E מעביר כל $a\in E$ לאחד הצמודים של $a\in E$.

הגדרה: הרחבה סופית E/F נקראת **גלואה** אם F הוא שדה השבת של חבורת ה-F-אוטומורפיזמים ($F=E^{Aut(E/F)}$). במקרה זה מסמנים את החבורה $Aut(E/F)$ ב- $Gal(E/F)$.

משפט: עבור הרחבה E/F התנאים הבאים שקולים:
(א) E הוא שדה הפיצול של איזה פולינום $f\in F[X]$ ספרבילי.
(ב) $F=E^G$ כאשר G חבורה סופית של אוטומורפיזמים של E
(ג) E/F סופית נורמלית וספרבילית
(ד) E/F הרחבת גלואה.

הוכחה:

(א $\Rightarrow$ ד) נסמן $G=Aut(E/F)$. אז $|G|\le[E:F]<\infty$. נסמן $F'=E^G$. E הוא שדה הפיצול של f גם מעל F'. מטענה (2.7) נובע ש- $[E:F]=|G|$ $[E:F']=|Aut(E/F')|$. אבל $F\subseteq F'$ ולכן $[E:F]\ge[E:F']$ ולכן $[E:F]\ge|Aut(E/F')|\ge|G|=[E:F]$ כי $G\subseteq Aut(E/F')$ ולכן $F=F'$.

(ד $\Rightarrow$ ב) $|Aut(E/F)|\le[E:F]<\infty$ $\Rightarrow$ $Aut(E/F)$ סופית.

(ב $\Rightarrow$ ג) נתון $F=E^G$. ממשפט ארטין $[E:F]=|G|<\infty$ ולכן E/F סופית. נראה ש- E/F ספרבילית ונורמלית. יהי $a\in E$ ויהיו $a=a_1,\dots,a_n$ (שונים) כל הצמודים של a ב- E/F. (רשום $f(x)=\prod_{i=1}^{n}(x-a_i)$. נטען ש- $f(x)\in F[X]$. לכל $\sigma\in G=Aut(E/F)$, $\sigma(f(x))=\prod(x-\sigma(a_i))=\prod(x-a_i)=f(x)$ כי σ עושה פרמוטציה על $a_1,\dots,a_n$ $\Rightarrow$ מקדמי f הם σ-אינווריאנטים לכל $\sigma\in G$. מהנתון (ב) נובע כי מקדמי f נמצאים ב- F, כלומר $f\in F[X]$. f מתפצל ב- E וספרבילי ולכן הפולינום המינימלי של a הוא גורם של f ולכן גם הוא מתפצל וספרבילי.

(ג $\Rightarrow$ א) אם $\alpha_1,\dots,\alpha_l$ יוצרים של E מעל F - $E=F(\alpha_1,\dots,\alpha_l)$, ניקח f_i פולינום מינימלי של α_i מעל F ונרשום $f=\prod f_i$. כל ה- f_i מתפצלים ולכן f מתפצל. E הוא שדה הפיצול של f מעל F. ☺
ו- f ספרבילי.

㉗ 30.6.08
מבנים

<u>הגדרה</u>: הרחבה סופית E/F תיקרא <u>הרחבת גלואה</u> אם עבור $G=Aut(E/F)$ מתקיים $E^G=\{a\in E: ga=a\ \forall g\in G\}=F$ (שדה השבת)

<u>הגדרה</u>: הרחבה סופית E/F תיקרא <u>נורמלית</u> אם לכל $\alpha\in E$ הפולינום המינימלי $f\in F[x]$ של α מתפצל ב- $E[x]$.

<u>משפט</u>: תהי E/F הרחבת שדות. אזי התנאים הבאים שקולים:
1. E שדה פיצול של פולינום ספרבילי $f\in F[x]$
2. $F=E^G$ עבור $G\le Aut(E)$ תת חבורה סופית
3. E/F הרחבה נורמלית ספרבילית סופית
4. E/F הרחבת גלואה.

<u>הגדרה</u>: הרחבה אלגברית E/F תיקרא ספרבילית אם לכל $\alpha\in E$ הפולינום המינימלי של α מעל F הוא ספרבילי.

<u>דוגמה</u>: הרחבה שאינה ספרבילית $\mathbb{F}_p(x^p)\subseteq\mathbb{F}_p(x)$
זה חייב להיות שדה ממציין p כי הראינו שכשמדובר בשדה ממציין 0 ההרחבה תמיד ספרבילית. גם חייבים להסתכל על שדה אינסופי...

<u>מטרה</u>: להראות קיום התאמה חח"ע ועל בין תתי חבורות של G ושדות חלקיים $F\subseteq M\subseteq E$

<u>משפט ארטין</u>: $G\le Aut(E)$ חבורה סופית ונסמן $F=E^G$.
אזי $[E:F]\le|G|$.

אם E/F הרחבת גלואה ! - $G=Gal(E/F)$ אז $F=E^G$.

$$\text{אז}\quad [E:F] \underset{\substack{\downarrow\\ \text{ארטין}}}{\le} |G| \underset{\substack{\downarrow\\ E\ \text{שדה}\\ \text{פיצול של פולינום}}}{\le} [E:G]$$

לכן $|G|=[E:G]$ במקרה זה.

אם E/F הרחבת גלואה ; $G = Gal(E/F)$. אם $\alpha \in E$ המסלול של α תחת G הוא הקבוצה $\{g\alpha : g \in G\} = \{\alpha_1, \dots, \alpha_n\}$ איברי המסלול נקראים צמודי α.

דוגמה: נתבונן בהרחבה $\mathbb{C}/\mathbb{R}$. אז $Gal(\mathbb{C}/\mathbb{R}) = \{id, \tau\}$ כאשר $\tau(z) = \bar{z}$.

טענה: כל הרחבה סופית ספרבילית $E \supseteq F$ מוכלת בהרחבת גלואה.
הוכחה: קיימים $\alpha_1, \dots, \alpha_m \in E$ כך ש- $E = F(\alpha_1, \dots, \alpha_m)$ כיוון ש- E/F ספרבילית, הפולינום המינימלי של α_i $f_i \in F[x]$ הוא ספרבילי. לכן $f(x) = \prod_{i=1}^{m} f_i(x)$ פולינום ספרבילי. יהי E' שדה הפיצול של הפולינום f. לפי המשפט כי הרחבת גלואה. ☺

הערה: אם E/F גלואה, $F \subseteq M \subseteq E$ אז E/M גלואה.
הוכחה: קיים פולינום $f \in F[x]$ ספרבילי כך ש- E שדה הפיצול שלו. ברור ש- $f \in M[x]$ ספרבילי ו- E שדה הפיצול שלו. לכן E/M גלואה. ☺

המשפט היסודי של תורת גלואה: תהי E/F הרחבת גלואה עם חבורת גלואה $G = Gal(E/F)$. אזי ההעתקות $E^H \longmapsfrom H$ עבור $H \leq G$ כאשר לכל $F \subseteq M \subseteq E$, $H = Gal(E/M)$ הן התאמות חח"ע ועל בין $\left\{\begin{matrix}\text{תת חבורות} \\ H \leq G\end{matrix}\right\}$ ו- $\left\{\begin{matrix}\text{שדות חלקיים} \\ F \subseteq M \subseteq E\end{matrix}\right\}$
יתר על כן:

1. ההתאמה הופכת סדר הכלה: לכל $H_1, H_2 \leq G$, $H_1 \subseteq H_2$ אמ"מ $E^{H_2} \subseteq E^{H_1}$
2. אינדקסים של חבורות שווים לדרגות הרחבות של שדות. כלומר, אם $H_2 \leq H_1 \leq G$ תת חבורות אז $[H_1 : H_2] = [E^{H_2} : E^{H_1}]$
3. עבור תת חבורה H ו- $\sigma \in G$ אם H מתאימה ל- M, כלומר $H = Gal(E/M)$ ו- $M = E^H$ אז $\sigma H \sigma^{-1}$ מתאימה ל- $\sigma M = E^{H\sigma^{-1}}$ ו- $\sigma H \sigma^{-1} = Gal(E/\sigma M)$
4. לכל $H \leq G$, H תת חבורה נורמלית אמ"מ ההרחבה $F \subseteq M = E^H$ היא

(28)

הרחבה נורמלית אמ"מ גלואה ! - $\text{Gal}(E^H/F) \cong G/H$.

<u>הוכחה</u>: ראשית צריך להראות שההתאמות

$$\omega: H \longmapsto E^H$$

$$\mu: M \longmapsto \text{Gal}(E/M)$$

הן הופכיות זו לזו.

$\text{Gal}(E/E^H) = H$ כי E/E^H גלואה $\vdots$ E שדה פיצול של f פולינום ספרבילי מעל E^H. לכן

$$|H| \underset{\text{ארטין}}{\geq} [E:E^H] \underset{\text{משפט קודם}}{=} |\text{Gal}(E/E^H)| \underset{H \subseteq \text{Gal}(E/E^H) \text{ כי}}{\geq} |H|$$

$\Leftarrow$ $|H| = |\text{Gal}(E/E^H)|$ $\Leftarrow$ $H = \text{Gal}(E/E^H)$.

$\Leftarrow$ $\mu \circ \omega = \text{id}_{\{\text{תת חבורות}\}}$.

צריך לבדוק גם ש-$\omega \circ \mu = \text{id}_{\{F \subseteq M \subseteq E\}}$. אם $F \subseteq M \subseteq E$ אז $M \subseteq E$ גלואה ולכן לפי ההגדרה $M = E^{\text{Gal}(E/M)}$.

אז הראנו שההתאמות חח"ע ועל. נראה את שאר התכונות.

1. ההתאמה הופכת סדר הכלה כי אם $H_2 \subseteq H_1$ אזי

$$E^{H_1} = \{a \in E : \tau a = a \ \forall \tau \in H_1\} \underset{H_2 \subseteq H_1}{\subseteq} \{a \in E : \tau a = a \ \forall \tau \in H_2\} = E^{H_2}$$

מכיוון שני, אם $M_1 \subseteq M_2$ ברור ש-$\text{Gal}(E/M_1) \subseteq \text{Gal}(E/M_2)$

2. אם $H_2 \subseteq H_1$, אם $H_2 = \{e\}$ אז

$$[H_1 : H_2] = [H_1 : \{e\}] = |H_1| = [E : E^{H_1}]$$

כעת, באופן כללי,

$$|H_1| = [E : E^{H_1}] = [E : E^{H_2}][E^{H_2} : E^{H_1}]$$

לכן

$$[H_1 : H_2] = \frac{|H_1|}{|H_2|} = \frac{[E:E^{H_2}][E^{H_2}:E^{H_1}]}{[E:E^{H_2}]} = [E^{H_2} : E^{H_1}]$$

3. $\{H \leq G\} \longleftrightarrow \{F \subseteq M \subseteq E\}$

$$H \longmapsto E^H$$

$$M = E^H$$

אם $\sigma \in G$ אז

$$E^{\sigma H \sigma^{-1}} = \{a \in E : \forall \tau \in H \ \sigma \tau \sigma^{-1} a = a\} =$$

$$= \{a \in E : \forall \tau \in H \ \tau(\sigma^{-1} a) = \sigma^{-1}(a)\}$$

$\Leftarrow$

$$\sigma^{-1} E^{\sigma H \sigma^{-1}} = \{\sigma^{-1} a \in E : \forall \tau \in H \ \tau(\sigma^{-1} a) = \sigma^{-1} a\} =$$

$$= \{b \in E : \forall \tau \in H \ \tau b = b\} = E^H$$

לכן $E^{\sigma H \sigma^{-1}} = \sigma E^H$.

~~4. נניח ש- $H \triangleleft G$ נורמלית. אזי לכל $\sigma \in G$ $\sigma H \sigma^{-1} = H$~~

~~$\Leftarrow$ $E^H = E^{\sigma H \sigma^{-1}} = \sigma E^H$, כלומר תת השדה $F \subseteq E^H \subseteq E$~~

~~אינווריאנטי תחת כל $\sigma \in G$. לכן ניתן להגדיר הומומורפיזם~~

~~$$f: Gal(E/F) \longrightarrow Gal(E^H/F)$$~~

~~$$\sigma \longmapsto \sigma|_{E^H}$$~~

~~$w \in Gal(E/F)$ שייך לגרעין של f פירושו $w|_{E^H} = id|_{E^H}$~~

~~לכן גרעין f הוא בדיוק H כי יש התאמה חח"ע ועל בין תתי שדות~~

~~ותתי חבורות. לכן $G/H \hookrightarrow Gal(E^H/F)$~~

~~$$(E^H)^{G/H} = (E^H)^G = E^G = F$$~~

~~$\Leftarrow$ $G/H = Gal(E^H/F)$~~

$(\Leftarrow)$ נתון $H \triangleleft G$ ורוצים להראות ש- E^H/F נורמלית (אף גלואה) ויש- $Gal(E^H/F) \cong G/H$.

מהנורמליות של H, לכל $\sigma \in G$ מתקיים $\sigma H \sigma^{-1} = H$. לכן $E^H = E^{\sigma H \sigma^{-1}} = \sigma E^H$. לכן יש הומומורפיזם

$$f: \underset{G}{\underset{\shortparallel}{Gal(E/F)}} \longrightarrow Aut(E^H/F)$$

הגרעין של f הוא $\ker f = \{\sigma \in G : \sigma|_{E^H} = id\} = Gal(E/E^H) = H$

לכן יש שיכון $G/H \hookrightarrow Aut(E^H/F)$. נחשוב על G/H כתת-חבורה של $Aut(E^H/F)$. אנו רוצים להראות שקיים שוויון $G/H = Aut(E^H/F)$, כלומר ההעתקה מ- G ל- $Aut(E^H/F)$ היא על, וכן שההרחבה E^H/F היא גלואה (ובפרט נורמלית)

מתקיים $(E^H)^{G/H} = (E^H)^G = E^G = F$. לכן E^H/F הרחבת גלואה (לפי משפט קודם). לכן $Aut(E^H/F) = Gal(E^H/F)$

קיבלנו הרחבת גלואה E^H/F ותת חבורה G/H ב- $Gal(E^H/F)$ כך ש- $(E^H)^{G/H} = F$. לכן בגלל חח"ע התאמת גלואה בין שדות לחבורות נובע ש- $Gal(E^H/F) = G/H$.

$(\Rightarrow)$ נניח ש- E^H/F הרחבה נורמלית (אף גלואה). יהי $\alpha \in E^H$ ויהי $f \in F[x]$ הפולינום המינימלי של α. f מתפצל ב- E^H, כלומר שורשיו שייכים ל- E^H. נסמן $G = \{\sigma_1, \dots, \sigma_m\}$. לכל i $\sigma_i \alpha$ שורש של f, כלומר לכל $\sigma \in G$ $\sigma\alpha$ שורש של f אך

(29)

$\sigma\alpha\in E^H$. $\Leftarrow$ לכל $\sigma\in G$ $\sigma E^H = E^H$ וזה אומר

$\sigma H\sigma^{-1} = H$ כי

$$\begin{tikzcd}
E^H = \sigma E^H = E^{\sigma H\sigma^{-1}} \\
H = \sigma H\sigma^{-1} \arrow[u, leftrightarrow]
\end{tikzcd}$$

☺ כלומר H נורמלית ב- G.

