3. Норма и след

Нека E - кон. разш. поля F, т.е. $|E:F| = n < \infty$.

E - в.п. над F и $\dim_F E = n$. $\forall x \in E$ определяем

лин. оператор $\rho^x : E \to E$, $\rho^x(y) = xy$ (умн-е на x слева)

Нека $u_1, \dots, u_n$ - базис E над F и $A(x) = [\rho^x]$ в этой базе.

След и норма $x \in E$ в расширение E/F:

$$T_{E/F}(x) = tr(\rho^x) = tr(A(x)) \text{ и } N_{E/F}(x) = \det(\rho^x) = \det(A(x))$$

Хар. мн-н $x \in E$: $\chi^x_{E/F}(t) = \det(tI - A(x)) =$

$$= t^n - T_{E/F}(x)\, t^{n-1} + \dots + (-1)^n N_{E/F}(x). \qquad (*)$$

Все они не зависят от выбора базиса E над F.

<u>Пример</u> $E=\mathbb{C}$, $F=\mathbb{R}$ $x=a+bi$

В базисе $1, i$ имеем

$$A(x)=\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \Rightarrow$$

$$T_{\mathbb{C}/\mathbb{R}}(x)=tr(A(x))=2a$$

$$N_{\mathbb{C}/\mathbb{R}}(x)=\det(A(x))=a^2+b^2$$

$$\chi^x_{\mathbb{C}/\mathbb{R}}(t)=\det(tI-A(x))=t^2-2at+a^2+b^2$$

<u>Упр 1</u> Пусть d свободно от кв-ов, $x=a+b\sqrt{d}\in E$, где $E=\mathbb{Q}[\sqrt{5}]$. Найдите $A(x)$, $T_{E/\mathbb{Q}}(x)$, $N_{E/\mathbb{Q}}(x)$, $\chi^x_{E/\mathbb{Q}}$.

Предл 1 (элем. св-ва следа и нормы) $\forall x, y \in E, \forall a \in F$

1) $T_{E/F}(x+y) = T_{E/F}(x) + T_{E/F}(y)$, $T_{E/F}(ax) = a\,T_{E/F}(x)$

2) $N_{E/F}(xy) = N_{E/F}(x)\,N_{E/F}(y)$, $N_{E/F}(ax) = a^n N_{E/F}(x)$.

Д-во: Св-ва следа и опр-ля мн-ца.

Предл 2 (транзитивность следа) $F \subseteq K \subseteq E$, $x \in E$

$$T_{E/F}(x) = T_{K/F}(T_{E/K}(x))$$

Упр 2 Д-ть предл 2.

Транзитивность нормы тоже имеет место, но при доп. предположениях!

Даже ρ^x определен также мин. анн. мн-н $\mu^x_{E/F}(t)$.

Как он связан с мин. мн-ном $f(t)\in F[t]$ для x (в смысле т. Гаусса), т.е. неразл. мн-н над F, т.ч. $f(x)=0$.

Это одно и то же, т.к. $f(\rho^x)\cdot \underset{E}{\underset{\cap}{1}} = f(x) \Longrightarrow$

$f(\rho^x)=0 \iff f(x)=0$.

в вл. E над F. в E

Далее, $f(t)=\mu^x_{E/F}(t)$ — унитарный мн-н

<u>Лемма 1</u> $\chi_{E/F}(t)=\mu_{E/F}(t)^r$, где $r=|E:\overset{\substack{K\\ \parallel}}{F(x)}|$

<u>Д-во:</u> пусть вначале $r=1$, т.е. $E=F(x)=F[x]=K$ (всп. т. Гаусс).

$\mu^x_{E/F}=\mu^x_{K/F}$ делит $\chi^x_{K/F}$ и $\deg \mu^x_{K/F}=|K:F|=d$.

$\Rightarrow \mu^x_{K/F}=\chi^x_{K/F}$ из-за унитарности обоих мн-нов.

Пусть $1, x, \ldots x^{d-1}$ – базис K над F

и $e_1, \ldots e_r$ – базис E над K.

