אלגברה מופשטת 3 - הרצאה מס' 9

K/F הרחבת גלואה.

$G = Gal(K/F)$

טענה: כל הרחבת גלואה (סופית) היא "פשוטה" (= נוצרת ע"י איבר יחיד).

הוכחה: להרחבה יש מספר סופי של שדות ביניים.

$K=F[\alpha]$ — F

נניח ש- F אינסופי.

עלינו להוכיח שאם $K=F[\alpha,\beta]$ אז קיים $\gamma\in K$ כך ש- $K=F[\gamma]$.

(במקרה הכללי, אם $K=F[\alpha_1,\dots,\alpha_n]$ אז ניקח $F'=F[\alpha_1,\dots,\alpha_{n-2}]$ ואז נקבל ש- $K=F'[\alpha_1,\dots,\alpha_n]$

ונקבל $K=F'[\gamma]$ כי K/F' גלואה ומסיימים באינדוקציה.)

נתבונן בשדות $F[\alpha+\mu\beta]$ לכל $\mu\in F$.

לפי הסופיות של מספר שדות הביניים, יש $\mu_1\neq\mu_2$ כך ש- $\underbrace{F[\alpha+\mu_1\beta]}_{L}=F[\alpha+\mu_2\beta]$

$\Leftarrow$ $\alpha+\mu_i\beta\in L$ $\Leftarrow$ $(\mu_1-\mu_2)\beta\in L$ $\Leftarrow$ $\beta\in L$ $\Leftarrow$ $\alpha\in L$

$\Leftarrow$ $L=K$ וזו הרחבה פשוטה.

הגדרה: תהי L/F הרחבה ספרבילית סופית.

אז יש לה סגור גלואה: שדה מינימלי K כך ש- $L\subset K$ כך ש- K/F גלואה.

הערה: קיום - כי ממימד סופי כי אפשר לקחת שפ"ע של המכפלה של הפול' המינימליים של יוצרים ידועים.

מסקנה: כל הרחבה ספרבילית סופית L/F יש מספר סופי של שדות ביניים: ניקח סגור גלואה k מעל F.

יש מספר סופי של שדות בין F ל- K $\Leftarrow$ יש מספר סופי של שדות בין F ל- L.

מסקנה: כל הרחבה ספרבילית סופית היא פשוטה. (אותה הוכחה).

"הלמה של שטייניץ"

<u>תזכורת:</u> תהי K/F הרחבת גלואה,

$K=F[\alpha_1,\alpha_2,\dots,\alpha_n]$, $\alpha_1,\dots,\alpha_n$ הם השורשים של פול׳ h

מעל F.

$$G=Gal(K/F)\leq S_n$$

<u>הערה:</u> אם h אי-פריק אז G פועלת טרנזיטיבית.

כי $F[\alpha_i]\cong F[\alpha_j]$ ואפשר להרים איזו׳ לאוטו׳.

שימו ♡ ש- $Tr(\alpha_i)=\alpha_1+\dots+\alpha_n\in F$

$N(\alpha_i)=\alpha_1\cdot\ldots\cdot\alpha_n\in F$

נסמן $\overset{\Delta}{disc}(h)=\prod_{i<j}(\alpha_i-\alpha_j)\underset{\neq 0}{\in} K$.

$$\forall\sigma\in G,\ \sigma(disc(h))=\prod_{i<j}(\sigma\alpha_i-\sigma\alpha_j)=\prod_{i<j}(\alpha_{\sigma_i}-\alpha_{\sigma_j})=$$

$$\sigma\alpha_i=\alpha_{\sigma_i}$$

$$=(sgn\,\sigma)\cdot\prod(\alpha_i-\alpha_j)$$

$\Leftarrow$ $\sigma(disc^2)=disc^2$ ולכן $disc^2\in F$.

הוכחנו מדויק יותר, $F[\Delta]=K^{G\cap A_n}$

<u>מסקנה:</u> $\Delta\in F\iff G\leq A_n$.