<u>מסקנות</u>:

(א) E/F הרחבת גלואה. נניח שנתונים שדות חלקיים $F\subseteq M_i\subseteq E$ $1\le i\le k$ ומתאימים להם לפי התאמת גלואה $H_i\le G=Gal(E/F)$ השדה $F\subseteq M_1\dots M_k\subseteq E$ הוא השדה הקטן ביותר המכיל את כל M_i $1\le i\le k$ והוא מתאים לחבורה הגדולה ביותר המוכלת בכל H_i $1\le i\le k$, כלומר הוא מתאים ל- $\bigcap_{i=1}^{k} H_i$.

(ב) G חבורה ו- $H\le G$ תת חבורה. תת החבורה הנורמלית המקסימלית המוכלת ב- H היא $\bigcap_{\sigma\in G}\sigma H\sigma^{-1}$. אזי

$$\begin{tikzcd}
M=E^H \arrow[r, leftrightarrow] & H \\
L=E^N \arrow[r, leftrightarrow] \arrow[u, phantom, "\cap"] & \bigcap_{\sigma\in G}\sigma H\sigma^{-1}=N \arrow[u, phantom, "\cup"]
\end{tikzcd}$$

L/F הרחבה נורמלית מינימלית המכילה את M ב- E.
לפעמים קוראים ל- L הסגור הנורמלי של M ב- E.

<u>טענה</u>: $V\supseteq E\supseteq F$, $V\supseteq L\supseteq F$. נניח ש- E/F הרחבת גלואה. אזי EL/L ו- $E/E\cap L$ הרחבות גלואה ומתקיים

$$Gal(EL/L)\cong Gal(E/E\cap L)$$

$$\begin{tikzcd}
 & V \\
 & EL \arrow[u, phantom, "\cup"] \\
E \arrow[ur, dash] & & L \arrow[ul, dash] \\
 & E\cap L \arrow[ul, dash] \arrow[ur, dash] \\
 & F \arrow[u, dash]
\end{tikzcd}$$

<u>הוכחה</u>: מדוע EL/L גלואה? ידוע ש- E/F גלואה ולכן קיים פולינום ספרבילי $f\in F[x]$ כך ש- E שדה פיצול של f. $F\subseteq L$ ולכן $f\in L[x]$ ושדה הפיצול שלו מכיל את L ומכיל את E ולכן הוא EL. לכן EL/L גלואה. באותו אופן $E/E\cap L$ גלואה.

נתבונן בחבורה $Gal(EL/L)$ ויהי $\sigma = Gal(EL/L)$.

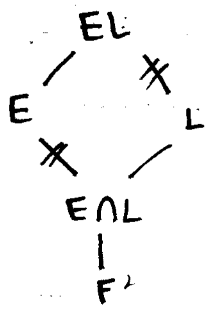
אזי $\sigma|_L = id$. אם $a \in E$ אז $\sigma a \in E$ כי אם $\sigma|_L = id_L$ אז $\sigma|_F = id_F$ ולכן σ שומר את f במקום ולכן מעתיק את שדה הפיצול של f לעצמו, כלומר $\sigma(E) = E$.

לכן צמצום σ ל- E הוא הומומורפיזם $Gal(EL/L) \to Gal(E/E \cap L)$

ניתן להראות שהומומורפיזם זה הוא חח"ע ועל.

מחר. או תרגיל...

1/7/08
מבנים



<u>טענה</u>: $F\subseteq E\subseteq V$, $F\subseteq L\subseteq V$.

נניח ש- E/F הרחבת גלואה. אזי EL/L

! - $E/E\cap L$ הרחבות גלואה ! $\mathrm{Gal}(EL/L)\cong\mathrm{Gal}(E/E\cap L)$

<u>הוכחה</u>: E שדה פיצול של פולינום ספרבילי $f\in F[x]$

אזי EL שדה הפיצול של הפולינום הספרבילי $f\in L[x]$

$\Leftarrow$ EL/L הרחבת גלואה. E הוא שדה הפיצול של $f\in(E\cap L)[x]$

אזי $E/E\cap L$ הרחבת גלואה.

כעת, יהי $\sigma\in\mathrm{Gal}(EL/L)$. היות ש- $F\subseteq L$! $f\in F[x]$ נקבל ש-

σ מעתיק את שורשי f לעצמם (בקבוצה) $\Leftarrow$ $\sigma(E)=E$.

נשים ♥ ש- $\sigma|_{E\cap L}=id|_{E\cap L}$ אזי $\sigma|_E\in\mathrm{Gal}(E/E\cap L)$. לכן

קיבלנו הומומורפיזם

$$\varphi:\mathrm{Gal}(EL/L)\longrightarrow\mathrm{Gal}(E/E\cap L)$$
$$\sigma\longmapsto\sigma|_E$$

נותר להראות ש- φ חח"ע ועל.

• חח"ע: נניח $\sigma\in\mathrm{Gal}(EL/L)$ כך ש- $\sigma|_E=id_E$ (כלומר $\sigma\in\ker\varphi$)

אבל גם $\sigma|_L=id_L$ (כי $\sigma\in\mathrm{Gal}(EL/L)$) אזי $\sigma|_{EL}=id|_{EL}$ אזי

φ חח"ע.

• על: רוצים להראות ש- $H=\varphi(\mathrm{Gal}(EL/L))\le\mathrm{Gal}(E/E\cap L)$ מקיימת

$H=\mathrm{Gal}(E/E\cap L)$. נראה ששדה השבת של H ב- E הוא $E\cap L$

וזה יספיק (לפי המשפט היסודי של תורת גלואה). יהי $\alpha\in E$ כך

ש- α מיוצב ע"י כל איברי $H=\varphi(\mathrm{Gal}(EL/L))$, כלומר לכל $\varphi\in\mathrm{Gal}(EL/L)$

מתקיים $\sigma(\alpha)=\alpha$ $\Leftarrow$ $\alpha\in L$ $\Leftarrow$ $\alpha\in E\cap L$. ☺

<u>טענה</u>: נניח שבנוסף לתנאים של הטענה הקודמת מתקיים גם ש- L/F הרחבה

סופית. אזי $$[EL:F]=\frac{[E:F][L:F]}{[E\cap L:F]}$$

<u>הוכחה</u>: מהכפליות $$[EL:F]=[EL:L][L:F]$$

מהאיזומורפיזם $$[EL:L]=[E:E\cap L]$$

ומהכפליות $$[E:E\cap L]=\frac{[E:F]}{[E\cap L:F]}$$

לכן $$[EL:F]=\frac{[E:F][L:F]}{[E\cap L:F]}$$ ☺

שאלה: האם חייבים להניח ש-E הרחבת גלואה?

טענה: נניח $F \subsetneq E_1 \subseteq V$, $F \subseteq E_2 \subseteq V$ רק ש-E_i/F הרחבות גלואה. אזי E_1E_2/F הרחבת גלואה ותמונת ההומומורפיזם

$$Gal(E_1E_2/F) \longrightarrow Gal(E_1/F) \times Gal(E_2/F)$$
$$\sigma \longmapsto (\sigma|_{E_1}, \sigma|_{E_2})$$

היא $H = \{ (\sigma_1, \sigma_2) \in Gal(E_1/F) \times Gal(E_2/F) : \sigma_1|_{E_1 \cap E_2} = \sigma_2|_{E_1 \cap E_2} \}$
כמובן, ההתאמה זו היא חח"ע.

הערה: אם נתונות זוג חבורות G_1, G_2 והומומורפיזמים $\varphi_i : G_i \to K$ אזי הקבוצה $\{(g_1, g_2) \in G_1 \times G_2 : \varphi_1(g_1) = \varphi_2(g_2)\}$ היא תת-חבורה (הבדיקה טריוויאלית)

הוכחת הטענה: E_i הוא שדה הפיצול של פולינום ספרבילי $f_i \in F[x]$ $\Leftarrow$ E_1E_2 הוא שדה הפיצול של הפולינום הספרבילי $f = f_1 f_2$ ולכן E_1E_2/F הרחבת גלואה.

אותו שיקול כמו קודם מראה שעבור $\sigma \in Gal(E_1E_2/F)$ מתקיים $\sigma(E_i) = E_i$ ולכן מקבלים הומומורפיזם $\rho : \sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2}) \in Gal(E_1/F) \times Gal(E_2/F)$
ברור שתמונת ρ מוכלת ב-H שהרי $\sigma|_{E_1}|_{E_1 \cap E_2} = \sigma|_{E_1 \cap E_2} = \sigma|_{E_2}|_{E_1 \cap E_2}$
קיבלנו ש-ρ היא הומומורפיזם $\rho : Gal(E_1E_2/F) \to H$. רוצים להראות שזה איזומורפיזם.

- חח"ע: נובע מההגדרה. נתבונן בגרעין של ρ. $\sigma \in \ker \rho$ פירושו $\sigma|_{E_1} = id_{E_1}$ ו- $\sigma|_{E_2} = id_{E_2}$ $\Leftarrow$ $\sigma|_{E_1E_2} = id_{E_1E_2}$. לכן $\ker \rho = \{id\}$ וזה העתקה חח"ע.
- על: נעשה זאת ע"י ספירה. (יש לנו העתקה חח"ע בין קבוצות סופיות. אם גודלן שווה אז בהכרח ההעתקה על) ראשית נטען ש-$E_1 \cap E_2/F$ הרחבת גלואה. (ראה שזו הרחבה ספרבילית ונורמלית (ונובע מכך ש-E_i/F ספרבילית). יהי $a \in E_1 \cap E_2$ ויהי f הפולינום המינימלי המתוקן של a מעל F. ל-f יש $\deg f$ שורשים ב-E_1, ויש $\deg f$ שורשים ב-E_2 ו- $\deg f$ שורשים ב-E_1E_2. לכן כל $\deg f$ שורשי f נמצאים ב-$E_1 \cap E_2$ ולכן f מתפצל ב-$(E_1 \cap E_2)[x]$, וקיבלנו ש-$E_1 \cap E_2/F$ גלואה (וזה נומ"א נורמלית וספרבילית)

(31)

לפי משפט קודם

$$Gal(E_1 \cap E_2 / F) \cong Gal(E_2/F) / Gal(E_2 / E_1 \cap E_2)$$

נניח $(\sigma_1, \sigma_2) \in H$. נסמן $\tau = \sigma_1|_{E_1 \cap E_2} \in Gal(E_1 \cap E_2 / F)$.

אז לכל $\sigma_1|_{E_1 \cap E_2} \in Gal(E_1 \cap E_2 / F)$ יש $|Gal(E_2 / E_1 \cap E_2)|$ מקורות ב- $Gal(E_2/F)$. לכן

$$H = \{ (\sigma_1, \sigma_2) : \tau = \sigma_1|_{E_1 \cap E_2} = \sigma_2|_{E_1 \cap E_2} \}$$

$$\Rightarrow |H| = |Gal(E_1 \cap E_2 / F)| \, |Gal(E_2 / E_1 \cap E_2)|$$

המשך אחר.

㉜ 7/7/08

מבנים

טענה: יהי F שדה. $E_1, E_2 \supseteq F$ הרחבות של F שמוכלות באיזושהי הרחבה משותפת. אם E_1/F ו- E_2/F הרחבות גלואה אז גם E_1E_2/F ו- $E_1\cap E_2/F$ הרחבות גלואה וההומומורפיזם

$$\varphi: Gal(E_1E_2/F) \longrightarrow Gal(E_1/F)\times Gal(E_2/F)$$
$$\sigma \longmapsto (\sigma|_{E_1}, \sigma|_{E_2})$$

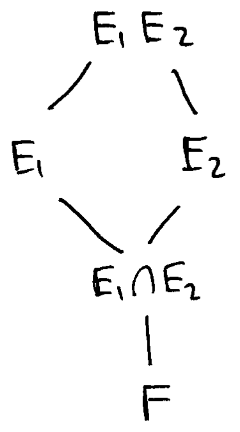
הוא חח"ע ותמונתו היא תת החבורה

$$H=\{(\sigma_1,\sigma_2)\in Gal(E_1/F)\times Gal(E_2/F) : \sigma_1|_{E_1\cap E_2} = \sigma_2|_{E_1\cap E_2}\}$$

הוכחה: יש $f_i \in F[X]$ פולינום ספרבילי כך ש- E_i שדה הפיצול של f_i מעל F. אז E_1E_2 שדה הפיצול של f_1f_2 מעל F. $\Leftarrow$ E_1E_2/F הרחבת גלואה.

אם $\sigma\in Gal(E_1E_2/F)$ אז σ מקבע את F וקודמת לכן $\sigma f_i = f_i$ לכן σ מעביר את קבוצת שורשי f_i לעצמה לכן $\sigma E_i = E_i$ ונוכל לצמצם את σ ל- $\sigma|_{E_i}$.

φ חח"ע כי אוטומורפיזם $\sigma: E_1E_2\to E_1E_2$ נקבע ע"י הצמצום שלו ל- E_1 ול- E_2 שהרי E_1 ו- E_2 יוצרים את E_1E_2.



ברור שתמונת φ מוכלת ב- H כי

$$(\sigma|_{E_1})|_{E_1\cap E_2} = \sigma|_{E_1\cap E_2} = (\sigma|_{E_2})|_{E_1\cap E_2}$$

נותר להראות שתמונת φ היא H. נראה זאת משיקולי ספירה.

טענת עזר: $E_1\cap E_2/F$ הרחבה נורמלית ספרבילית.

הוכחה: יהי $\alpha\in E_1\cap E_2$ ויהי $f\in F[X]$ פולינום מינימלי עבור α.

ל- f יש: $\deg f$ שורשים ב- E_1

$\deg f$ שורשים ב- E_2

$\deg f$ שורשים ב- E_1E_2

$\Leftarrow$ ט $\deg f$ שורשי f נמצאים ב- $E_1\cap E_2$

לכן $E_1\cap E_2/F$ הרחבה נורמלית.

$$\begin{tikzcd} E_2 \arrow[d, dash] \\ E_1\cap E_2 \arrow[d, dash] \\ F \end{tikzcd}$$

מהמשפט היסודי של תורת גלואה נובע ש-

$$Gal(E_1\cap E_2/F) \cong Gal(E_1/F)/Gal(E_2/E_1\cap E_2)$$

והאיזומורפיזם נתון ע"י צמצום $\tau\in Gal(E_1/F)$ ל- $\tau|_{E_1\cap E_2}$.

