בס"ד ט"ו שבט תשע"ד 16.01.14

אלגברה מופשטת 3 - הרצאה מס' 14.

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

"

השדה של המספרים הניתנים לבניה

"

= השדה הקטן ביותר של $\mathbb{C}$ הסגור להוצאת שורש.

משפט: α בר-בניה $\Leftrightarrow$ חב' גלואה של שדה הפיצול היא חבורת-2. $\Leftrightarrow$ המימד של שדה הפיצול הוא חזקת 2 $\Rightarrow$ $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^i$ $\not\Leftarrow$

הבעיות של ימי קדם:

- להכפיל את הקוביה: $\sqrt[3]{2}$
- לשלש את הזווית: $\alpha \to \alpha/3$
- לרבע את המעגל: $\sqrt{\pi}$ (משפט של לינדמן: π לא אלגברי) (משפט ממוזן)
- לבנות מצולע משוכלל בן 7 צלעות.

נראה שהן לא אפשריות:

- להכפיל את הקוביה:

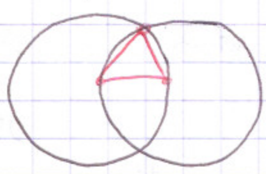
$\sqrt[3]{2}$ מאפס את הפול' האי-פריק $2-x^3$ ולכן $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$.

אי-אפשר במחוגה וסרגל.

- בניה של זווית θ = בניית $e^{i\theta} = \cos\theta + i\sin\theta$ $\Leftrightarrow$

בניית $\cos\theta$ ו- $\sin\theta$ $\Leftrightarrow$ בניית $\cos\theta$ $\Leftrightarrow$ בניית $\sin\theta$.

אפשר לבנות $60°$:



אי-אפשר לבנות $20°$:

אך צריך להכיר את הנוסחאות הבאות:

$$\cos 3\theta + i\sin 3\theta = e^{3i\theta} = (e^{i\theta})^3 = (\cos\theta + i\sin\theta)^3 =$$

$$= \cos^3\theta + 3i\cos^2\theta\sin\theta - 3\cos\sin^2\theta - i\sin^3\theta$$

$$\Rightarrow \cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

$$\sin 3\theta = 3\sin\theta - 4\sin^3\theta$$

(סימון: $x=\cos 20°$ ונציב $\theta=20°$:

המשך

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

$8x^3-6x^2-1=0$

נשאר להראות שהפולינום הזה אי-פריק,

אם הפולינום היה קיים שורש $\frac{r}{s}\in\mathbb{Q}$ כך ש הוא מתפרק

ולכן האפשרויות הן: $\pm1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$

מציבים ורואים שאף אחד מהם אינו שורש

$\Rightarrow [\mathbb{Q}[x]:\mathbb{Q}]=3$

ומכאן רואים שאי-אפשר לשלש זווית

- לבנות מצולע משוכלל בן n צלעות ≡ לבנות את הזווית $\frac{2\pi}{n}$

≡ לבנות את ρ_n.

ההרחבה $\mathbb{Q}[\rho_n]/\mathbb{Q}$ גלואה.

אפשר לבנות את ρ_n ⇔ $\phi(n)=[\mathbb{Q}[\rho_n]:\mathbb{Q}]=2^i$

אם $(n,m)=1$, $U_{nm}\cong U_n\times U_m$

כי $(\mathbb{Z}/nm\mathbb{Z})^\times\cong(\mathbb{Z}/n\mathbb{Z})^\times\times(\mathbb{Z}/m\mathbb{Z})^\times$.

$|U_{p^j}|=\phi(p^j)=p^{j-1}(p-1)$

$\phi(p_1^{i_1}p_2^{i_2}\cdots p_t^{i_t})=\prod(p_j-1)\cdot p_j^{i_j-1}$

<u>הגדרה:</u> ראשוני מהצורה $F_m=2^{2^m}+1$ נקרא "ראשוני פרמה".

<u>טענה:</u> כל ראשוני מהצורה 2^s+1 הוא ראשוני פרמה.

<u>הוכחה:</u> אחרת, יש t אי-זוגי וכך

$$2^s+1=2^{tt'}+1=(2^{t'}+1)(2^{tt'-t'}-2^{tt'-2t'}+\dots+1)$$

$t-1 \quad t-2 \quad t-3 \quad \dots \quad 0$

באינדקס האחרון הסימן יהיה + כי t אי-זוגי לכן $t-1$ זוגי ולכן הגורם סימן +..