<u>דוגמה:</u> נניח שהפול׳ המינימלי ממעלה 2, למשל: $h=ax^2+bx+c$,

$$\Delta=\frac{2\sqrt{b^2-4ac}}{2a}=\frac{\sqrt{b^2-4ac}}{a}$$

<u>המקרה $[K:F]=3$:</u>

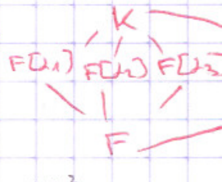
$h(x)=x^3-ax+b$ אי-פריק מעל F.

יש שורשים $\alpha_1,\alpha_2,\alpha_3$, ושדה פיצול $K=F[\alpha_1,\alpha_2,\alpha_3]$.

$G=Gal(K/F)\leq S_3$.

מקרה ש- $G=S_3$ או $G=A_3$.

$G=S_3$	$G=A_3$
$[K:F]=6$	$[K:F]=3$
$F[\alpha_1]$ לא גלואה	$F[\alpha_1]$ גלואה
$\Delta\notin F$	$\Delta\in F$



$$\Delta^2=\prod_{i<j}(\alpha_i-\alpha_j)^2=(-1)^{\binom{n}{2}}\prod_{i\neq j}(\alpha_i-\alpha_j)$$

צריך לחשב את

כפונק׳ של a ו- b.

12/12/13 משפט 3 מכבר מעגל

(שוב נניח ש- n כללי)
(מסמן

$$A=\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \cdots & \alpha_n^2 \\ \vdots & & & & \\ \alpha_1^{n-1} & \cdots & \cdots & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

$$\det(A)=\Delta$$

$$A\cdot A^t=\begin{pmatrix}\alpha_1^i & \cdots & \alpha_n^i\end{pmatrix}\begin{pmatrix}\alpha_1^j \\ \vdots \\ \alpha_n^j\end{pmatrix}=\left(tr(\alpha^{i+j})\right)\in M_n(F)$$

לכן
$$\Delta^2=|A|^2=|AA^t|=|(tr(\alpha_1^{i+j}))_{i,j}|$$

במקרה $n=3$, אז הפולינום המינימלי $h(\lambda)=\lambda^3-a\lambda+b$

$$\Delta^2=\begin{vmatrix} 3 & tr(\alpha) & tr(\alpha^2) \\ tr(\alpha) & tr(\alpha^2) & tr(\alpha^3) \\ tr(\alpha^2) & tr(\alpha^3) & tr(\alpha^4)\end{vmatrix}$$

$$\lambda^3-a\lambda+b=\prod(\lambda-\alpha_i)=\lambda^3-(\sum\alpha_i)\lambda^2+(\sum_{i<j}\alpha_i\alpha_j)\lambda-\prod\alpha_i$$

$$\Rightarrow \left.\begin{array}{l} \sigma_1=\alpha_1+\alpha_2+\alpha_3=0 \\ \sigma_2=\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3=-a \\ \sigma_3=\alpha_1\alpha_2\alpha_3=-b\end{array}\right\}\Rightarrow \begin{array}{l}\sigma_2=-\alpha_1^2-\alpha_1\alpha_2-\alpha_2^2 \\ \sigma_3=-\alpha_1\alpha_2(\alpha_1+\alpha_2)\end{array}$$

$$tr(\alpha_1^2)=\sigma_1^2-2\sigma_2=2a$$

$$tr(\alpha^3)=\cancel{\alpha_1^3}+\cancel{\alpha_2^3}-\cancel{\alpha_1^3}-\cancel{\alpha_2^3}-3\alpha_1^2\alpha_2-3\alpha_1\alpha_2^2$$

$$\Rightarrow tr(\alpha^3)=3\sigma_3=-3b$$

$$tr(\alpha^4)=\cancel{\alpha^4}+\cancel{\beta^4}-\cancel{\alpha^4}+4\alpha^3\beta+6\alpha^2\beta^2+4\alpha\beta^3+\cancel{\beta^4}=$$

$$=2(\underset{1}{\alpha^4}+\underset{2}{2\alpha^3\beta}+\underset{3}{3\alpha^2\beta^2}+\underset{2}{2\alpha\beta^3}+\underset{1}{\beta^4})$$

$$\Rightarrow tr(\alpha_1^4)=2\sigma_2^2=2a^2$$

$$\Rightarrow \Delta^2=\begin{vmatrix} 3 & 0 & 2a \\ 0 & 2a & -3b \\ 2a & -3b & 2a^2\end{vmatrix}=3(4a^3-9b^2)-8a^3=\boxed{4a^3-27b^2}$$