נחזור להוכחת הטענה:

$$H=\{(\sigma_1,\sigma_2)\in Gal(E_1/F)\times Gal(E_2/F) : \underset{\substack{\Cap \\ Gal(E_1\cap E_2/F)}}{\sigma_1|_{E_1\cap E_2}} = \sigma_2|_{E_1\cap E_2}\}$$

לכן מספר המקורות $\sigma_2\in Gal(E_2/F)$ ל- $\sigma_1|_{E_1\cap E_2}$ הוא $|Gal(E_2/E_1\cap E_2)|$. לכן

$$|H| = \underset{\uparrow}{|Gal(E_1/F)|}\,\underset{\uparrow}{|Gal(E_2/E_1\cap E_2)|} = [E_1:F][E_2:E_1\cap E_2] =$$

מספר הדרכים לבחור $\sigma_1\in Gal(E_1/F)$

בהינתן $\sigma_1\in Gal(E_1/F)$ מספר הדרכים לבחור $\sigma_2\in Gal(E_2/F)$ כך ש- $\sigma_1|_{E_1\cap E_2}=\sigma_2|_{E_1\cap E_2}$

$$= \frac{[E_1:F][E_2:F]}{[E_1\cap E_2:F]} \underset{\substack{\downarrow \\ \text{טענה קודמת}}}{=} [E_1E_2:F] = |Gal(E_1E_2/F)|$$

לכן ההומומורפיזם התח"ס φ חייב להיות על! ☺

<u>תזכורת</u>: $\alpha\in\mathbb{R}$ ניתן לבנייה באמצעות סרגל ומחוגה אמ"מ קיימים $a_1,\dots,a_n\in\mathbb{R}$ כך ש- $\alpha\in\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_n})$ ולכל $1\le i\le n$ $a_i\in\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_{i-1}})$

<u>מסקנה</u>: אם $\alpha\in\mathbb{R}$ ניתן לבנייה אז $[\mathbb{Q}(\alpha):\mathbb{Q}]=2^k$

<u>הערה</u>: הכיוון ההפוך אינו נכון!!!

משפט: אם $\alpha\in\mathbb{R}$ שייך להרחבת גלואה $E/\mathbb{Q}$ כך ש- $[E:\mathbb{Q}]=2^k$ אזי α ניתן לבניה באמצעות סרגל ומחוגה.

הוכחה: די להראות קיום שרשרת של שדות חלקיים

$$E_0=\mathbb{Q}\subseteq E_1\subseteq E_2\subseteq\ldots\subseteq E_k$$

כך ש- $[E_i:E_{i-1}]=2$.

מציאת שרשרת כזו שקולה למציאת שרשרת של תתי חבורות

$$G_0=G\geq G_1\geq G_2\geq\ldots\geq G_k=\{1\}$$

כאשר $G=Gal(E/\mathbb{Q})$ ו- $[G_{i-1}:G_i]=2$.

הנתון אומר ש- $|G|=2^k$. נזכור שחבורות מסדר p^r (בפרט 2^k) הן נילפוטנטיות, כלומר הסדרה העולה של תתי חבורות נורמליות

$Z_0=\{1\}$ $\quad Z_1=Z(G)$

$Z_i\leq G$ היא תת חבורה כך ש- Z_i/Z_{i-1} מרכז של G/Z_{i-1}

מתייצבת עבור $m\in\mathbb{N}$ מספיק גדול, כלומר $Z_m=G$.

$$Z_m=G\geq Z_{m-1}\geq Z_{m-2}\geq\ldots\geq Z_1\geq Z_0=\{1\}$$

היות של- Z_i/Z_{i-1} אבלית מסדר 2^{r_i} ניתן לעדן את השרשרת ולהוסיף תתי חבורות נוספות כך שנקבל

$$G=G_0\geq G_1\geq\ldots\geq G_k=\{1\}\qquad [G_{i-1}:G_i]=2$$

וזה מה שרצינו. ☺

תרגיל: **מסקנה:** יהי p ראשוני כך ש- $p=2^k+1$ (זה גורר ש- $k=2^r$). אזי ניתן לבנות מצולע משוכלל בן p צלעות.

יהי F שדה ויהי $f\in F[x]$ פולינום ספרבילי. נסמן ב- $E=F_f$ את שדה הפיצול של f מעל F. חבורת גלואה של f מוגדרת להיות $G_f=Gal(F_f/F)$. נסמן ב- $\alpha_1,\ldots,\alpha_d$ את שורשי הפולינום f. אזי $E=F_f=F(\alpha_1,\ldots,\alpha_d)$

אם $\sigma\in G_f=Gal(E/F)$ אזי σ מעתיק את $\{\alpha_1,\ldots,\alpha_d\}$ לעצמה ונקבע ע"י $\sigma|_{\{\alpha_1,\ldots,\alpha_d\}}$. כלומר, ניתן לזהות את חבורת גלואה $Gal(E/F)$ כתת חבורת תמורות של $\{\alpha_1,\ldots,\alpha_d\}$,

כלומר כתת חבורה של $\mathrm{Sym}\{\alpha_1,\dots,\alpha_d\}$

משפט: יהי p ראשוני. אזי קיים פולינום $f\in\mathbb{Q}[X]$ ממעלה p כך ש- $G_f\cong S_p$.

הוכחה: אם $\deg f=p$ אז חבורת גלואה של מוכלת ב- S_p. אם $f\in\mathbb{Q}[X]$ פולינום אי פריק ממעלה p כך שיש ל- f p שורשים שונים $\alpha_1,\dots,\alpha_{p-2},\alpha_{p-1},\alpha_p\in\mathbb{C}$ כך ש- $\{\alpha_1,\dots,\alpha_{p-2}\}\subseteq\mathbb{R}$; $\alpha_{p-1},\alpha_p\notin\mathbb{R}$ אזי ההעתקה $\mathbb{C}\to\mathbb{C}$, $z\mapsto\bar{z}$ משרה איבר $\sigma\in Gal(E/\mathbb{Q})$ כאשר $E=\mathbb{Q}(\alpha_1,\dots,\alpha_p)$; $\sigma|_{\{\alpha_1,\dots,\alpha_{p-2}\}}=id|_{\{\alpha_1\dots\alpha_{p-2}\}}$; $\sigma(\alpha_{p-1})=\alpha_p=\overline{\alpha_{p-1}}$ - $\sigma(\alpha_p)=\alpha_{p-1}=\overline{\alpha_p}$

נטען ש- $S_p=\langle(i_0,j_0),(k_1,k_2,\dots,k_p)\rangle$ כלומר כל טרנספוזיציה ב- S_p וציקלוס באורך p יוצרים את S_p עבור p ראשוני. ע"י שינוי שמות ניתן להניח ש- $i_0=1$; $j_0=2$, כלומר נתונים השחלוף $(1\,2)$ ומחזור כלשהו באורך p. מספיק להוכיח שאפשר לייצר מחזור מהצורה $(1\,2\,\dots)$ כי ידוע ממבנים 1 ש- $S_p=\langle(1\,2),(1\,2\dots)\rangle$. נסמן $f=(k_1,k_2,\dots,k_p)$. בה"כ $k_1=1$. תכונה של מחזורים באורך ראשוני היא שכשמעלים אותו בחזקה נשארים עם ציקלוס באותו אורך. אז נניח ש- $k_j=2$. אז $f^{j-1}=(1\,2,\dots)$ וזה מה שרצינו.

נשים לב כעת שאם $f\in\mathbb{Q}[X]$ אי פריק ממעלה p אז $|G_f|$ מתחלק ב- p: יהי α_1 שורש של f. $\mathbb{Q}\subseteq\mathbb{Q}(\alpha_1)\subseteq E$ לכן

$$|G_f|=[E:\mathbb{Q}]=[E:\mathbb{Q}(\alpha_1)]\underbrace{[\mathbb{Q}(\alpha_1):\mathbb{Q}]}_{=p}$$

משפט קושי אומר שקיים איבר מסדר p ב- $G_f=Gal(E/\mathbb{Q})$ ואיבר כזה הוא ציקלוס באורך p.

נותר להראות שפולינום כזה אכן קיים. ברור שהפולינום יהיה מהצורה

$$(x-a_1)(x-a_2)\dots(x-a_{p-2})(x^2+k)$$

כאשר $a_1,\dots,a_{p-2}\in\mathbb{Q}$ שונים זה מזה ; $0<k\in\mathbb{Q}$.

עכשיו צריך לדאוג שהוא יהיה אי-פריק.

(34) נבחר $a_1, \dots, a_{p-2} \in \mathbb{Z}$ זוגיים שונים. כלומר $a_i = 2m_i$

ו- $m_i \in \mathbb{Z}$. אז

$$g(x) = (x-2m_1)(x-2m_2)\dots(x-2m_{p-2})(x^2+2m)$$

כאשר $0 < m \in \mathbb{N}$.

נבחר $r \in \mathbb{Q}$ קש- $0 < |r| < \min_{f'(t)=0} |f(t)| > 0$

אז ל- $f = g(x) + r$ יש בדיוק $p-2$ שורשים ממשיים.

נבחר $\min_{f'(t)=0} |f(t)| > r = \frac{2}{2d+1}$ ונקבל ב-

$$f(x) = g(x) + \frac{2}{2d+1}$$

נטען שהפולינום f אי פריק מעל $\mathbb{Q}$. נסמן $g(x) = \sum_{i=0}^{k} b_i x^i$

כאשר $b_p = 1$ וכל שאר ה-b_i זוגיים. אז

$$(2d+1)f(x) = (2d+1)x^p + (2d+1)\sum_{i=1}^{p-1} b_i x^i + \underbrace{(2d+1)b_0+2}_{c_0}$$

אז c_0 זוגי אבל $4 \nmid c_0$. אז לפי קריטריון אייזנשטיין עם $p=2$ הפולינום אי-פריק.

קיבלנו פולינום $f \in \mathbb{Z}[x]$ ממעלה p עם מקדם עליון אי-זוגי. כל שאר המקדמים זוגיים ומקדם חופשי זוגי שאינו מתחלק ב-4. $\Rightarrow$ בעזרת קריטריון אייזנשטיין f אי-פריק מעל $\mathbb{Q}$.

(35) 8/7/08
מבנים

בהינתן חבורה סופית H איך נמצא הרחבת גלואה E/F כך ש- $Gal(E/F) \cong H$?

מהינתן H קיים ראשוני p ושיכון של H ב- S_p. יהי $f \in \mathbb{Q}[X]$ פולינום כך ש- $G_f \cong S_p$ = חבורת גלואה של E (הפיצול) של f מעל $\mathbb{Q}$

נגדיר F = שדה השבת של $H \leq Gal(E/\mathbb{Q})$ ב- E. אזי $H \cong Gal(E/F)$.

ראינו שעבור פולינום $f \in F[X]$ מדרגה n, G_f משוכנת בחבורת התמורות של שורשי f (כלומר ב- S_n).

<u>שאלה</u>: נניח ש- f פולינום ספרבילי. מתי $G_f \subseteq A_n$? $f \in F[X]$. נסמן ב- $\alpha_1, \dots, \alpha_n$ את שורשי f בשדה הפיצול. אז $G_f \subseteq S_{\{\alpha_1, \dots, \alpha_n\}}$. נגדיר:

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$$
$$D(f) = \Delta(f)^2 = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

$D(f)$ נקרא הדיסקרימיננטה של f.

עבור $\sigma \in Gal(E/F)$ מתקיים $\sigma(D(f)) = D(f)$ שהרי σ תמורה של השורשים:

$$\sigma(D(f)) = \sigma\Big(\prod_{1 \leq j < j \leq n} (\alpha_i - \alpha_j)^2\Big) = \prod_{1 \leq i < j \leq n} (\sigma(\alpha_i) - \sigma(\alpha_j))^2 =$$
$$\underset{\sigma \text{ תמורה}}{=} \prod_{k<l} (\alpha_k - \alpha_l)^2 = D(f)$$

ואילו $\sigma(\Delta(f)) = \text{sign}\,\sigma \cdot \Delta(f)$

(למעשה, בשנה א' ככה הגדרנו סימן של תמורה)

<u>מסקנה</u>: $A_n \supseteq Gal(E/F)$ אמ"מ $\Delta(f) = \sigma(\Delta(f))$ לכל $\sigma \in Gal(E/F)$

אמ"מ $\Delta(f) \in F$ אמ"מ

ל- $D(f) \in F$ יש שורש ריבועי ב- F.

טענה: יהי f פולינום מתוקן. $D(f)$ היא פונקציה פולינומיאלית במקדמי f.

דוגמה: $n=2$

$$f=(x-\alpha_1)(x-\alpha_2)=$$
$$=x^2-(\alpha_1+\alpha_2)x+\alpha_1\alpha_2$$
$$=x^2-c_1x+c_2$$
$$\downarrow$$
$$c_1=\alpha_1+\alpha_2$$
$$c_2=\alpha_1\alpha_2$$
$$\Rightarrow D(f)=(\alpha_1-\alpha_2)^2=\alpha_1^2+\alpha_2^2-2\alpha_1\alpha_2=$$
$$=c_1^2-4c_2$$

באופן כללי

$$(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)=$$
$$=\sum_{i=0}^{n}(-1)^i c_i x^{n-i}$$

$$c_0=1$$
$$c_1=\alpha_1+\alpha_2+\dots+\alpha_n$$
$$c_2=\sum_{i<j}\alpha_i\alpha_j$$
$$\vdots$$
$$c_n=\alpha_1\dots\alpha_n$$

הגדרה: פולינום $p(x_1,\dots,x_n)$ יקרא סימטרי אם לכל $\sigma\in S_n$ $p(x_1\dots x_n)=p(x_{\sigma(1)},\dots,x_{\sigma(n)})$

אוסף הפולינומים הסימטריים: $F[x_1,\dots,x_n]^{S_n}$

זהו חוג!

עבור $0\le k\le n$ נגדיר

$$F[x_1,\dots,x_n]\ni C_k(x_1,\dots,x_n)=\sum_{1\le i_1<\dots<i_k\le n}x_{i_1}\dots x_{i_k}$$

נשים לב ש- $C_k(x_1,\dots,x_n)\in F[x_1,\dots,x_n]^{S_n}$

משפט: חוג הפולינומים הסימטריים ב- n משתנים נוצר ע"י $\{C_k(x_1,\dots,x_n)\}_{0\le k\le n}$.

אינטואיציה: F שדה ; חוג $R_n = F[x_1,\dots,x_n]$ הפולינומים ב-n משתנים מעל F.

S_n פועלת על $F[x_1,\dots,x_n]$ באופן הבא: אם $\sigma\in S_n$; $p(x_1\dots x_n)\in R_n$ - אז

$$\sigma(p)(x_1\dots x_n) = p(x_{\sigma^{-1}(1)},\dots,x_{\sigma^{-1}(n)})$$

$$R_n^{S_n} = \{p\in R_n : \sigma(p)=p \ \forall\sigma\in S_n\} -$$

$$=\{p\in R_n : p(x_{\sigma^{-1}(1)},\dots,x_{\sigma^{-1}(n)}) = p(x_1,\dots,x_n) \ \forall\sigma\}$$

קל לראות ש $c_k(x_1,\dots,x_n)$ עבור $0\le k\le n$ כולם ב-$R_n^{S_n}$.

משפט: המשפט היסודי של פולינומים סימטריים.

$R_n^{S_n}$ = החוג הנוצר מעל F ע"י $\{c_k(x_1,\dots,x_n)\}_{0\le k\le n}$

רעיון ההוכחה: באינדוקציה על מספר המשתנים ועל מעלת הפולינום.

$$\deg(x_1^{r_1}\cdots x_n^{r_n}) = r_1+\dots+r_n$$

פולינום $p(x_1\dots x_n) = \sum_{r_1\dots r_k} a_{r_1\dots r_n} x^{r_1}\dots x^{r_n}$ (הסכום סופי!!)
ייקרא פולינום הומוגני ממעלה m אם כל המחוברים מקיימים $r_1+\dots+r_n=m$.

בהינתן פולינום p ניתן להציגו כסכום (סופי) של פולינומים הומוגניים. $p=\sum_{i=0}^{M} q_i$ כאשר $M=\deg p$
כל q_i פולינום הומוגני מדרגה i.

p סימטרי אמ"מ q_i סימטרי לכל $0\le i\le \deg p = M$
די להראות שכל פולינום הומוגני סימטרי שייך לחוג הנוצר ע"י $c_0,\dots,c_n$. המשפט מוכח באינדוקציה על המעלה (עבור פולינומים סימטריים הומוגניים).