Если $\mu^x_{L/F} = t^d + \alpha_1 t^{d-1} + \ldots + \alpha_d$, $\alpha_i \in F$, то

$p^x: 1 \to x, x \to x^2 \ldots x^{d-1} \to x^d = -\alpha_1 x^{d-1} - \ldots - \alpha_d$

Поэтому в базисе $(\underbrace{e_1, e_1 x, \ldots e_1 x^{d-1}}_{K_1}; \underbrace{e_2, e_2 x, \ldots e_2 x^{d-1}}_{K_2}, \ldots)$ $\ldots$

$$p^x\Big|_{K_i} = \begin{pmatrix} 0 & & & -\alpha_d \\ 1 & \ddots & & \vdots \\ & \ddots & & \\ & & 1 & -\alpha_1 \end{pmatrix} \Rightarrow (p^x \text{ „не трогает" } e_i) \Rightarrow$$

$$E = \bigoplus_{i=1}^{r} (\underbrace{Fe_i + Fe_i x + \ldots + Fe_i x^{d-1}}_{p^x - \text{инв. подпр-во.}}) \Rightarrow \chi^x_{E/F} = (\mu^x_{E/F})^r$$

<u>Следствие</u>. Если $x_1 \ldots x_d$ – корни $\mu^x_{F/E}$ в алг. зам. $\overline{F}$ поля F, то

$\mu^x_{E/F}(t) = \prod_{i=1}^{d} (t - x_i)$, $\chi^x_{E/F} = (\mu^x_{E/F})^r$, $T_{E/F}(x) = \frac{n}{d} \sum_{i=1}^{d} x_i$, $N_{E/F}(x) = \prod_{i=1}^{d} x_i^{n/d}$.

Теорема 1 Пусть A – обл. целостности, $F = Q(A)$ – поле частных, E/F – кон. расширение, $B = \overline{A}^E$ – целое замыкание, $x \in B$. Тогда $\chi_{E/F}(t), \mu_{E/F}(t) \in \overline{A}^{Q(A)}[t]$, т.е. коэф-ты этих мн-нов целые над A.

Д-во: $x \in E$ – целый над A $\Rightarrow$

$$x^n = a_1 x^{n-1} + \ldots + a_n, \; a_i \in A$$

$h(t) = t^n - a_1 t^{n-1} - \ldots - a_n \in A[t] \subset F[t]$ делится на $\mu^x_{E/F}(t)$. Если $x_1, \ldots x_d \in \overline{F}$ – корни $\mu^x_{E/F}(t)$ $\Rightarrow$ они корни и $h(t)$ $\Rightarrow$ целые над A.

По т. Виета коэф-ты $\mu^x_{E/F}(t)$ выражаются через $x_1 \ldots x_d$ $\Rightarrow$ целые над A. Т.к. $\chi = \mu^r$, то все доказано ∎

Следствие 1 Если A целозамкнутая область, то $\chi^{x}_{L/F}(t)$ и $\mu^{x}_{L/F}(t) \in A[t]$.

Следствие 2 K – алг. числовое поле. Тогда $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

Д-во: Для $A = \mathbb{Z}$ и $E = \mathbb{Q}[a]$ имеем $\mu_{E/\mathbb{Q}}(t) = t - a$ $\Rightarrow a$ цел над $\mathbb{Z} \Rightarrow a \in \mathbb{Z}$.

Добавим теперь условие сепарабельности расширения, т.е $\forall x \in E$ сепарабелен над F, т.е. $\mu_{E/F}(t)$ не имеет кратных корней.

Напоминание (из теории Галуа): E/F сепарабельно и $|E:F|=n$ $\Rightarrow$ $\exists$ ровно n инъект. вложений $\sigma_i : E \to \overline{F}$, $i=1\ldots n$, таких что $\sigma_i|_F = id$.

Кроме того, любое сепар. расш. просто, т.е. $\exists\, z \in E : E = F(z)$. Поэтому σ_i задаются так: $\sigma_i|_F = id$ и $\sigma_i(z) = z_i$, где z_i, $i=1..n$, - корни $\mu^{z}_{E/F}(t)$.

Если расш. E поля F ещё и нормально (т.е. каждый неразл. мн-н из $F[x]$ расскл. в E на лин. мн-ли), то оно явл-ся расш. Галуа $\Rightarrow$ σ_i индуцируют разл. автоморфизмы поля E (тожд. на F).

