הערה

נניח f_a=פולינום המינימלי של a(ספרבילי)

$$f_a=\prod_{i=0}^{m}\left(\lambda-a_i\right)=\lambda^n-\sum_{j=1}^{n}\sigma_j\left(a\right)\lambda^{n-1}+\cdots\pm\cdots+\left(-1\right)^n\prod_{j=1}^{n}\sigma_j\left(a\right)$$

$$\lambda^n-\mathrm{Tr}_{E/F}\left(a\right)\lambda^{n-1}+\cdots+\left(-1\right)^nN_{E/F}\left(a\right)$$

E שדה הפיצול של f_a מעל F.

הערה

נניח K/F הרחבת שדות כאשר $[K:F]=n$. אז כל איבר $a\in K$ מגדיר טרנספורמציה לינארית $A:K\to K$ לפי $A\left(w\right)=aw$ לכל $w\in K$. לכן יש לנו הומומורפיזם $\Phi:K\hookrightarrow M_n\left(F\right)$ לפי $\Phi\left(a\right)=A$.

הוכחה

נניח $b_1,\dots b_n$ בסיס של K מעל $ab_i=\sum_{j=1}^{n}\alpha_{ij}b_j$ $(\alpha_{ij}\in F)$, לכן עבור $A=\left(\alpha_{ij}\right)$,

$$ab_i=\sum_i\alpha_{ij}b_j=A\begin{pmatrix}0\\ \vdots\\ 1\\ \vdots\\ 0\end{pmatrix}\leftarrow i\text{'th place}$$

$$A\leftrightarrow\left(\alpha_{ij}\right)$$

$$A'\leftrightarrow\left(\alpha'_{kj}\right)$$

$$A'A=\left(\alpha'_{kj}\right)\left(\alpha_{ji}\right)=\left(\left(\sum_j\alpha'_{kj}\alpha_{ji}\right)\right)$$

$$a'ab_i=a'\left(\sum\alpha_{ji}b_j\right)=\sum_j\left(\sum_k\alpha_{ji}\alpha'_{kj}\right)=A'A\left(b_k\right)\qquad\forall b$$

לכן $a'aw\leftrightarrow A'A\left(w\right)$ לכל $w\in K$, ולכן Φ הומומורפיזם $\Phi\left(a'a\right)=\Phi\left(a'\right)\Phi\left(a\right)$.
מה הגרעין של Φ?

$$\ker\Phi=\{a|\forall_{w\in K}aw=0\}$$

אבל זה אומר שאם ניקח $w=1$ $\Longleftarrow$ $a=0$.

הערה

K שדה $\Longleftarrow A=\Phi\left(a\right)$ מטריצה אי סינגולרית $\forall_{0\neq a\in K}$.

כל A ניתן לכתוב בצורה של בלוקים: $\begin{pmatrix}A_1 & 0 & \cdots & 0\\ 0 & A_2 & 0 & \vdots\\ \vdots & 0 & \ddots & 0\\ 0 & \cdots & 0 & A_d\end{pmatrix}$ כאשר $A_i=\begin{pmatrix}0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1\\ & & & 0\\ -\alpha_0 & -\alpha_1 & \cdots & -\alpha_{n-1}\end{pmatrix}$

כאשר $p_i=\sum_{i=0l}\alpha_i\lambda^i$ הוא פולינום האופיני של A, שגם הפולינים המינימלי של A_i.

נניח $\mathrm{ord}\left(A_d\right)\geq\cdots\geq\mathrm{ord}\left(A_2\right)\geq\mathrm{ord}\left(A_1\right)$

$$p_1\left(A\right)=\begin{pmatrix}\overbrace{p_1\left(A_1\right)}^{=0} & & & \\ & p_1\left(A_2\right) & & \\ & & \ddots & \\ & & & p_1\left(A_d\right)\end{pmatrix}$$

לכן $p_1\left(a\right)\leftrightarrow p_1\left(A\right)$ מטריצה סינגולרית של K $\Longleftarrow p_1\left(A\right)=0\Longleftarrow\forall_i p_1\left(A_i\right)=0$

$\Longleftarrow A_1=A_2=\cdots=A_d$.

$$N\left(a\right)=\left(-1\right)^n\alpha_0^d=\left(\left(-1\right)^{n/d}\alpha_0\right)^d=\left|A_1\right|^d=\left|A\right|$$

$$\mathrm{Tr}\left(a\right)=d\left(-\alpha_{n-1}\right)=d\mathrm{Tr}\left(A_1\right)=\mathrm{Tr}\left(A\right)$$

פעם שעבר אמרנו $\mathrm{Tr}_{E/F}$ טרנס' לינארית מעל F, אבל $\dim_F F=1\Longleftarrow$ או $\mathrm{Tr}_{E/F}=0$ או $\mathrm{Tr}_{E/F}$ על. אבל אם $[E:F]=n$ אז $\mathrm{Tr}\left(1\right)=1+\cdots+1=n\neq0$ אם $\mathrm{char}\left(F\right)\nmid n$.