(34) 14.7.08
מבנים

$f \in F[x]$ ספרבילי. E שדה פיצול. $G_f = Gal(E/F)$ משוכנת בחבורת התמורות של שורשי f.

שאלה: מתי G_f מוכלת ב- A_n (חבורת התמורות הזוגיות)?

נסמן ב- $\alpha_1, \dots, \alpha_n$ את שורשי f ונגדיר

$$D(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

$$\Delta f = \sqrt{D(f)} = \prod_{i<j} (\alpha_i - \alpha_j)$$

ראינו ש- $G_f \subseteq A_n$ אמ"מ $\Delta(f) \in F$.

$D(f)$ הוא פולינום סימטרי ב- $\alpha_1, \dots, \alpha_n$ ומתקיים

$$F(x_1, \dots, x_n)^{S_n} = F(c_0, c_1, \dots, c_n)$$

כאשר $c_k = \sum_{i_1 < \dots < i_k} x_{i_1} \cdots x_{i_k}$ הפולינומים הסימטריים היסודיים.

לכן $D(f)$ פולינום במקדמים של f.

טענה: יהי $f \in F[x]$ פולינום עם שורשים פשוטים בלבד. אזי f אי-פריק אמ"מ $Gal(E/F)$ פועלת טרנזיטיבית על שורשי f כאשר E שדה הפיצול של f.

הוכחה: [פעולה טרנזיטיבית פירושו שלכל זוג שורשים α, β של f קיים $\sigma \in G_f$ כך ש- $\sigma(\alpha) = \beta$]

נניח ש- f אי-פריק ויהיו α, β שורשים של f. אז

$$F(\alpha) \cong F[x]/(f) \cong F(\beta)$$

לכן אפשר לקבל איזומורפיזם $\varphi : F(\alpha) \to F(\beta)$ שמקבע את F. אפשר להרחיב את φ ל- F-איזומורפיזם מ- $E = F(\alpha_1, \dots, \alpha_n)$ ל- $E = F(\alpha_1, \dots, \alpha_n)$. בהרחבה זו α עובר ל- β, אז קיבלנו $\sigma \in G_f$ כך ש- $\sigma(\alpha) = \beta$.

מאידך, נניח ש- f פריק ונראה שהפעולה לא טרנזיטיבית. נניח ש- $f = gh$ כאשר $1 \le \deg g < \deg f$ ו- $1 \le \deg h < \deg f$ עבור $g, h \in F[x]$. כל $\sigma \in G_f$ מעתיק את g לעצמו ולכן מעתיק את שורשי g לשורשי g. אבל קבוצת השורשים של g

היא קבוצה חלקית ממש לקבוצת השורשים של f. לכן G_f אינה טרנזיטיבית. ☺

הגדרה: הרחבה סופית E/F תיקרא הרחבה פשוטה אם $E=F[\alpha]$.

משפט: יהי F שדה ! $E=F[\alpha_1,\dots,\alpha_r]$ הרחבה סופית כך ש- $\alpha_2,\dots,\alpha_r$ ספרבליים (כלומר הפולינומים המינימליים שלהם ספרבליים) אזי קיים $\gamma\in E$ כך ש- $E=F[\gamma]$.

הוכחה: מספיק להראות שאם β ספרבלי (כלומר הפולינום המינימלי של β ספרבלי) אזי $F[\alpha,\beta]=F[\gamma]$ עבור איזה γ.

מקרה 1: F (ולכן גם E) שדה סופי. E שדה סופי. לכן E^* חבורה ציקלית. כלומר, קיים $\gamma\in E$ כך ש- $E=\{0,1,\gamma,\gamma^2,\dots,\gamma^k\}=F[\gamma]$.

מקרה 2: נניח ש- F שדה אינסופי. נראה שקיים $c\in F$ כך ש- $\gamma=\alpha+c\beta$ מקיים $F[\gamma]=F[\alpha,\beta]$ (ההכלה $\subseteq$ מתקיימת תמיד). α אלגברי מעל F. יהי $f\in F[x]$ הפולינום המינימלי של α ויהיו $\alpha=\alpha_1,\dots,\alpha_n$ שורשי f. β אלגברי מעל F. יהי g הפולינום המינימלי של β ויהיו $\beta=\beta_1,\dots,\beta_m$ שורשי g. נזכור ש- g ספרבלי. אזי $g=\prod_{i=1}^{m}(x-\beta_i)$
הקבוצה $\left\{\frac{\alpha_i-\alpha_j}{\beta_k-\beta_l}:k\neq l\right\}\subset F[\alpha,\beta]$ סופית. היות ש- F אינסופי קיים $c\in F$ כך ש- c לא בקבוצה הזאת. נובע ש- $\alpha+c\beta\neq\alpha_i+c\beta_j$ אלא אם $i=j=1$ (אם יש שוויון נקבל $c=\frac{\alpha_i-\alpha}{\beta-\beta_j}$). נסמן $\gamma=\alpha+c\beta$. נתבונן בפולינומים $g(x)\in F[\gamma][x]$, $h(x)=f(\gamma-cx)\in F[\gamma][x]$
מתקיים $g(\beta)=0$ וגם $h(\beta)=f(\gamma-c\beta)=f(\alpha)=0$
$\Leftarrow$ $x-\beta$ מחלק את ה gcd של h ו- g. נסמן $p(x)=gcd(g,h)$. אזי $p(x)\in F[\gamma][x]$. נשים לב ששורשי g הם בדיוק $\beta_1,\dots,\beta_m$ (g ספרבלי!). לכן שורשי $p(x)$ הם מתוך הקבוצה $\{\beta_1,\dots,\beta_m\}$
נניח שעבור $i\neq 1$ $0=h(\beta_i)=f(\gamma-c\beta_i)$. אז קיים $1\le j\le n$ כך ש- $\gamma-c\beta_i=\alpha_j$. אזי $\alpha+c\beta-c\beta_i=\alpha_j$ ולכן $\alpha+c\beta=\alpha_j+c\beta_i$ וזה לא ייתכן לפי בחירת c. לכן השורש היחידי של $p(x)$

נניח ו- $\beta_j = \beta$. קיבלנו ש- $p(x) = (x-\beta)^s$. אבל היות ש- $p(x)$ מחלק את $g(x)$ ו- g ספרבילי נובע ש- $s=1$. כלומר $p(x) = x-\beta$. אבל $p(x) \in F[\gamma][x]$ ולכן $\beta \in F[\gamma]$. והיות ש- $\gamma = \alpha + c\beta$ נובע $\alpha = \gamma - c\beta$ ולכן $\alpha \in F[\gamma]$. לכן $F[\alpha,\beta] \subseteq F[\gamma]$ וזה מה שרצינו. ☺

E/F הרחבה סופית פשוטה של F, כלומר $E = F[\alpha]$. כמה שדות ביניים $F \subseteq M \subseteq E$ יש?

<u>טענה</u>: תהי E/F הרחבה סופית פשוטה (כלומר $E = F(\alpha)$ ו- α אלגברי מעל F). אזי יש רק מספר סופי של שדות חלקיים $F \subseteq M \subseteq E$.

<u>הוכחה</u>: יהי $f \in F[x]$ פולינום מינימלי עבור α מעל F. יהי $F \subseteq M \subseteq E$ שדה חלקי. יהי $g \in M[x] \subseteq E[x]$ הפולינום המינימלי של α מעל M. נגדיר $F \subseteq M' \subseteq E$ את השדה הנוצר מעל F ע"י מקדמי g. ברור ש- $M' \subseteq M$. נראה ש- $M = M'$ ומכאן תנבע הטענה כי ל- f יש מספר סופי של גורמים ב- $E[x]$.
כדי להראות ש- $M = M'$ די להראות ש- $[E:M] = [E:M']$ כי ידוע ש- $M' \subseteq M$ ולכן $[E:M'] \geq [E:M]$. אבל $F[\alpha] = E = M[\alpha]$ ולכן $[E:M] = [M[\alpha]:M] = \deg g =$ מעלת הפולינום המינימלי. מאידך, גם $E = M'[\alpha]$ ולכן $[E:M'] = \deg g$ כי g הפולינום המינימלי עבור α מעל M'. ☺

פולינומים ציקלוטומיים

יהי F שדה. נתבונן בכל שורשי היחידה מסדר n $\mu_n = \{\alpha \in E : \alpha^n = 1\}$ כאשר E שדה פיצול מעל F של $x^n - 1$. μ_n חבורה כפלית סופית ולכן μ_n חבורה ציקלית.
נניח שמציין F הוא 0 או p שזר ל- n. במקרים אלו $x^n - 1$ פולינום עם שורשים פשוטים.

קיים ζ שורש יחידה פרימיטיבי מסדר n, כלומר $\zeta^n=1$! ו-$\zeta^k\neq 1$ לכל $1\le k\le n-1$. אז $\{1,\zeta,\zeta^2,\dots,\zeta^{n-1}\}$ חבורה ציקלית באורך n. (סמן) $\Phi_n(x)=\prod\limits_{\substack{\zeta \text{ שורש} \\ \text{יחידה פרימיטיבי} \\ \text{מסדר } n}}(x-\zeta)\in E[X]$

פונקציית אוילר φ היא $\varphi(n)=\deg\Phi_n(x)$ (תרגיל!)

[תזכורת: $\varphi(n)=\#$ המספרים הזרים ל-n ב-$\mathbb{Z}_n$]

נטען ש-$\Phi_n\in F[X]$. מספיק להראות שעבור כל $\sigma\in Gal(E/F)$ כאשר E שדה הפיצול של x^n-1 $\sigma(\Phi_n)=\Phi_n$. אבל זה נכון כי כל σ הנ"ל מעבירה שורש פרימיטיבי ζ כי $\sigma(\zeta)$ שורש יחידה פרימיטיבי...

מתקיים $\sigma(\zeta)^i=\sigma(\zeta^i)$. אם $1\le i\le n-1$ אז $\zeta^i\neq 1$ מכאן $1\neq\sigma(\zeta^i)=\sigma(\zeta)^i$. כל ζ^i עבור $0\le i\le n-1$ הוא שורש יחידה מסדר n: $(\zeta^i)^n=(\zeta^n)^i=1^i=1$. כל ζ^i עבור $0\le i\le n-1$ הוא שורש יחידה פרימיטיבי מסדר d כאשר $d|n$

<u>המסקנה</u>: $x^n-1=\prod\limits_{i=0}^{n}(x-\zeta^i)=\prod\limits_{d|n}\Phi_d$

<u>דוגמה</u>: $n=6$

$$\prod_{i=0}^{5}(x-\zeta^i)=[(x-\zeta)(x-\zeta^5)][(x-\zeta^2)(x-\zeta^4)]\cdot$$
$$\cdot[x-\zeta^3][x-1]=\Phi_6\,\Phi_3\,\Phi_2\,\Phi_1=$$
$$=(x^2-x+1)(x^2+x+1)(x+1)(x-1)$$

<u>הגדרה</u>: Φ_n נקרא הפולינום הציקלוטומי ה-n-י.

עבור p ראשוני $\overbrace{\quad}^{\text{כי } x^p-1=\Phi_p\cdot\Phi_1}$ $\Phi_p=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\dots+x+1$. מהמסקנה קל לחשב באינדוקציה את Φ_n לכל n.

<u>משפט</u>: יהי F שדה ויהי $n\in\mathbb{N}$. אם $\text{char}F=0$ או $\text{char}F=p$ כאשר p זר ל-n, אז הטענות שקולות:

① Φ_n אי-פריק ב-$F[X]$ ② $\varphi(n)=[F[\zeta]:F]$ עבור ζ שורש פרימיטיבי מסדר n ③ $Gal(F[\zeta]/F)\longrightarrow Gal(\mathbb{Z}_n^*)$ העתקה על שמוגדרת ע"י $\sigma\mapsto k$ כאשר $\sigma(\zeta)=\zeta^k$.

<u>הוכחה</u>: Φ_n אי-פריק אמ"מ $[F[\zeta]:F]=\varphi(n)$ אמ"מ ההעתקה הנ"ל היא על (כי ברור ש-$\sigma\in Gal(F[\zeta]/F)$ נקבע ע"י $\sigma(\zeta)=\zeta^k$ ולכן חח"ע ולכן מתקיים שוויון בגדלים של החבורות אם ההעתקה היא על ושוויון זה פירושו $[F[\zeta]:F]=|Gal(F[\zeta]/F)|\underset{\text{כי על}}{=}|\mathbb{Z}_n^*|=\varphi(n)$

㊴ 15.7.08
מבנים

פולינומים ציקלוטומיים

F שדה. $\Phi_n = \prod_{\xi}(x-\xi) \in F[x]$

כאשר ξ שורש יחידה פרימיטיבי מסדר n בשדה פיצול של x^n-1.

משפט: עבור $F=\mathbb{Q}$ $\Phi_n \in \mathbb{Q}[x]$ אי-פריק.

הוכחה: נניח בשלילה ש- $\Phi_n = fg$, עבור $f,g \in \mathbb{Q}[x]$ מתוקנות $\neq 1$.
היות ש- $\Phi_n \in \mathbb{Z}[x]$ נובע שאפשר להניח כי הפירוק $\Phi_n = fg$ הוא ב- $\mathbb{Z}[x]$, כלומר $f,g \in \mathbb{Z}[x]$. מאחר ש- $f,g \neq 1$ קיים שורש יחידה פרימיטיבי מסדר n ξ_0 וקיים p ראשוני זר ל- n כך ש- $f(\xi_0)=0$, $f(\xi_0^p)\neq 0$: נשים לב שאוסף שורשי היחידה הפרימיטיביים מסדר n הוא מהצורה $\{\omega^i : i \in \mathbb{Z}_n^*\}$ כאשר $\omega = e^{\frac{2\pi i}{n}}$ (או כל שורש יחידה פרימיטיבי מסדר n אחר). יהי ξ שורש של f, כלומר $f(\xi)=0$. אם לכל $i \in \mathbb{Z}_n^*$ גם $f(\xi^i)=0$ אזי כל שורשי היחידה הפרימיטיביים היו שורשים של f והיינו מקבלים $f=\Phi_n$. לכן קיים $i \in \mathbb{Z}_n^*$ כך ש- $f(\xi^i)\neq 0$.