<u>Предл 3</u> Пусть E/F — кон сепар. расш. $|E:F|=n$ и $\sigma_i : E \to \overline{F}$, $i=1..n$, $\sigma_i|_F = id$. Тогда $\forall x \in E$

$$\chi^x_{E/F}(t) = \prod_{i=1}^n (t - \sigma_i(x)),\ T_{E/F}(x) = \sum_{i=1}^n \sigma_i(x),\ N_{E/F}(x) = \prod_{i=1}^n \sigma_i(x).$$

<u>Д-во:</u> Пусть $x_1, \ldots x_d$ — корни (разл) $\mu^x_{E/F}(t)$ в $\overline{F}$. Тогда каждое из d-разл. вл-й τ_j $F(x)$ в $\overline{F}$ от. ет x в $\overline{\text{сущ}}$. эл-т. x_j и τ_j продолж до n/d вложений E в $\overline{F}$.

Тогда набор $\sigma_1(x), \ldots \sigma_n(x)$ состоит из $\tau_j(x) = x_j$, перечисленных по n/d раз. По следствию из л. 1

$$\chi^x_{E/F}(t) = \left(\mu^x_{E/F}(t)\right)^{n/d} = \left(\prod_{j=1}^d (t - x_j)\right)^{n/d} = \left(\prod_{j=1}^d (t - \tau_j(x))\right)^{n/d} =$$

$$= \prod_{i=1}^n (t - \sigma_i(x)).$$ Ф-лы для след и нормы следуют ▣

<u>Следствие</u> (Транзитивность нормы). Пусть $F \subseteq K \subseteq E$ — башня сепараб. расширений. Тогда $\forall x \in E$ $N_{E/F}(x) = N_{K/F}(N_{E/K}(x))$.

<u>Д-во:</u> В $\overline{F}$ можно выбрать норм. расширение L поля F, т.ч. $L \supseteq E$. Обозн. через $\sigma_1, \dots, \sigma_n$ разл. F-вложения K в L, а через $\tau_1, \dots, \tau_m$ разл. K-вложения E в L. Т.к. L/F нормально, то σ_i и τ_j продолжаются до автоморфизмов L, поэтому их можно перемножать. Имеем $N_{K/F}(N_{E/K}(x)) = \prod\limits_{i=1}^{n} \sigma_i \left(\prod\limits_{j=1}^{m} \tau_j(x)\right) = \prod\limits_{i=1}^{n} \prod\limits_{j=1}^{m} \sigma_i(\tau_j(x))$ $= \prod\limits_{i=1}^{n} \prod\limits_{j=1}^{m} (\sigma_i \circ \tau_j)(x)$. Каждое из отоб-й $\sigma_i \circ \tau_j$ — F-вл-е E в L,

их кол-во $= n\cdot m = |E:F|$. Осталось заметить, что все они различны. Действ-но, если $\sigma_i \circ \tau_j = \sigma_k \circ \tau_l$, то $\sigma_i \circ \tau_j \big|_K = \sigma_k \circ \tau_l \big|_K$, получаем $\sigma_i = \sigma_k$. Отсюда $\tau_j = \tau_l$ при ограничении на E. Значит,

$$N_{E/F} = \prod_{i} (\sigma_i \circ \tau_j)(x) \quad \blacksquare$$

<u>Пример</u> (использования предл. 3) У расш. $\mathbb{C}/\mathbb{R}$ два автоморфизма (тожд. на $\mathbb{R}$): id и сопряжение

$\Rightarrow$ для $x = a + bi$ имеем

$$\chi^{x}_{\mathbb{C}/\mathbb{R}}(x) = (t - x)(t - \overline{x}) = t^2 - 2at + a^2 + b^2$$

$$T^{x}_{\mathbb{C}/\mathbb{R}}(x) = x + \overline{x} = 2a \qquad N^{x}_{\mathbb{C}/\mathbb{R}}(x) = x \cdot \overline{x} = a^2 + b^2.$$

Теорема 2 (критерий сепарабельности). Конечное расширение E поля F сепарабельно $\Longleftrightarrow$ билинейная форма $E \times E \to F$, $(x,y) = \mathrm{T}_{E/F}(xy)$ невырождена (т.е. $(x, E) = 0 \Rightarrow x = 0$)

Д-во (см., напр., Гуьбарев, лекции по алг. теории чисел).