5. Норма и след

Пусть E – кон. расш. поля F, т.е. $|E:F| = n < \infty$.

E – в.п. над F и $\dim_F E = n$. $\forall x \in E$ определен лин. оператор $\rho^x : E \to E$, $\rho^x(y) = xy$ (умн-е на x слева)

Пусть $u_1, \dots, u_n$ – базис E над F. и $A(x) = [\rho^x]$ в этом базе

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

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

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

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

Все они не зависят от выбора базиса E над F.

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

В базисе $1, i$ имеем

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

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

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

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

Упр 1 Пусть d свободно от кв-тов, $x = a + b\sqrt{d} \in E$, где $E = \mathbb{Q}[\sqrt{d}]$. 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-я мн-ли.

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

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

Упр 2 Д-ть предл 2.

Транзитивность нормы тоже имеет место, но при доп. предположениях (см. далее)

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

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

Это одно и то же, т.к $f(\rho^x)(1) = f(x) \cdot 1 = f(x)$

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

В вл. E над F. в E

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

Лемма 1 $\chi_{E/F}(t) = \mu_{E/F}(t)^r$, где $r = |E : F(x)|$

Д-во: Пусть сначала $r = 1$, т.е. $E = F(x) = F[x] = K$ (вспом. т. Галуа).

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

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

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

и $e_1 \dots e_r$ – базис E над K.

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

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

Получим в базисе $\underbrace{(e_1, e_1 x, \dots e_1 x^{d-1}}_{K e_1}, \underbrace{e_2, e_2 x, \dots e_2 x^{d-1}}_{K e_2}, \dots)$

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

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

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

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

Теорема Пусть A – ОБЛ. целостности, $F = Q(A)$ – поле частных E/F – Кон. расширение, $B = \overline{A}^{E}$ – целое замыкание $x \in B$. Тогда $\chi^{x}_{E/F}(t), \mu^{x}_{E/F}(t) \in \overline{A}^{Q(A)}[t]$, т.е Коэф. эти мн-нов целые над A.

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

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

$h(t) = t^n - a_1 t^{n-1} - \dots - a_n \in A[t] \subset F[t]$ делится на $\mu^{x}_{E/F}(t)$. Если $x_1, \dots x_d \in \overline{F}$ – корни $\mu^{x}_{E/F}(t)$

$\Rightarrow$ они корни и $h(t) \Rightarrow$ целые над A.

По т. Виета коэф. $\mu^{x}_{E/F}(t)$ выражаются через $x_1 \dots x_d$

$\Rightarrow$ целые над A. Т.к. $\chi = \mu^{r}$, то все доказано ∎

Следствие 1 Если A – целозамкнутая область целостности, то $\chi^x_{L/F}(t)$ и $\mu^x_{L/F}(t) \in A[t] \Leftrightarrow x$ цел над A.

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 $\mu^a_{E/\mathbb{Q}}(t) = t - a$ и a цел над $\mathbb{Z} \underset{\text{сл. 2}}{\Rightarrow} a \in \mathbb{Z}$.

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

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

Кроме того, любое сепар. расш. прост, 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 $\mu_{E/F}^{z}(t)$.

Если расш. E поля F сепарабельно и нормально (т.е. каждый неприв. многочл. из $F[x]$ расп. в E не мин. мн-ов), то оно наз. расш. Галуа $\Rightarrow \sigma_i$ индуцируют разл. автоморфизмы поля E (тождест. на F).

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

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

(разл)

Д-во: Пусть $x_1,\dots x_d$ – корни $\mu^x_{E/F}(t)$ в $\overline{F}$. Тогда каждое из d-разл. вл-й τ_j $F(x)$ в $\overline{F}$ от-ет x в ушк. за-т. x_j и τ_j продолж до n/d включений E в $\overline{F}$. Тогда набор $\sigma_1(x),\dots,\sigma_n(x)$ состоит из $\tau_j(x) = x_j$, перечисленных по n/d раз. По следствию из п. 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-ии для следа и нормы следуют ▣

Следствие (транзитивность нормы). Пусть $F \subseteq K \subseteq E$ — башня сепарабельных расширений. Тогда $\forall x \in E \quad N_{E/F}(x) = N_{K/F}(N_{E/K}(x))$.

Д-во: 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 $N_{K/F}(N_{E/K}(x)) = \prod_{i=1}^{n} \sigma_i \left(\prod_{j=1}^{m} \tau_j(x) \right) = \prod_{i=1}^{n} \prod_{j=1}^{m} \sigma_i(\tau_j(x)) = \prod_{i=1}^{n} \prod_{j=1}^{m} (\sigma_i \circ \tau_j)(x)$. Каждое из отображений $\sigma_i \circ \tau_j$ — F-вложение E в L,

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

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

Пример (использовали пред. 3) У расш. $\mathbb{C}/\mathbb{R}$ две автоморфизма (тождество $\mathbb{R}$): id и сопряжение

$\Rightarrow$ для $x = a + bi$ имеем

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

$$T_{\mathbb{C}/\mathbb{R}}(x) = x + \bar{x} = 2a, \quad N_{\mathbb{C}/\mathbb{R}}(x) = x \cdot \bar{x} = a^2 + b^2.$$

Теорема 2 (критерий сепарабельности). Конечное расширение E поля F сепарабельно $\Leftrightarrow$ билинейная форма $E \times E \to F$, $(x, y) = T_{E/F}(xy)$ невырожденная (т.е. $(x, E) = 0 \Rightarrow x = 0$)

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