נרשום את i כמכפלת ראשוניים - $i = p_1^{e_1}\cdots p_k^{e_k}$ ונתבונן ב-

$$\underset{\substack{\shortparallel\\ \alpha_0}}{\xi},\ \underset{\substack{\shortparallel\\ \alpha_1}}{\xi^{p_1}},\ \underset{\substack{\shortparallel\\ \alpha_2}}{\xi^{p_1^2}},\ \dots,\ \xi^{p_1^{e_1}},\ \xi^{p_1^{e_1}p_2},\ \dots,\ \underset{\substack{\shortparallel\\ \alpha_m}}{\xi^{i}}$$

אז קיבלנו i כך ש- $f(\xi^i)\neq 0$. אבל אנחנו צריכים שיהיה ראשוני. נסתכל ברשימה שלנו. יש מקום ראשון j כך ש- $f(\alpha_j)\neq 0$ ולכל אלה שלפניו $f(\alpha_l)=0$. אז נסמן $\xi_0 = \alpha_{j-1}$. זה שורש יחידה פרימיטיבי כי הוא התקבל מ- ξ ע"י העלאה בחזקה שזרה ל- n. ואז α_j הוא α_{j-1}^p עבור p ראשוני (לפי הבנייה של הסדרה) ומתקיים $f(\xi_0^p)=0$.
אז ישנו $\Phi_n = fg$ עבור $f,g \in \mathbb{Z}[x]$; ξ_0 - שורש יחידה פרימיטיבי מסדר n; p - ראשוני זר ל- n כך ש- $f(\xi_0)=0$; $f(\xi_0^p)\neq 0$. ξ_0^p הוא שורש יחידה פרימיטיבי מסדר n ולכן $\Phi_n(\xi_0^p)=0$. $\Rightarrow g(\xi_0^p)=0$. נגדיר פולינום $h(x)\in\mathbb{Z}[x]$ ע"י $h(x)=g(x^p)$. מתקיים $h(\xi_0)=g(\xi_0^p)=0$. לכן $x-\xi_0$ מחלק הן את f והן את h ולכן $\gcd(f,h)=g(x)\neq 1$

נתבונן בהעתקה $\mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$, $w(x) \mapsto \bar{w}(x)$. נניח ש- $\gcd(\bar{f},\bar{h}) \neq 1$ כי $\bar{g}$ (פולינום מתוקן) מחלק הן את $\bar{f}$ והן את $\bar{h}$. קיבלנו $\gcd(\bar{f},\bar{h}) \neq 1$.
נזכור ש- $h(x)=g(x^p)$ ולכן $\bar{h}(x)=\bar{g}(x^p)=(\bar{g}(x))^p$ ולכן $\gcd(\bar{f},(\bar{g}(x))^p) \neq 1$
$\Leftarrow \gcd(\bar{f},\bar{g}) \neq 1$. אבל $\bar{\Phi}_n = \bar{f}\bar{g}$ וקיבלנו ש- $\bar{\Phi}_n$ יש
שורשים כפולים בשדה פיצול מעל $\mathbb{Z}_p$. אבל $\bar{\Phi}_n$ הוא גורם של x^n-1
כאיבר ב- $\mathbb{Z}_p[x]$ (כי ב-$\mathbb{Z}[x]$ מתקיים $x^n-1=\prod_{d|n}\Phi_d$ ולכן ב-$\mathbb{F}_p[x]$ $x^n-1=\prod_{d|n}\bar{\Phi}_d$]
אבל היות ש-p ראשוני זר ל-n נובע של- x^n-1 אין שורשים כפולים בסתירה. ☺

משפט דדקינד: תהי G חבורה. ויהי F שדה. כל קבוצה סופית $\{\chi_1,\dots,\chi_m\}$ של קרקטרים $\chi_i: G \to F^*$
היא בלתי תלויה לינארית. [קרקטר $\chi: G \to F^*$ הוא הומומורפיזם של חבורות - $\chi(g_1g_2)=\chi(g_1)\chi(g_2)$]

הסבר: נסמן ב- $\hat{G}$ את אוסף כל הקרקטרים של G. כל קרקטר הוא פונקציה מ-G ל- $F^* \subseteq F$.
אז $\hat{G} \subseteq F^G$ והרי F^G מרחב וקטורי מעל F והטענה היא שכל הקבוצה בלתי תלויה

הוכחה: נניח בשלילה שקיימת תלות לינארית לא טריוויאלית של קרקטרים. כלומר קיימים
$a_1,\dots,a_m \in F$ כך ש- $\sum_{i=1}^m a_i\chi_i=0$ (כלומר לכל $g \in G$ $\sum_{i=1}^m a_i\chi_i(g)=0$) ולא
כל $a_1,\dots,a_m$ הם אפס. נבחר תלות כזו שבה מספר ה-a_i-ים השונים מאפס הוא מינימלי.
נסמן מספר זה ב-k. בה"כ לאחר שינוי סדר מתקיים $\sum_{i=1}^k a_i\chi_i=0$ ו- $a_i \neq 0$ לכל i.
היות ש- $\bar{0} \in F^G$ אינו קרקטר (כי התמונה של קרקטר היא ב-F^* שאינו כולל את 0)
נובע ש- $2 \le k$. נראה שנובע קיום תלות עבור פחות מ-k קרקטרים מבין $\chi_1,\dots,\chi_k$
ונקבל סתירה. לכל $g \in G$ מתקיים $a_1\chi_1(g)+a_2\chi_2(g)+\dots+a_k\chi_k(g)=0$ (*)
ויהי $h \in G$. אז לכל $g \in G$ מתקיים $a_1\chi_1(hg)+a_2\chi_2(hg)+\dots+a_k\chi_k(hg)=0$
ולכן לכל $g \in G$ $a_1\chi_1(h)\chi_1(g)+a_2\chi_2(h)\chi_2(g)+\dots+a_k\chi_k(h)\chi_k(g)=0$ (**)
נכפול את (*) ב- $\chi_k(h)$ ונחסיר מ-(**) ונקבל שלכל $g \in G$

$$a_1(\chi_1(h)-\chi_k(h))\chi_1(g)+\dots+a_{k-1}(\chi_{k-1}(h)-\chi_k(h))\chi_{k-1}(g)=0$$

ואז יש $k-1 < k$ מחוברים וכן לדאוג שלא כל המקדמים $a_i(\chi_i(h)-\chi_k(h))=0$
לשם כך די רק שנבחר $h \in G$ כך ש- $\chi_1(h) \neq \chi_k(h)$. ויש כזה כי $k \neq 1$
והקרקטרים $\chi_1,\dots,\chi_k$ שונים. ☺

(40) 21.07.08
מבנים

<u>משפט דדקינד</u>: G חבורה ו- F שדה. 6 קבוצה של הומומורפיזמים $\chi: G\to F^*$ (שונים) הם בלתי תלויה לינארית מעל F.

<u>סימונים</u>: $G^* = \{\chi: G\to F^* ;$ הומו' $\chi\}$
נשים לב ש- $G^* \subseteq F^G = \{f: G\to F\}$

<u>הגדרה</u>: תהי G חבורה. F שדה ו- V מ"ו מעל F. הצגה של G היא הומומורפיזם $G\to GL(V)$ ($GL(V)$ = חבורת הטרנספורמציות הלינאריות ההפיכות ממרחב וקטורי V לעצמו)

נשים ♡ ש- $GL(F)=F^*$

בהינתן הצגה $\rho: G\to GL(V)$ כאשר V מרחב וקטורי ממימד סופי הקרקטר של ρ הוא הפונקציה $\chi_\rho: G\to F$ המוגדרת ע"י $\chi_\rho(g)=tr\rho(g)$. בפרט הצגה ממימד סופי של G התאמנו פונקציה $\chi_\rho: G\to F$.

<u>עובדה</u>: χ_ρ קובעת את ההצגה ρ.

<u>דוגמאות</u>:

- $G=\mathbb{Z}/n\mathbb{Z}$ חבורה ציקלית ו- $F=\mathbb{C}$. הומומורפיזם מ- G ל- $\mathbb{C}^*$ (כלומר הצגה חד-ממדית) נקבע ע"י התמונה של 1. לכל שורש יחידה מסדר n $\omega\in\mathbb{C}$ נגדיר הומומורפיזם $\rho_\omega: \mathbb{Z}/n\mathbb{Z}\to\mathbb{C}^*$
$k\longmapsto\omega^k$
ולמעשה, אלה כל ההומומורפיזמים מ- $\mathbb{Z}/n\mathbb{Z}$ ל- $\mathbb{C}^*$..
- $G=\mathbb{Z}/n\mathbb{Z}=\langle g\rangle$ כאשר g יוצר ו- $V=\mathbb{F}^n$.

$$A_1=\begin{pmatrix} 0 & 1 & & \\ 0 & 0 & 1 & 0 \\ \vdots & & & \ddots \\ 0 & & & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix} \qquad \rho(g^i)=A_1^i \quad 0\le i\le n-1$$

<u>מסקנה</u>:

① יהיו F_1,F_2 שדות ויהיו $\sigma_1,\dots,\sigma_n: F_1\to F_2$ הומומורפיזמים אזי הם בלתי תלויים לינארית כאיברים במרחב הוקטורי $V=F_2^{F_1}$ מעל F_2

② E/F הרחבה (ספרבילית) מדרגה m. $\alpha_1,\dots,\alpha_m$ בסיס ל-E מעל F ויהיו $\sigma_1,\dots,\sigma_m: E\to\Omega$ F-הומומורפיזמים שונים ואשר $\Omega \supseteq F$ שדה כלשהו. אזי המטריצה $A=(a_{ij})$ כאשר $a_{ij}=\sigma_i(\alpha_j)$ היא הפיכה.

<u>הוכחה</u>:

② נניח ש- $\det A = 0$. אזי קיימים $\overbrace{c_1,\dots,c_m}^{\text{לא כולם 0}}\in\Omega$ כך ש-
$\sum_{i=1}^{m} c_i\sigma_i(\alpha_j)=0$ לכל j. כלומר לכל j
$(\sum_{i=1}^{m} c_i\sigma_i)(\alpha_j)=0 \Leftarrow$ לכל $(\sum_{i=1}^{m} c_i\sigma_i)(\alpha)=0,\alpha\in E$
$\Leftarrow \sum_{i=1}^{m} c_i\sigma_i = 0$ (במרחב הפונקציות מ-E ל-Ω).
אבל היות ש- $\sigma_1,\dots,\sigma_m$ בת"ל נקבל $c_1=\dots=c_m=0$ וזו סתירה. ☺

<u>הגדרה</u>: תהי E/F הרחבת גלואה ממימד סופי. <u>בסיס נורמלי</u> ל-E מעל F הוא בסיס מהצורה $\{\sigma(\alpha):\sigma\in Gal(E/F)\}$ עבור α קבוע כלשהו. (נזכור ש- $|Gal(E/F)|=[E:F]$)

<u>משפט</u>: לכל הרחבת גלואה סופית יש בסיס נורמלי. (יש גם הרחבות אינסופיות, אבל לא דיברנו על זה)

<u>הוכחה</u>: נפריד בין שני מקרים:

① F שדה אינסופי

② F שדה סופי.

נעיר שאם F שדה סופי אז $Gal(E/F)$ ציקלית.

① השדה F אינסופי

עובדה/תרגיל: אם $f\in E[X_1,\dots,X_n]$ לכל $a_1,\dots,a_n\in F$ $f(a_1,\dots,a_n)=0$ אזי $f=0$.

הוכחת העובדה: באינדוקציה על מספר המשתנים n. אם $0\neq f\in E[X]$ אז יש לו לכל היותר $\deg f$ שורשים שונים. לכן היות ש- F אינסופי קיים $a_1\in F$ כך ש- $f(a_1)\neq 0$ בסתירה.
נניח באינדוקציה עבור פולינומים ב- $E[X_1,\dots,X_{n-1}]$ ונתבונן בפולינום $0\neq f\in E[X_1,\dots,X_n]$. נרשום

עבור $f = \sum_{i=0}^{M} g_i(X_1,\dots,X_{n-1})X_n^i$

$g_i(X_1,\dots,X_{n-1}) \in E[X_1,\dots,X_{n-1}]$. היות ש- $f \neq 0$ קיים $0 \le i_0 \le M$

כך ש- $g_{i_0} \neq 0$. לכן לפי הנחת האינדוקציה קיימים

$a_1,\dots,a_{n-1} \in F$ כך ש- $g_{i_0}(a_1,\dots,a_{n-1}) \neq 0$ ולכן

הפולינום $E[X_n] \ni h(X_n) = f(a_1,\dots,a_{n-1},X_n) = \sum_{i=0}^{M} g_i(a_1,\dots,a_{n-1})X_n^i$

שונה מאפס. לכן מהנחת האינדוקציה קיים $a_n \in F$ כך ש-

$0 \neq h(a_n) = f(a_1,\dots,a_n)$.

נחזור להוכחה. נסמן $G = Gal(E/F) = \{\sigma_1,\dots,\sigma_m\}$

טענה: אם $f \in F[X_1,\dots,X_m]$ מקיים שלכל $\alpha \in E$

$f(\sigma_1(\alpha),\dots,\sigma_m(\alpha)) = 0$ אזי $f = 0$.

הוכחת הטענה: יהי $\alpha_1,\dots,\alpha_m$ בסיס ל-E מעל F ונגדיר

$$E[Y_1,\dots,Y_m] \ni g(Y_1,\dots,Y_m) = f(\sigma_1(\sum Y_i\alpha_i),\dots,\sigma_m(\sum Y_i\alpha_i)) =$$
$$= f(\sum_{i=1}^{m} Y_i\sigma_1(\alpha_i),\dots,\sum Y_i\sigma_m(\alpha_i))$$

נשים לב שאם נציב במקום ה-Y_i-ים איברים מ-F (=השדה

השבת של כל ה-σ_i-ים) אזי

$$g(b_1,\dots,b_m) = f(\sigma_1(\sum b_i\alpha_i),\dots,\sigma_m(\sum b_i\alpha_i))$$

נתון ש-f מקיים $f(\sigma_1(\alpha),\dots,\sigma_m(\alpha)) = 0$ לכל $\alpha \in E$

$\Leftarrow$ $g(b_1,\dots,b_m) = 0$ לכל $b_1,\dots,b_m \in F$

$\Leftarrow$ $g = 0$ (מה שטענו).

נשים לב ש- $g(Y_1,\dots,Y_m) = f((Y_1,\dots,Y_m)B)$ כאשר

$B = (b_{ij}) \in M_m(E)$, $b_{ij} = \sigma_i(\alpha_j)$, שהרי:

$$(Y_1 \dots Y_m)(\sigma_i(\alpha_j)) = (\sum Y_j\sigma_1(\alpha_j),\dots,\sum Y_j\sigma_m(\alpha_j))$$

נשים לב שהמטריצה $B = (\sigma_i(\alpha_j))$ הפיכה (מהמסקנה (ב))

מתקיים $f(Y_1,\dots,Y_m) = g((Y_1,\dots,Y_m)B^{-1})$

לכן אם g פונקצית האפס על F^m גם f פונקצית האפס

על F^m $\Leftarrow$ $f = 0$ כפולינום.

נחזור להוכחה. נתבונן במשתנים $\{X_{\sigma_i} : \sigma_i \in G\}$ כאשר

$G=\mathrm{Gal}(E/F)$. תהי $A=(a_{ij})\in M_m(F(x_{\sigma_1},\dots,x_{\sigma_m}))$

כאשר $a_{ij}=x_{\sigma_i\sigma_j}$ (נניח בה"כ ש- $\sigma_1=id$ היחידה).

נגדיר $h(x_{\sigma_1},\dots,x_{\sigma_m})=\det A$

זה אכן פולינום האפס משום ש- $h(1,0,\dots,0)=\det\left(\text{מטריצת תמורה}\right)=\pm1\neq0$

⇐ קיים $\alpha\in E$ כך ש- $0\neq h(\sigma_1(\alpha),\dots,\sigma_m(\alpha))=\det C$

כאשר $C=(c_{ij})$; $c_{ij}=(\sigma_i\sigma_j)(\alpha)$

טענה: $\{\sigma_i\alpha\}_{i=1}^{m}$ בסיס ל-E וגם בסיס נורמלי.