בסתירה לראשוניות.

<u>למשל:</u> $2^{12}+1=(2^4+1)(2^8-2^4+1)$ ✓

4097 17 241

<u>מסקנה:</u> ניתן לבנות מצולע בן n צלעות ⇔ n הוא מהצורה $2^k\cdot p_1\cdots p_l$ כאשר p_i ראשוני פרמה.

16.01.14 הערה: ט"ו שבט שמח!

$F_0 = 3$

$F_1 = 5$

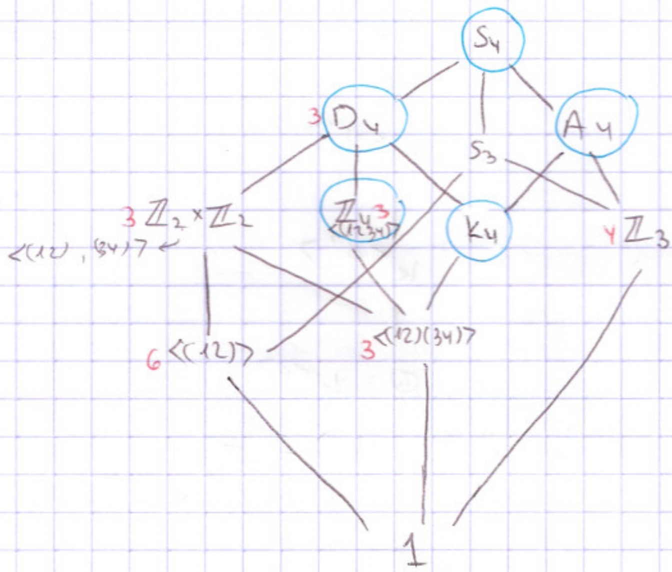
$F_2 = 17$

$F_3 = 257$

$F_4 = 65537$

מה שהוכחנו בהרצאה "7" לא נתן הוכחה של הדבר שלא ניתן לבנות מצולע משוכלל בן 7 צלעות..

נניח $[\mathbb{Q}[\alpha]:\mathbb{Q}] = 4$. נסמן ב-$E$ את שדה הפיצול.
$G = Gal(E/\mathbb{Q}) \le S_4$, מה האפשרויות



⇐ G איזומורפי לאחד מהנ"ל:

$$\begin{array}{ccccc} G_0 & G_1 & G_2 & G_3 & G_4 \\ \mathbb{Z}_4, & K_4, & D_4, & A_4, & S_4 \\ | & | & | & | & | \\ 1 & 1 & \langle(13)\rangle & \mathbb{Z}_3 & S_3 \end{array}$$

$\underbrace{\hphantom{\mathbb{Z}_4,\ K_4,\ D_4}}_{\alpha \text{ ניתן לבנייה}}$ $\underbrace{\hphantom{A_4,\ S_4}}_{\alpha \text{ לא ניתן לבנייה למרות ש-} [\mathbb{Q}[\alpha]:\mathbb{Q}]=4}$

מייצבים של α ב-G_i:

$$\begin{array}{ccc} E & & 1 \\ | & & | \\ \mathbb{Q}[\alpha] & & G_\alpha \\ | & & | \\ ? & & ? \\ | & & | \\ 1 & & G \end{array}$$

← שאלנו האם יש שדה ביניים, זה כמו לבדוק
האם יש חבורה ביניים, ברור בגלל... וכו'..

⇐ מסקנה: α מספר שחבורת גלואה שלו היא S_4 לא ניתן לבנייה..

תרגיל טוב למבחן

תרגיל: מצא α כך ש- $\mathbb{Q}[\alpha]/\mathbb{Q}$ שדה עם חבורת גלואה $\mathbb{Z}_4$.

פתרון: $\alpha = \rho_5$.

אנחנו יודעים למצוא חבורת גלואה לשורשי יחידה:

$$Gal(\mathbb{Q}[\rho_n]:\mathbb{Q}) = U_n$$

$U_{p^\alpha} \cong \mathbb{Z}_{p^{\alpha-1}(p-1)}$

$U_{2^\alpha} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$

תרגיל: מצאו שדה שגלואה שלו $\mathbb{Z}_8$:

$U_{17} \cong \mathbb{Z}_{16}$

$U_{32} \cong \mathbb{Z}_2 \times \mathbb{Z}_8 \quad = \langle \alpha, \beta \rangle$