דוגמה: נניח ש- $h(\lambda)=\lambda^3-2\lambda+9$ אי-פריק מעל $\mathbb{Q}$

האם $\mathbb{Q}[x]/\langle x^3-2x+9\rangle$ גלואה מעל $\mathbb{Q}$?

נחשב דיסקרימיננטה: $\Delta^2 = 4\cdot 8 - 27\cdot 9^2 = -2111 \notin \mathbb{Q}^2$

$\Leftarrow$ $\mathbb{Q}[\sqrt{-2111}] \subseteq$ שדה הפיצול שהוא ממימד 6

שורשי יחידה

טענה: יהי F שדה. תהי $G \le F^\times$ חבורה סופית אז G ציקלית.

הוכחה: זו חבורה אבלית, יש אקספוננט,

$$e = \exp(G) = \mathrm{lcm}\{o(g) \mid g\in G\}$$

(זה e המינימלי כך ש- $\forall g\in G: g^e=1$) $e \le |G|$.

תרגיל: אם $\exp(G)=|G|$ אז G ציקלית.

$\Updownarrow$

בכל חבורה אבלית יש איבר מסדר $\exp(G)$ $\llcorner$

יהי $e=\exp(G)$. כל איברי G הם שורשים של הפולינום x^e-1.

$\Leftarrow$ $|G|\le e$ ולכן $|G|=e$.

שאלה: מהו הממד של $\mathbb{Q}[\rho_n]$?
$\swarrow$ שורש יחידה פרימיטיבי מסדר n.
(השאלה הזו היא מין מוטיבציה למה שאנחנו עושים עכשיו)

הגדרה: $\Phi_1(x) = x-1$

$\Phi_n(x) = \dfrac{x^n-1}{\prod_{\substack{d|n\\ d<n}} \Phi_d(x)}$ - "הפולינום הציקלוטומי מסדר n".

$x^n - 1 = \prod_{i=1}^{n}(x-\rho^i) =$ כאשר ρ שורש יחידה (...).

$$= \prod_{d|n}\prod_{(i,n)=d}(x-\rho^i)$$

טענה:
$$\Phi_n(x) = \prod_{(i,n)=1}(x-\rho^i)$$

(**הערה:** הסדר של ρ^i הוא $\frac{n}{(n,i)}$)

$n=12$: d	
1	1,5,
2	2,10
3	3,9
4	4,8
6	6
12	12

הוכחה: לפי הנחת האינדוקציה

$$\prod_{d|n}\Phi_d(x) = x^n - 1 = \prod_{d|n}\Big[\prod_{(i,n)=d}(x-\rho^i)\Big] =$$

$$\underset{i=jd}{=} \prod_{d|n}\Big[\prod_{(j,\frac{n}{d})=1}(x-\rho^{jd})\Big] \underset{i=1}{=} \boxed{\prod_{(i,n)=1}(x-\rho^i)} \prod_{\substack{d|n\\ 1<d}}\Phi_{n/d}(x)$$

$$\Rightarrow \Phi_n(x) = \boxed{}$$

מסקנה ד' סעיף משפט

מכאן ש- $\deg \Phi_n(x) = \phi(n)$.

מכאן גם ש- $\Phi_n(x) \in \mathbb{Q}[x]$: Φ_n הוא פולינום ולכן

$x^n-1 \mid \prod \Phi_n(x)$ ולכן $\mathbb{Q}[\rho] \Leftarrow$ זה מעל $\mathbb{Q}$.