הוכחה: די להראות ש- $\sigma_1\alpha,\dots,\sigma_m\alpha$ בת"ל מעל F.

נניח ש- $\sum a_j\sigma_j(\alpha)=0$ עבור $a_1,\dots,a_m$.

נפעיל σ_i על (*) ונקבל שלכל $1\le i\le m$

$$0=\sigma_i\left(\sum_{j=1}^{m}a_j\sigma_j\alpha\right)=\sum_{j=1}^{m}a_j(\sigma_i\sigma_j)\alpha$$

קיבלנו מערכת של m משוואות ב-m "נעלמים" $a_1,\dots,a_m$

שמטריצת מקדמיה היא $(\sigma_i\sigma_j\alpha)$. זו מטריצה הפיכה ולכן

$a_1=a_2=\dots=a_m=0$.

סיימנו עם המקרה של $|F|=\infty$.

② נניח ש- $|F|=p^n$ עבור p ראשוני ; $n\ge1$.

טענה: $\mathrm{Gal}(E/F)$ ציקלית

הוכחה: $\mathbb{F}_p\subseteq F$ וקיים $\mathrm{Gal}(E/F)\le\mathrm{Gal}(E/\mathbb{F}_p)$.

כאשר $|E|=p^m$. מספיק להראות ש- $\mathrm{Gal}(E/\mathbb{F}_p)$ ציקלית. נשים לב שעבור שדה סופי E מסדר p^m $E/\mathbb{F}_p$ הרחבת גלואה. $|\mathrm{Gal}(E/\mathbb{F}_p)|=[E:\mathbb{F}_p]=m$

יהי $\sigma_p:E\to E,\ a\mapsto a^p$ אוטומורפיזם פרובניוס. נשים לב ש $\sigma_p\in\mathrm{Gal}(E/\mathbb{F}_p)$ וכן הסדר של σ_p הוא m, כלומר $\sigma_p^m=1$ ב- $\mathrm{Gal}(E/\mathbb{F}_p)$; $\sigma_p^l\neq1$ לכל $1\le l\le m-1$.

נשים לב שקבוצת נקודות השבת של σ_p^l היא בדיוק תת השדה בן p^l איברים ב-E.

$\{a\in E:\sigma_p^l(a)=a\}=\{a\in E: a^{p^l}-a=0\}=$

$=\{a\in E: f(a)=0,\ f(x)=x^{p^l}-x\}=$ ~~תת~~ השדה בן p^l איברים ב-E.

⟸ $Gal(E/\mathbb{F}_p) = \langle \sigma_p \rangle$ חבורה ציקלית

מסדר m.

אנחנו רוצים להראות שקיים $\alpha \in E$ כך שמסלולו $\alpha, \sigma_p(\alpha), \dots, \sigma_p^{k-1}(\alpha)$
הוא בסיס ל-E מעל F כאשר $Gal(E/F) = \{1, \sigma, \dots, \sigma^{k-1}\}$
חבורה ציקלית. $\sigma_p : E \to E$ ט"ל כך ש- $\sigma_p^k - 1 = 0$
כאשר $[E:F] = k$; $x^k - 1$ פולינום מינימלי של σ.
רוצים להראות שיש בסיס מהצורה $\alpha, \sigma_p(\alpha), \dots, \alpha_p^{k-1}(\alpha)$.
נוח לחלק למקרים ש- k זר ל- p ו- k לא זר ל- p.

(43) 22.07.08
מבנים

משפט: E/F הרחבת גלואה סופית. אזי יש ל-E בסיס נורמלי מעל F.

הוכחה: הראינו למקרה ש- $|F|=\infty$. נותר לטפל במקרה $|F|<\infty$.
ראינו שאז $G=Gal(E/F)$ ציקלית. נסמן
$$G=\langle\sigma\rangle=\{1,\sigma,\dots,\sigma^{n-1}\}$$
כש $n=[E:F]$

טענה: אם $\sigma:E\to E$ ט"ל מעל F כך ש- x^n-1 הפולינום המינימלי של σ אזי קיים $\alpha\in E$ כך ש- $\alpha,\sigma\alpha,\dots,\sigma^{n-1}\alpha$ בסיס.

ברור ש- $\sigma^n-1=0$. למה x^n-1 הפולינום המינימלי של σ? אם היה פולינום $0\neq q(x)$ ממעלה $k<n$ כך ש- $q(\sigma)=0$ אז $q(x)=\sum_{i=0}^{k}c_ix^i$; $q(\sigma)=\sum_{i=0}^{k}c_i\sigma^i$ זאת תלות לינארית בין $1,\sigma,\dots,\sigma^{n-1}$ וזו סתירה למסקנה מהרצאה אחרונה (ראינו שכל קבוצה של הומומורפיזמים שונים $\varphi_1,\dots,\varphi_m:F_1\to F_2$ בין שדות הן בת"ל לינארית (לכן $1,\sigma,\dots,\sigma^{n-1}$ בת"ל). $\Leftarrow$ σ אינו שורש של פולינום מעל E ממעלה $<n$.

הוכחת הטענה:

מקרה 1: נניח n זר למציין F (או $\text{char}F=0$. כרגע מעניין אותנו רק המקרה שהשדה סופי אבל הטענה נכונה באופן כללי)

אם $\text{char}F=0$ או $\text{char}F=p$ עבור $p\nmid n$ ל- x^n-1 יש שורשים שונים (באיזשהי הרחבה L של F).
אם $T:E\to E$ ט"ל מעל F כך ש- x^n-1 הפולינום המינימלי של T אזי T ו- σ דומות. כלומר יש $g\in GL(V)$ כך ש- $T=g^{-1}\sigma g$. נזהה את E עם F^n וניקח

הט"ל $T:F^n \to F^n$ המתאימה למטריצה

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 \dots & 0 \\ \vdots & & & & \\ 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

ביחס לבסיס הסטנדרטי.

עבור T יש וקטור β כך ש- $\beta, T\beta, \dots, T^{n-1}\beta$ בסיס ולכן גם עבור σ.

טיעון אחר: נניח לשם פשטות ששורשי היחידה מסדר n שונים ב-F. אז ניתן ללכסן את σ. יהיו $\{\lambda_1, \dots, \lambda_n\}$ שורשי x^n-1 אז $E = \oplus V_i$ כאשר V_i המרחבים העצמיים של σ. כלומר $\sigma v_i = \lambda_i v_i$. המרחבים חד-ממדיים. אם $\alpha = \sum_{i=1}^{n} a_i v_i$ כאשר כל $a_i \neq 0$ אז מעגל α הוא בסיס: למשל,

$$\alpha = v_1 + v_2 + \dots + v_n$$

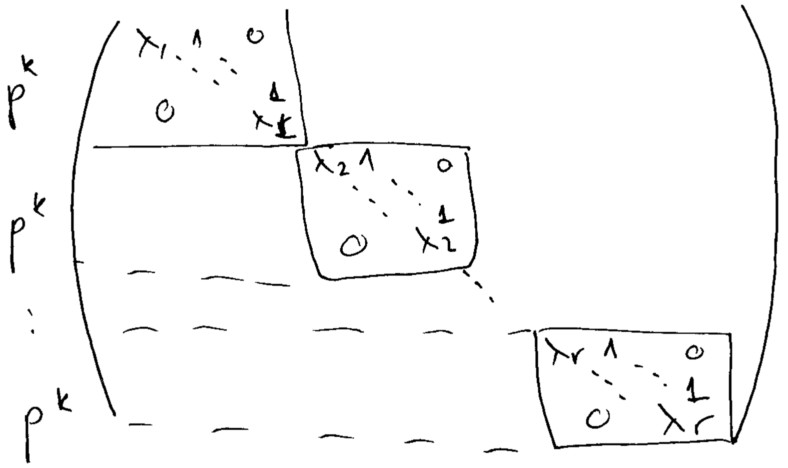
$$\sigma\alpha = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n \qquad \lambda_i \neq \lambda_j$$

$$\vdots$$

$$\sigma^{n-1}\alpha = \lambda_1^{n-1} v_1 + \lambda_2^{n-1} v_2 + \dots + \lambda_n^{n-1} v_n$$

מרק שהמטריצה $\begin{pmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_n \\ \vdots & & \\ \lambda_1^{n-1} & \dots & \lambda_n^{n-1} \end{pmatrix}$ הפיכה נובע שהוקטורים בת"ל.

<u>מקרה 2</u>: $\operatorname{char} F = p$; $p \mid n$. נרשום $n = p^k r$ עבור $(p,r)=1$. הפולינום המינימלי של σ הוא $x^{p^k r}-1 = (x^r-1)^{p^k}$. שוב נניח לשם פשטות ששורשי יחידה מסדר n שונים ב-F. לכן נובע שהערכים העצמיים של σ הם $\lambda_1, \dots, \lambda_r$ וצורת ז'ורדן של σ היא



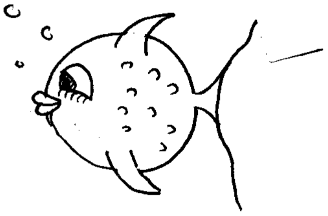
עובדה: אם $T, \tilde{T}$ ט"ל של מ"ו וקטורי כך ששתיהן יש אותה צורת ז'ורדן ביחס לבסיסים מתאימים אזי הן דומות.
בפרט ל-$\tilde{T}$ ול-$A=\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{pmatrix}$ יש אותו פולינום מינימלי ולכן אותה צורת ז'ורדן $\Rightarrow$ הן דומות. ומאחר של-A יש וקטור שמסלולו בסיס כך גם עבור $\tilde{T}$.
לא נטפל במקרה שהשורשים לא ב-F, אבל זה נכון גם אז. ☺

הרחבות ציקליות

משפט: יהי F שדה המכיל שורש יחידה פרימיטיבי מסדר n, ו-$E=F[\alpha]$ הרחבה כך ש- $\alpha^n \in F$; $\alpha^k \notin F$ לכל $1 \le k < n$. אזי E/F גלואה ; ו- $Gal(E/F)$ ציקלית מסדר n. להפך, אם F כנ"ל ; E/F גלואה כך ש- $Gal(E/F)$ ציקלית מסדר n אזי $E=F[\alpha]$ עבור $\alpha^n \in F$; $\alpha^k \notin F$ ל- $1 \le k < n$.

משפט: יהי F שדה המכיל שורש יחידה פרימיטיבי מסדר $n:=(\deg f)!$ כאשר f פולינום. אזי G_f פתירה אמ"מ שדה הפיצול של f מוכל בשדה M כך ש- $F_0=F \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_k=M$ כאשר $F_{i+1}=F_i[\beta]$; $\beta^{r_i} \in F_i$.

(45) 28.07.08
אמנים



הרחבות ציקליות

משפט: יהי F שדה המכיל ζ שורש יחידה פרימיטיבי מסדר n. אם $E=F[\alpha]$ שדה הרחבה כאשר $\alpha^n \in F$ ו- $\alpha^k \notin F$ לכל $1 \le k < n$ אזי E/F הרחבת גלואה ו- $Gal(E/F)$ ציקלית מסדר n. להפך, אם F שדה המכיל שורש יחידה פרימיטיבי מסדר n ו- E/F הרחבת גלואה עם חבורת גלואה ציקלית מסדר n אזי $E=F[\alpha]$ כאשר $\alpha^n \in F$ ו- $\alpha^k \notin F$ לכל $1 \le k < n$.

הוכחה: נניח ש- $E=F[\alpha]$ כאשר $\alpha^n \in F$ ו- $\alpha^k \notin F$ עבור $1 \le k < n$. נשים ♡ ש- α שורש של $f(x)=x^n-\alpha^n$ אזי $f(x)=\prod_{i=0}^{n-1}(x-\zeta^i\alpha)$. לכן E שדה פיצול של F, כי הרי $\zeta, \alpha \in E$. לכן E/F הרחבת גלואה. לכל $\tau \in Gal(E/F)$ מתקיים $\tau\alpha=\zeta^i\alpha$ (כי שורשים עוברים לשורשים). נגדיר הומומורפיזם $\Phi: Gal(E/F) \longrightarrow \mu_n=\{\zeta^i\}_{i=0}^{n-1}$ ע"י $\tau \longmapsto \zeta^i_\alpha = \frac{\tau\alpha}{\alpha}$. קל לראות שזה הומומורפיזם. μ_n חבורה ציקלית מסדר n. ברור שההומומורפיזם חח"ע (היות ש- $E=F[\alpha]$, $\tau \in Gal(E/F)$ נקבע ע"י פעולתו על α). נותר לוודא ש- Φ על. תמונת Φ היא תת חבורה של חבורה ציקלית מסדר n ולכן היא ציקלית מסדר k עבור $k|n$. לכל $\tau \in Gal(E/F)$ מתקיים $1=\left(\frac{\tau\alpha}{\alpha}\right)^k=\frac{(\tau\alpha)^k}{\alpha^k}=\frac{\tau(\alpha^k)}{\alpha^k}$ לכן לכל $\tau \in Gal(E/F)$ $k=n \Leftarrow \alpha^k \in F \Leftarrow \tau(\alpha^k)=\alpha^k$. (כי $a^k \notin F$ עבור $1 \le k < n$).

מאידך, נניח ש- F שדה שמכיל ζ שורש יחידה פרימיטיבי מסדר n. ו- E/F הרחבת גלואה כך ש- $Gal(E/F)=\langle\sigma\rangle$ ציקלית מסדר n. נטען שקיים $0 \ne \alpha \in F$ כך ש- $\sigma\alpha=\zeta^{-1}\alpha$: קיים $\gamma \in E$ כך ש- $\alpha=\sum_{i=0}^{n-1}\zeta^i\sigma^i\gamma \ne 0$ (נובע מכך שההומומורפיזמים $\sigma^i: E^* \to E^*$, $0 \le i \le n-1$ הם בת"ל מעל E ולכן הפונקציה $\sum_{i=0}^{n-1}\zeta^i\sigma^i: E \longrightarrow E$ אינה פונקציית האפס).

כעת נחשב:

$$\sigma\alpha=\sigma\left(\sum_{i=0}^{n-1}\zeta^i\sigma^i\gamma\right)=\sum_{i=0}^{n-1}\sigma(\zeta^i)\sigma^{i+1}\gamma=\sum_{i=0}^{n-1}\zeta^i\sigma^{i+1}\gamma=$$
$$=\zeta^{-1}\sum_{i=0}^{n-1}\zeta^{i+1}\sigma^{i+1}\gamma=\zeta^{-1}\alpha$$

עכשיו יש לנו $0\neq\alpha\in F$ כך ש- $\sigma\alpha=\zeta^{-1}\alpha$. נטען שזה ה-$\alpha$ שאנחנו צריכים. צריך להראות:

(א) $\alpha^n\in F$, - $\alpha^k\notin F$ $1\leq k<n$.

(ב) $E=F[\alpha]$

כדי לבדוק אם איבר בשדה F אולי נבדוק איך פועלת עליו איבר מחבורת גלואה:

$$\sigma(\alpha^k)=(\sigma\alpha)^k=(\zeta^{-1}\alpha)^k=\zeta^{-k}\alpha^k$$

אם $k=n$ קיבלנו $\sigma(\alpha^n)=\alpha^n$ ולכן גם לכל $\sigma^i=\tau\in Gal(E/F)$ מתקיים $\tau\alpha^n=\alpha^n$ ולכן $\alpha^n\in F$.