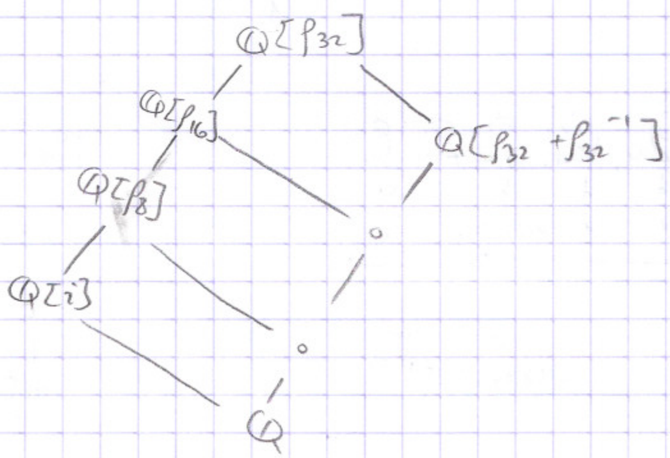
$Gal(\quad) = \langle \sigma \rangle \qquad \sigma: \rho \longmapsto \rho^3$

$$\begin{array}{l}
\mathbb{Q}[\rho_{17}] = k \\
\quad | \\
k^{\langle \sigma^8 \rangle} = \mathbb{Q}[\rho+\rho^{-1}] = \mathbb{Q}[\cos(\frac{2\pi}{17})] \\
\quad | \\
k^{\langle \sigma^4 \rangle} \\
\quad | \\
k^{\langle \sigma^2 \rangle} \\
\quad | \\
\mathbb{Q} = k^{\langle \sigma \rangle}
\end{array}$$

$Gal(\mathbb{Q}[\cos(\frac{2\pi}{17})] : \mathbb{Q}) \cong \mathbb{Z}_8$ //

$\alpha: \rho \longmapsto \rho^{-1}$

$\beta: \rho \longmapsto \rho^5$



העשרה- הוכחת קיום הסגור האלגברי.

הרחבה אלגברית = כל האיברים אלגבריים.

הרחבה נוצרת סופית = נוצרת ע"י מספר איברים סופי.

אלגברית נוצרת סופית $\Leftrightarrow$ ממימד סופי.

טענה: הרחבה אלגברית של הרחבה אלגברית היא אלגברית.

$$\begin{array}{ccc} k_0[\alpha] & \subseteq & E \\ | & & | \\ k_0 & \subseteq & k \\ & & |\infty \\ & & F \end{array}$$

הגדרה: שדה סגור אלגברית

≡ כל פולינום מעליו מתפצל

≡ לכל פולינום מעליו יש שורש

≡ אין הרחבות אלגבריות

≡ אין הרחבות ממימד סופי.

הגדרה: $\bar{F}$ הוא סגור אלגברי של F אם:

$\bar{F}$ אלגברי מעל F, וסגור אלגברית.

משפט: לכל שדה F יש סגור אלגברי

לכל שדה F יש הרחבה אלגברית E שיש בה שורש לכל פולינום עם מקדמים מ-F.

הוכחת הלמה: לכל פולינום ~~[illegible]~~ מתוקן מעל F, נתאים משתנה x_f.

נבנה חוג $R = F[\{x_f\}]$,

נבנה אידיאל $I = \langle \{f(x_f)\} \rangle$

$I \neq R$ כי $1 \notin I$ כי אחרת היינו יכולים לכתוב את

(כסכום סופי מספר סופי של פולי')

$1 = \sum g_i \cdot f_i(x_{f_i})$. הצגנו את 1 כצ"ל סופית של $f_i(x_{f_i})$,

נרחיב לשדה הפיצול של $\{f_i(x_f)\}_i$ ונשלח כל שורש של הפולינומים האלו

לפולינום והצבנו אותו.

לפי הלמה של צורן יש אידיאל מקסימלי $I \subset M \triangleleft R$.

R/M הוא שדה ונוצר סופית כי ~~[illegible]~~ R מעל F.

נשאר לנו.

ולהוכחת המשפט: נסמן $F = F_0$

לכל n, נניח את F_n.

F_{n+1} = הרחבה אלגברית שלה, יש שורש לכל פולינום מעל F_n.

כעת $E = \cup F_n$ סגור אלגברית.

(האם יש צורך בשלב? האם F_1 סגור אלגברית?)

$$\begin{array}{c}\vdots\\ | \\ F_2\\ |\\ F_1\\ |\\ F_0\end{array}$$