רוצים להוכיח $\exists_a\sum\sigma_i\left(a\right)\neq0$

למת דיריכלט Dirichlet

נניח $\sigma_1,\ldots\sigma_n$ אוטומורפיזמים של שדה E שונים. אם $\sum\limits_{i=1}^{t}a_i\sigma_i=0$ כפונקציה ($\left(\sum\alpha_i\sigma_i\right)\left(a\right)=$ $\sum a_i\sigma_i\left(a\right)$) אז כל $a_i=0$

הוכחה - באינדוקציה על t

אחרת ניקח $\sum\limits_{i=1}^{t}a_i\sigma_i=0$ עבור t מינימלי. אם $t=1$ אז $a_1\sigma_1=0\Longleftarrow\forall_{0\neq a\in E}a_1\sigma_1\left(a\right)=$ $0\Longleftarrow a_1=0$.

באופן כללי נניח $a_1\neq0$ כאשר $\sigma_1=1$(אפשר להפעיל σ_1^{-1}).

$$\forall_{ai\in A}\sum a_i\sigma_i\left(aa'\right)=0=\sum a_i\sigma_i\left(a\right)\sigma_i\left(a'\right)=0$$

$$\left(\sum a_i \sigma_i\left(a\right)\right) \sigma_t\left(a'\right) = 0\sigma_t\left(a'\right) = 0$$

$$\sum_{i=1}^{t} a_i \sigma_i\left(a\right)\left(\sigma_i\left(a'\right) - \sigma_f\left(a'\right)\right) = 0 = \sum_{i=1}^{t-1} a_i \sigma_i\left(a\right)\left(\sigma_i\left(a'\right) - \sigma_t\left(a'\right)\right)$$

לפי אינדוקציה על t כל מקדם $a_i\left(\sigma_i\left(a'\right) - \sigma_t\left(a'\right)\right) = 0 \Longleftarrow \forall_{a'} \sigma_i\left(a'\right) = \sigma_t\left(a'\right)$
$\Longleftarrow \sigma_i = \sigma_t$

$\blacksquare$

מסקנה

$\sigma_1, \ldots \sigma_n \in \mathrm{Gal}\left(E/F\right)$ בלתי תלויים במובן הלמה $\Longleftarrow 0 \neq \sum \sigma_i = \mathrm{Tr}_{E/F} \Longleftarrow$
$\exists_{a \in E} \mathrm{Tr}_{E/F}\left(a\right) \neq 0 \Longleftarrow \mathrm{Tr}_{E/F}$ על.

שימוש של דיריכלט עבור הנורמה

מתי $N\left(a\right) = 1$?
ברור: אם $a = \frac{b}{\sigma(b)}$ ו־$\mathrm{Gal}\left(E/F\right) = \langle\sigma\rangle$ אז

$$N\left(a\right) = \frac{\cancel{b}}{\cancel{\sigma\left(b\right)}} \frac{\cancel{\sigma\left(b\right)}}{\cancel{\sigma^2\left(b\right)}} \cdots \frac{\cancel{\sigma^{n-1}\left(b\right)}}{\cancel{\sigma^n\left(b\right)}} = 1$$

משפט 90 של פילברט

אם $\mathrm{Gal}\left(E/F\right) = \langle\sigma\rangle$ (מסדר n) ו־$N\left(a\right) = 1$ אז $a = \frac{b}{\sigma(b)}$ עבור איזשהו $b \in E$.

הוכחה

נגדיר

$$b_i = a\sigma\left(a\right)\sigma^2\left(a\right)\cdots\sigma^{i-1}\left(a\right)$$

$$\sigma\left(b_i\right) = \sigma\left(a\right)\sigma^2\left(a\right)\cdots\sigma^i\left(a\right) = \frac{b_{i+1}}{a}$$

$$b = \sum b_i$$

$$\sigma\left(b\right) = \sum \frac{\sigma\left(b_{i+1}\right)}{a} = \frac{b}{a}$$

(כי $\sigma\left(b_{n-1}\right)=N\left(a\right)=1$)

$$\therefore a=\frac{b}{\sigma\left(b\right)}$$

אבל $\sum b_i\sigma^i\neq 0$ לפי דיריכלט $\Longleftarrow$ קיים a' כך ש$b\neq 0$ $\surd$

הגדרה

נתון $a_1,\dots a_n$. השורשים של הפולינום f. נגדיר $d=\prod_{i>j}\left(a_i-a_j\right)$. אז לכל $\sigma\in\mathrm{Gal}\left(E/F\right)$ (E שדה פיצול), $\sigma\left(d\right)=\left(\mathrm{Sgma}\right)d$

(הוכחה: ברור עבור $\sigma=\left(ij\right)$ חילוף, אבל כל תמורה היא מכפלת חילופים).

זה מוכיח: טענה

$d\in F\iff\mathrm{Gal}\left(E/F\right)\subset A_n$ (כי $\sigma\left(d\right)=d\iff\sigma\in A_n$)

דוגמה

נניח $\deg f=3$

$$F\underbrace{\subset}_{2}F\left[\rho_3\right]\underbrace{\subset}_{1\text{ or }2}F\left[\rho_3,d\right]\underbrace{\subset}_{3}E\left[\rho_3\right]$$

($F\left[\rho_3,d\right]\subset E\left[\rho_3\right]$ היא הרחבה שורשית)