אם $1\leq k<n$ אז $\zeta^{-k}\neq1$ אז $\sigma(\alpha^k)\neq\alpha^k$ ולכן $\alpha^k\notin F$ (כי F שדה השבת)

כעת, ברור ש- $E\supseteq F[\alpha]$. הדרגה של $F[\alpha]$ היא דרגת α. α מקיים את הפולינום $x^n-\alpha^n$. לכן מספיק להראות ש- $x^n-\alpha^n$ אי-פריק. נשים לב ששורשי $x^n-\alpha^n$ הם הקבוצה $\{\zeta^i\alpha : 0\leq i<n\}$ והיא מהווה מסלול של α תחת $\langle\sigma\rangle=Gal(E/F)$ ולכן בהכרח הפולינום אי-פריק. (לפי טענה קודמת). לכן E ו- $F[\alpha]$ הרחבות מאותה דרגה ולכן $E=F[\alpha]$ וסיימנו.

<u>תזכורת</u>: אילו היה פירוק $f_\alpha=gh$ עבור $g,h\in F[x]$ פולינומים מדרגה ≥1. אז נניח ש $g(\alpha)=0$. אבל $Gal(E/F)$ שומרת על g ולכן מעבירה שורש של g לשורש של g. ולכן מסלול α מוכל בשורשי g ואינו כל שורשי f_α סתירה.

<u>הוכחה אחרת לכך ש- $E=F[\alpha]$</u>: נתבונן בתת השדה $F[\alpha]\subseteq E$ תת החבורה המתאימה אותו ב- $Gal(E/F)$ היא

$$\{\tau\in Gal(E/F) : \tau\alpha=\alpha\}=\{\sigma^i : \sigma^i\alpha=\alpha\}=$$

$$= \{ \sigma^i : \zeta^{-i}\alpha = \alpha \} = \{ \sigma^0 \} = \{id\}$$

$$\hookrightarrow \sigma^i(\alpha) = \sigma^{i-1}(\sigma\alpha) = \sigma^{i-1}(\zeta^{-1}\alpha) = \zeta^{-1}\sigma^{i-1}(\alpha)$$

$$\overset{\text{אינדוקציה}}{=} \zeta^{-1}\zeta^{-(i-1)}\alpha = \zeta^{-i}\alpha$$

$\Leftarrow$ $E = F[\alpha]$.

<u>הגדרה</u>: יהי F שדה. נאמר שפולינום $f \in F[X]$ ניתן לפתרון ע"י רדיקלים אם שדה הפיצול E של f מוכל בשדה F_m כך שקיימת סדרת הרחבות

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_m$$

כאשר לכל $0 \le i \le m-1$, $F_{i+1} = F_i[\alpha_i]$ ו- $\alpha_i^{r_i} \in F_i$.

<u>למה</u>: יהי $f \in F[X]$ פולינום ספרבילי כך שחבורת גלואה שלו פתירה. אזי גם עבור שדה הרחבה $F' \supseteq F$ חבורת גלואה של f כאיבר ב- $F'[X]$ פתירה.

<u>הוכחה</u>: יהי $F' \subseteq E'$ שדה פיצול של f מעל F' ויהיו $\alpha_1, \dots, \alpha_n$ שורשי f ב- E'. $E = F[\alpha_1, \dots, \alpha_n]$ שדה פיצול של f מעל F. $Gal(E'/F')$ מעתיקה את $\{\alpha_1, \dots, \alpha_n\}$ ל- $\{\alpha_1, \dots, \alpha_n\}$ ומקבעת את F. לכן איברי $Gal(E'/F')$ מעתיקים את E ל- E ומקבעים את F וקיבלנו שצמצום $\sigma \in Gal(E'/F')$ ל- E הוא הומומורפיזם $\Phi : Gal(E'/F') \to Gal(E/F)$. (נזכור ש- $E' = F'[\alpha_1, \dots, \alpha_n]$) לכן Φ שיכון. לכן מפתירות $Gal(E/F)$ נובעת פתירות $Gal(E'/F')$.

<u>תזכורת</u>: G חבורה פתירה אמ"מ קיימת סדרה נורמלית

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_m = \{e\}$$

כך ש- G_i/G_{i+1} אבלית. אם $H \le G$ תת חבורה נגדיר $H_i = H \cap G_i$ ואז $H = H_0 \triangleright H_1 \triangleright H_2 \triangleright \dots \triangleright H_m = \{e\}$

ו- H_i/H_{i+1} איזומורפית לתת חבורה של G_i/G_{i+1} לכן אבלית.
לכן תת חבורה של חבורה פתירה היא חבורה פתירה.

משפט: יהי F שדה ממציין 0. אז $f\in F[X]$ פתיר בעזרת רדיקלים אמ"מ G_f חבורה פתירה.

הוכחה:

($\Rightarrow$) נניח ש- G_f פתירה ונראה ש- f פתיר בעזרת רדיקלים. יהי $F\subseteq F'=F[\zeta]$ עם ζ שורש יחידה פרימיטיבי מסדר $(\deg f)!$. מהלמה נובע שחבורת גלואה של f מעל F' גם היא פתירה.

נסמן $F'\subseteq E$ שדה הפיצול של f, $G=Gal(E/F')$ קיימת סדרה $G=G_0\rhd G_1\rhd G_2\rhd\dots\rhd G_m=\{1\}$ כך ש- G_i/G_{i+1}. הנחת הנורמליות פירושה שיש סדרה $G=L_0\rhd L_1\rhd\dots\rhd L_k=\{1\}$ כך ש- L_i/L_{i+1} אבליות. היות שמדובר בחבורות סופיות, כל L_i/L_{i+1} היא מכפלה ישרה של חבורות ציקליות ולכן ניתן לעדן את הסדרה של תת החבורות ולקבל סדרת הרכב כך ש- G_i/G_{i+1} ציקליות.

נגדיר $F_i=E^{G_i}$ - שדות השבת של E תחת G_i. אז
$$E=F_m\supseteq F_{m-1}\supseteq\dots\supseteq F_0=F[\zeta]\supseteq F$$
; - F_{i+1}/F_i הרחבת גלואה ציקלית מסדר שמחלק את $(\deg f)!$
(כי $[E:F']\le(\deg f)!$. נתון פולינום f ממעלה $k=\deg f$ בניית שדה הפיצול הוא ע"י הוספת השורשים $\alpha_1,\dots,\alpha_n$ של f אחד אחד לה
$$F'\subseteq \underset{\le\deg f}{F'[\alpha_1]}\subseteq \underset{\le\deg f-1}{F'[\alpha_1,\alpha_2]}\subseteq\dots\subseteq \underset{1}{F'[\alpha_1,\dots,\alpha_k]}$$
)

לכן $Gal(F_{i+1}/F_i)$ ציקלית מסדר r_i ; . F_i מכיל שורש יחידה פרימיטיבי מסדר r_i ולכן קיים α_i כך ש- $F_{i+1}=F_i[\alpha_i]$; $\alpha_i^{r_i}\in F$ ולכן f פתיר בעזרת רדיקלים.

($\Leftarrow$) נניח ש- $f\in F[X]$ פתיר בעזרת רדיקלים. יהי $F\subseteq E$ שדה פיצול של f. אזי קיימת סדרת שדות $F=F_0\subseteq F_1\subseteq F_2\subseteq\dots\subseteq F_m$ כך ש- $F_i=F_{i-1}[\alpha_i]$; $\alpha_i^{r_i}\in F_{i-1}$ ל- $1\le i\le m$; $E\subseteq F_m$. נסמן $n=r_1r_2\dots r_m$. קיימת הרחבת גלואה $F\subseteq\Omega$ שמכילה את F_m ; - ζ שורש יחידה פרימיטיבי מסדר n.

קיים $\gamma\in F_m$ יק ש- $F_m=F[\gamma]$. יהי g פולינום מינימלי
עבור γ, ונתבונן בשדה פיצול של $(x^n-1)g(x)\in F[X]$.
Ω/F הרחבת גלואה. ⁝- $\Omega\supseteq F_m[\zeta]$. יהי $\tilde{E}$ סגור
גלואה של $\Omega\supseteq F_m[\zeta]$. $\tilde{E}$ = הרחבה נורמלית מינימלית של F
ב- Ω המכילה את $F_m[\zeta]$ (הנו קיים כי $F\subseteq F_m[\zeta]\subseteq\Omega$
ואשר $F_m[\zeta]=\Omega^H$ עבור איזו תת חבורה $H\le Gal(\Omega/F)=G$
נגדיר $N=\bigcap_{g\in G}g^{-1}Hg$ ⁝- $\tilde{E}=\Omega^N$).

(48) 29.07.08

מבנים

משפט: F שדה ממציין 0 ! $f \in F[X]$ פולינום. אז f פתיר באמצעות רדיקלים אמ"מ G_f פתירה.

הוכחה:

($\Rightarrow$) עשינו אתמול

($\Leftarrow$) נניח ש- f פתיר באמצעות רדיקלים. נסמן ב- E את שדה הפיצול של f מעל F אז $Gal(E/F)$ פתירה.

הערה: כדי להראות שחבורה היא פתירה די להראות שהיא מנה של חבורה פתירה.

נתון ש- $E \subseteq F_m$ כאשר $F_0 = F \subseteq F_1 \subseteq \dots \subseteq F_m$ שדות רק ש- $F_i = F_{i-1}[\alpha_i]$ כאשר $\alpha_i^{r_i} \in F_{i-1}$ $r_i \in \mathbb{N}$.

נגדיר $n = r_1 \cdot \dots \cdot r_m$ ויהי ζ שורש יחידה פרימיטיבי מסדר n.

הראינו של הרחבה סופית של F מוכלת באיזשהי הרחבת גלואה סופית. $F_m[\zeta] = F[\alpha_1, \dots, \alpha_m, \zeta]$. נבחר עבור α_i פולינום $g_i \in F[X]$ ספרבלי רק ש- $g_i(\alpha_i) = 0$ ויהי Ω שדה הפיצול של $(x^n - 1)\prod_{i=1}^{m} g_i \in F[X]$. אז $F_m[\zeta] \subseteq \Omega$.

$$\begin{tikzcd}
\Omega \arrow[d, dash] \\
F_m[\zeta] \arrow[d, dash] \\
E \arrow[d, dash] \\
F
\end{tikzcd}$$

ויהי $\tilde{E}$ סגור גלואה של $F_m[\zeta]$ ב- Ω. קיימת תת חבורה $H < Gal(\Omega/F)$ רק ש- $F_m[\zeta] = \Omega^H$.

נגדיר $N = \bigcap_{g \in Gal(\Omega/F)} g^{-1} H g$, אז $\tilde{E} = \Omega^N$.

אזי $\tilde{E}/F$ היא הרחבת גלואה. $\tilde{E}$ נוצר ע"י ט השדות $g F_m[\zeta]$ עבור $g \in Gal(\Omega/F)$.

הרחבה $\tilde{E}/F$ נורמלית אמ"מ אם לפולינום אי פריק $h \in F[X]$ יש שורש ב- $\tilde{E}$ אזי הוא מתפצל לגורמים לינאריים ב- $\tilde{E}[X]$

נותר להראות ש- $Gal(\tilde{E}/F)$ פתירה. $\tilde{E}$ נוצר מ- F ע"י הוספת האיברים $\zeta, \alpha_1, \alpha_2, \dots, \alpha_m$ וגם

$g_1\alpha_1, \dots, g_1\alpha_m, \dots, g_k\alpha_1, \dots, g_k\alpha_m$

כאשר $Gal(\Omega/F) = \{id, g_1, \dots, g_k\}$.

מקבלים שרשרת של שדות

$$F \subseteq \overset{F'}{F[\zeta]} \subseteq F'[\alpha_1] \subseteq F'[\alpha_1,\alpha_2] \subseteq \dots \subseteq F'[\alpha_1,\dots,\alpha_m] \subseteq$$
$$\subseteq F'[\alpha_1,\dots,\alpha_m,g_1\alpha_1] \subseteq \dots \subseteq F'[\alpha_1,\dots,\alpha_m,g_1\alpha_1,\dots,g_k\alpha_m] \subseteq \tilde{E}$$

$F\subseteq F[\zeta]$ הרחבת גלואה עם חבורת גלואה אבלית.

כל שלב בשרשרת הוא מהצורה $K\subseteq K[g\alpha_i]$ (*) עבור $g\in Gal(\Omega/F)$; $F[\zeta]\subseteq K$.

$$(g\alpha_i)^{r_i} \in F[g\alpha_1,\dots,g\alpha_{i-1}] \subseteq K$$

$\Leftarrow$ (*) הרחבת גלואה עם חבורת גלואה ציקלית (בפרט אבלית)

קיבלנו שבשרשרת $F\subseteq F[\zeta]\subseteq F'[\alpha_1]\subseteq \dots \subseteq \tilde{E}$

ט שלב הוא הרחבת גלואה עם חבורת גלואה אבלית.

$\Leftarrow$ $Gal(\tilde{E}/F)$ פתירה לכן היות ש- $F\subseteq E\subseteq \tilde{E}$

ו- E/F גלואה נובע ש- $Gal(E/F)$ מנה של $Gal(\tilde{E}/F)$

לכן גם היא חבורה פתירה.

פולינום כללי ממעלה n

F שדה ממציין 0 ; $F[t_1,\dots,t_n]$ חוג הפולינומים ב-n משתנים. $F(t_1,\dots,t_n)$ שדה הפונקציות הרציונליות ב-n משתנים (שדה השברים של חוג הפולינומים).

פולינום כללי ממעלה n מעל F הוא $h_n(x)=x^n-t_1x^{n-1}+t_2x^{n-2}+\dots+(-1)^n t_n$

כלומר $h_n(x)\in F(t_1,\dots,t_n)[X]$.

מהי חבורת גלואה של h? תשובה: S_n.

נסמן ב- $F(t_1,\dots,t_n)\subseteq\Omega$ את שדה הפיצול של h_n.

חבורת גלואה היא S_n אם $[\Omega:F(t_1,\dots,t_n)]=n!$ כי הרי חבורת גלואה היא חבורת תמורות של קבוצה בגודל לכל היותר n. אז אם ההרחבה היא מסדר $n!$ בהכרח מדובר ב- S_n.

4.8.08
מבנים

טענה: F שדה. $F(t_1,\dots,t_n)$ שדה הפונקציות הרציונליות מעל F.
$$f(x) = x^n - t_1x^{n-1} + t_2x^{n-2} - \dots + (-1)^n t_n \in F(t_1,\dots,t_n)[x]$$
חבורת גלואה של f היא S_n.

הוכחה: דרך להראות זאת היא להראות ש- E שדה הפיצול של f מעל $F(t_1,\dots,t_n)$ מקיים $[E : F(t_1,\dots,t_n)] = n!$

נתבונן בשדה $L = F(x_1,\dots,x_n)$. S_n פועלת על L ע"י תמורות של $x_1,\dots,x_n$: אם $\sigma \in S_n$ ו- $g(x_1,\dots,x_n) \in L$ אז $(\sigma g)(x_1,\dots,x_n) = g(x_{\sigma^{-1}(1)},\dots,x_{\sigma^{-1}(n)})$. נסמן ב- M את שדה השבת של S_n ב- L. כלומר $M = L^{S_n}$. נטען ש- $M = L^{S_n} = F(p_1,\dots,p_n)$ כאשר $p_k = \sum_{i_1<\dots<i_k} x_{i_1}\cdots x_{i_k}$ (הפולינום הסימטרי היסודי ה- k.) כלומר M הוא תת השדה של L הנוצר ע"י F והאיברים $p_1, p_2,\dots,p_n \in L$.
היות ש- $p_1,\dots,p_n \in L^{S_n}$ ברור ש- $F(p_1,\dots,p_n) \subseteq L^{S_n}$.
מאידך, נשים ♡ ש- $F(x_1,\dots,x_n)$ הוא שדה הפיצול של הפולינום $h(Y) = \prod(Y-x_i) = Y^n - p_1Y^{n-1} + \dots + (-1)^n p_n \in F(p_1,\dots,p_n)[Y]$ ולכן $[F(x_1,\dots,x_n) : F(p_1,\dots,p_n)] \le \deg h! = n!$.
אבל $[L : L^{S_n}] = |S_n| = n!$ אז יש לנו
$$\underbrace{F(p_1,\dots,p_n) \subseteq \underbrace{L^{S_n} \subseteq L}_{n!}}_{\le n!}$$

$\Leftarrow$ $L^{S_n} = F(p_1,\dots,p_n)$ ו- $[F(x_1,\dots,x_n) : F(p_1,\dots,p_n)] = n!$.
נראה כעת שקיים איזומורפיזם של שדות $\varphi : E \longrightarrow F(x_1,\dots,x_n)$ כך ש- $\varphi(F(t_1,\dots,t_n)) = F(p_1,\dots,p_n)$ ונסיים.
די להראות איזומורפיזם $\varphi : F(t_1,\dots,t_n) \longrightarrow F(p_1,\dots,p_n)$ כך ש- $\varphi(t_i) = p_i$ כי אז הפולינום $Y^n - t_1Y^{n-1} + \dots + (-1)^n t_n$ מועתק ל- $Y^n - p_1Y^{n-1} + \dots + (-1)^n p_n$ ולכן φ נמשך לאיזומורפיזם מ- E ל- $F(x_1,\dots,x_n)$ והטענה נובעת.
נראה ראשית שההעתקה $t_i \mapsto p_i$ משרה איזומורפיזם $F[t_1,\dots,t_n] \longrightarrow F[p_1,\dots,p_n]$. ברור שכל בחירה של תמונות של $t_1,\dots,t_n$ ב- $F[p_1,\dots,p_n]$ ניתנת להרחבה להומומורפיזם של חוגים מ-

$F[t_1,\dots,t_n]$ ל- $F[p_1,\dots,p_n]$. ברור שאם $t_i \mapsto p_i$ ההומומורפיזם המתקבל הוא על. צריך לוודא שמתקבלת העתקה חח"ע.

קיום גרעין פירושו קיום פולינום $q(t_1,\dots,t_n)=\sum_{\vec{\alpha}} a_{\vec{\alpha}} t^{\vec{\alpha}}$ (סכום סופי)
כאשר $\vec{\alpha}=(d_1,\dots,d_n)\in\{\mathbb{N}\cup\{0\}\}^n$ ו- $t^{\vec{\alpha}}=t_1^{d_1}\cdots t_n^{d_n}$ כך ש-
$\varphi(q)=0$. $\Leftarrow$ $(*)\quad 0=q(p_1,\dots,p_n)=\sum a_{\vec{\alpha}}p_1^{d_1}\cdots p_n^{d_n}$

קיום $a_{\vec{\alpha}}$ כנ"ל שלא כולם 0 כך ש- (*) מתקיים פירושו תלות אלגברית בין $p_1,\dots,p_n$. נטען שההומומורפיזם φ הוא חח"ע, כלומר $p_1,\dots,p_n$ הם בלתי תלויים אלגברית מעל F כלומר לא קיימת קבוצה סופית של מקדמים $a_{\vec{\alpha}}\in F$ לא כולם אפס כך ש- $\sum a_{\vec{\alpha}}p_1^{d_1}\cdots p_n^{d_n}=0$

נתבונן בביטוי מהצורה $\sum a_{d_1\dots d_n}p_1^{d_1}\cdots p_n^{d_n}$. אותו אפשר לרשום בצורה $\sum b_{e_1\dots e_n}x^{e_1}\cdots x^{e_n}$. (נראה שאם לא כל ה- $a_{\vec{\alpha}}$ הם אפס אז לא כל ה- $b_{\vec{\beta}}$ הם אפס. נגדיר יחס סדר בין מונומים $x_1^{k_1}\cdots x_n^{k_n}$. נאמר ש- $x_1^{k_1}\cdots x_n^{k_n}$ גדול מ- $x_1^{m_1}\cdots x_n^{m_n}$ אם מתקיימת אחת מהאפשרויות הבאות:

א $\sum_{i=1}^{n}k_i > \sum_{i=1}^{n}m_i$

ב אם ב- א יש שוויון ($\sum k_i=\sum m_i$) ומתקיים $k_i=m_i$ ל- $1\le i\le r$ ו- $k_{r+1}>m_{r+1}$.

זה יחס סדר שבו כל שני מונומים ניתנים להשוואה.

נתבונן ב- $p_1^{d_1}\cdots p_n^{d_n}$. המונום המקסימלי שלו הוא
$x_1^{d_1+\dots+d_n}x_2^{d_2+\dots+d_n}\cdots x_n^{d_n}=Z$

נשים לב ש- $p_k=\sum x_{i_1}\cdots x_{i_k}$ הוא סכום מונומים שכל אחד מהם ממעלה k. $\Leftarrow$ $p_1^{d_1}\cdots p_n^{d_n}$ הוא סכום מונומים שכל אחד מהם מעלתו היא $1\cdot d_1+2\cdot d_2+\dots+n\cdot d_n$. לכן Z הוא מונום מ מעלה הנכונה. כעת קל לבדוק (באינדוקציה למשל) כי זה אכן המונום הגדול ביותר המופיע ב- $p_1^{d_1}\cdots p_n^{d_n}$.
(או שפשוט מסתכלים על $(x_1+\dots+x_2)^{d_1}(x_1x_2+x_1x_3+\dots+)^{d_2}\cdots(x_1\cdots x_n)^{d_n}$ ורואים מהן החזקות של $x_1,\dots,x_n$).

נשים ♡ שהמונום המירבי של $p_1^{d_1}\cdots p_n^{d_n}$ קובע את $d_1,\dots,d_n$

אבל אם הסכום $\sum a_{d_1\dots d_n} p_1^{d_1}\cdots p_n^{d_n} = 0$ נובע שכל המקדמים
הם אפס, כי נתבונן במחובר עם מקדם $a_{d_1'\dots d_n'} \neq 0$ רק
שהמונום המרבי שלו הוא מקסימלי מבין כל המחוברים עם מקדם
$a_{d_1\dots d_n} \neq 0$. היות שמונום זה גדול ממש מכל המונומים המופיעים
מכל שאר המחוברים הוא לא יכול להתבטל וזו סתירה..
לכן הראינו ש- $p_1,\dots,p_n$ בת"ל אלגברית ולכן ההעתקה
$F[t_1,\dots,t_n]\to F[p_1\dots p_n]$ המושרית ב- $t_i \mapsto p_i$ היא חח"ע ולכן
היות שהיא גם על היא משרה איזומורפיזם בין שדות השברים
☺ $F(t_1,\dots,t_n)\to F(p_1,\dots,p_n)$.

סקיצה של ההוכחה: $f(Y) = Y^n - t_1Y^{n-1} + t_2Y^{n-2} + \dots + (-1)^n t_n$
על $F(t_1,\dots,t_n)$. E שדה הפיצול של $f(Y)$ מעל
$F(t_1,\dots,t_n)$. טוענים ש- $Gal(E/F(t_1,\dots,t_n)) \cong S_n$
מתבוננים בהרחבת השדות $F(x_1,\dots,x_n)^{S_n} = F(p_1,\dots,p_n) \subseteq F(x_1,\dots,x_n)$
כאשר $p_k = \sum_{i_1<\dots<i_k} x_{i_1}\cdots x_{i_k}$. ראינו ש- $|Gal(F(x_1\dots x_n)/F(p_1\dots p_n))| = n!$
ראינו שההעתקה $t_i \mapsto p_i$ משרה איזומורפיזם בין $F(t_1,\dots,t_n)$
לבין $F(p_1,\dots,p_n)$ ומשרה איזומורפיזם בין שדה הפיצול של
$f = Y^n - t_1Y^{n-1} + \dots + (-1)^n t_n$ (כלומר E) לבין שדה הפיצול
של הפולינום $g = Y^n - p_1Y^{n-1} + \dots + (-1)^n p_n$ (כלומר $F(x_1,\dots,x_n)$)
ואיזומורפיזם זה מעתיק את $F(t_1,\dots,t_n)$ ל- $F(p_1,\dots,p_n)$
איזומורפית. לכן

$$Gal(E/F(t_1,\dots,t_n)) \cong Gal(F(x_1\dots x_n)/F(p_1\dots p_n)) \cong S_n$$

צורת ז'ורדן

יהי V מ"ו ממימד n מעל שדה F, $T:V\to V$ ט"ל ונניח שהפולינום
המינימלי של T הוא $p(x)$ ומתקיים $\lambda_i\neq\lambda_j$ $p(x)=\prod_{i=1}^{k}(x-\lambda_i)^{d_i}$
כאשר $\lambda_1,\dots,\lambda_k \in F$ (כלומר הפולינום המינימלי מתפרק מעל F)

אזי יש בסיס ל-V שביחס אליו המטריצה של T הוא מהצורה

$$\begin{pmatrix} \boxed{L_1} & & & 0 \\ & \boxed{L_2} & & \\ & & \ddots & \\ 0 & & & \boxed{L_k} \end{pmatrix}$$

כאשר כל בלוק L_i הוא מהצורה

$$L_i = \begin{pmatrix} \boxed{J_{\lambda_i}(n_1)} & & & \\ & \boxed{J_{\lambda_i}(n_2)} & & \\ & & \ddots & \\ & & & \boxed{J_{\lambda_i}(n_r)} \end{pmatrix}$$

כאשר

$$J_\lambda(m) = \underbrace{\begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}}_{m} \Big\} m$$

ולמעשה, עד כדי סדר של הבלוקים $J_\lambda(m)$ המטריצה היא יחידה.

בהוכחה יש שני חלקים.

<u>חלק א</u> אם T טרנספורמציה נילפוטנטית, כלומר קיים n כך ש- $T^n = 0$ אזי קיים בסיס שביחס אליו המטריצה היא מהצורה

$$\begin{pmatrix} J_0(n_1) & & \\ & \ddots & \\ & & J_0(n_r) \end{pmatrix} = \begin{pmatrix} \boxed{\begin{matrix} 0 & 1 & \\ & \ddots & 1 \\ & & 0 \end{matrix}} & & \\ & \boxed{\begin{matrix} 0 & 1 \\ & \ddots \end{matrix}} & \\ & & \boxed{\begin{matrix} 0 & 1 & \\ & \ddots & 1 \\ & & 0 \end{matrix}} \end{pmatrix}$$

<u>חלק ב</u> רדוקציה לחלק א': נגדיר פולינומים

$$g_j = \prod_{i \neq j} (x - \lambda_i)^{d_i} \qquad p_j = (x - \lambda_j)^{d_j}$$

$$p(x) = g_j(x) p_j(x) \quad \forall j$$

נגדיר $V_j = g_j(T)V$. הטענה היא ש- $V_j \neq 0$ ו-

$$V = \bigoplus_{j=1}^{k} V_j$$

$V_j \neq 0$ כי $g_j(T) \neq 0$ (כי הפולינום המינימלי לא מחלק את g_j)

קל לראות ש- $g_1(x), \dots, g_k(x)$ זרים. לכן קיימים פולינומים $a_1(x), \dots, a_k(x)$ כך ש- $1 = \sum g_i(x) a_i(x)$ $\Leftarrow$ $id = \sum a_i(T) g_i(T)$

$\Leftarrow$ $v = \sum g_i(T) a_i(T) v$ לכל $v \in V$.

לכן $V=V_1+\dots+V_k$. צריך להראות שאם $u_i\in V_i$
ומתקיים $u_1+\dots+u_k=0$ אזי לכל i $u_i=0$ (וזה
נקבל שזה סכום ישר)
אפשר לראות ש- $g_i(T)g_j(T)=0$ עבור $i\neq j$
כי הפולינום המינימלי מחלק את g_ig_j.

$\Leftarrow$ $0=g_i(T)0=\sum g_i(T)u_j=$
$=\sum g_i(T)g_j(T)u_j=g_i(T)u_j$
$\Leftarrow$ $u_j=0$

$\Leftarrow$ $V=\oplus V_i$. כמו כן, קל לראות ש- $V_i=g_i(T)V$ הוא
T-אינווריאנטי. לכן ניתן להתבונן בצמצום T ל-V_i ולנתח
את מבנהו.
יהי $U=V_i$ הפולינום המינימלי של T הוא $(x-\lambda_i)^{d_i}$.
נחליף את T ב- $S=T-\lambda_i Id$. אז $S:U\to U$
טרנספורמציה נילפוטנטית ובכך ביצענו את הרדוקציה.

נניח ש- $S:U\to U$ נילפוטנטית ויהי $u_0\in U$ כך ש-
$S^{n_1-1}u_0\neq 0$ ו- $S^{n_1}u_0=0$, כאשר n_1 המקסימלי האפשרי.
$U_1=sp(u_0,Su_0,\dots,S^{n_1-1}u_0)$ הוא S-אינווריאנטי והמטריצה
של ההעתקה על U_1 היא $\begin{pmatrix}0 & 1 & & \\ & \ddots & \ddots & \\ & & & 1 \\ 0 & & & 0\end{pmatrix}$

למה: קיים תת מרחב $W\subseteq U$ S-אינווריאנטי כך ש $U=U_1\oplus W$
הוכחה: יהי $W\subseteq U$ תת מרחב מרבי כך ש- W הוא S-אינווריאנטי
ו- $W\cap U_1=\{0\}$ ונראה ש- $U_1\oplus W=U$. אחרת, אם
$U_1+W\neq U$ אז קיים וקטור $v\in U$ כך ש- $v\notin U_1+W$.
אבל $Sv\in U_1+W$. אם היה $Sv\in W$. מתקיים $Sv=u_1+w_1$
נטען ש- $S^{n_1-1}u_1=0$. אחרת, אם $S^{n_1-1}u_1\neq 0$ נקבל ש-
$S^{n_1}v\neq 0$ וזו סתירה לבחירת n_1. לכן קיים $u_2\in U_1$ כך
ש- $u_1=Su_2$ ונגדיר $v'=v-u_2$ $\Leftarrow$ $v'\notin W$ וגם
$Sv'=Sv-Su_2=u_1+w_1-u_1=w_1\in W$ ו- $W'=W+Fv'$

מקיים W' Z-אינווריאנטי ; $W' \cap U_1 = \{0\}$ וזו סתירה
למקסימליות W כי $W' \supsetneq W$!
☺

המבחן

עוד לא נכתב. אבל שאר יסתכל על התרגילים ועל מבחנים אחרות. יהיו משפטים להוכיח. תהיה בחירה.