
Лекция №3 (17.09.20)

---

1. Предварительные сведения из теории конечных полей.

1.4. Нормы и следы.

Концепция норм и следов является важным инструментом в изучении расширений конечных полей. Пусть E/F – расширение Галуа, $G = Gal(E/F)$ – группа Галуа соответствующего расширения. Определим след и норму элемента $u \in E$:

$$\mathrm{Tr}_{E/F}(u) = \sum_{\tau \in G} \tau(u), \quad \mathrm{N}_{E/F}(u) = \prod_{\tau \in G} \tau(u).$$

Если $F = \mathbb{F}_q$, $E = \mathbb{F}_{q^n}$, то $G = \langle \sigma \rangle$, где $\sigma : x \mapsto x^q$. Тогда для любого $\alpha \in E$ справедливо:

$$\mathrm{Tr}_{E/F}(\alpha) = \sum_{k=0}^{n-1} \alpha^{q^k}, \quad \mathrm{N}_{E/F}(\alpha) = \prod_{k=0}^{n-1} \alpha^{q^k}.$$

Если $F = \mathbb{F}_p$, то обычно записывают $\mathrm{Tr}_E(\alpha)$, $\mathrm{N}_E(\alpha)$ и называют *абсолютной нормой и следом* элемента α.

Лемма 1. *Пусть $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ – неприводимый многочлен над $\mathbb{F}_q$ и пусть α – корень f, такой, что $f = m_\alpha$ и $E = F(\alpha) = \mathbb{F}_{q^n}$. Тогда*

$$\mathrm{Tr}(\alpha) = -a_{n-1}, \quad \mathrm{N}(\alpha) = (-1)^n a_0.$$

Предложение 1. *Пусть $F = \mathbb{F}_q$ и $E = \mathbb{F}_{q^n}$. Тогда функция следа $\mathrm{Tr}_{E/F}$ является линейным отображением $E \to F$ и обладает следующими свойствами:*

1. $\mathrm{Tr}(\alpha^q) = \mathrm{Tr}(\alpha)$ *для произвольного* $\alpha \in E$.
2. $\mathrm{Tr}(a) = na$ *для произвольного* $a \in F$.
3. $\mathrm{Tr}(\gamma) = 0$ *тогда и только тогда, когда* $\gamma = \alpha^q - \alpha$ *для некоторого* $\alpha \in E$.

В рамках предыдущих обозначений отображение $\phi : \beta \mapsto \phi_\beta$ является изоморфизмом, отображающим F-векторное пространство E в дуальное к нему пространство $\mathrm{Hom}_F(E, F)$, где $\phi_\beta : \alpha \mapsto \mathrm{Tr}_{E/F}(\alpha\beta)$.

Рассмотрим отображение $T : E \times E \to F$, $T(\alpha, \beta) = \mathrm{Tr}_{E/F}(\alpha\beta)$, которое определяет след билинейной формы. Билинейность T легко следует из линейности следа.

Определение 1. *Дискриминант n элементов $\alpha_1, \cdots, \alpha_n \in E$ определяется следующим образом:*

$$\triangle_{E/F}(\alpha_1, \cdots, \alpha_n) = \begin{vmatrix} \mathrm{Tr}(\alpha_1\alpha_1) & \mathrm{Tr}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}(\alpha_1\alpha_n) \\ \mathrm{Tr}(\alpha_2\alpha_1) & \mathrm{Tr}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}(\alpha_2\alpha_n) \\ \cdots & \cdots & \cdots & \cdots \\ \mathrm{Tr}(\alpha_n\alpha_1) & \mathrm{Tr}(\alpha_n\alpha_2) & \cdots & \mathrm{Tr}(\alpha_n\alpha_n) \end{vmatrix}$$

Теорема 2. *Пусть $F = \mathbb{F}_q$ и $E = \mathbb{F}_{q^n}$. След билинейной формы $T : E \times E \to F$ является невырожденным. Кроме того, элементы $\alpha_1, \cdots, \alpha_n \in E$ образуют базис расширения E/F тогда и только тогда, когда $\triangle_{E/F}(\alpha_1, \cdots, \alpha_n) \neq 0$.*

Следствие 1. *Пусть $F = \mathbb{F}_q$ и $E = \mathbb{F}_{q^n}$ и $\alpha_1, \cdots, \alpha_n \in E$. Тогда $\alpha_1, \cdots, \alpha_n$ образуют базис E/F тогда и только тогда, когда*

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_n^q \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots & \alpha_n^{q^{n-1}} \end{vmatrix} \neq 0.$$

Предложение 3. *Пусть $F = \mathbb{F}_q$ и $E = \mathbb{F}_{q^n}$. Тогда функция нормы $\mathrm{N}_{E/F}$ является мультипликативным отображением $E \to F$ и обладает следующими свойствами:*

1. $\mathrm{N}(\alpha) = 0$ *тогда и только тогда, когда* $\alpha = 0$.
2. $\mathrm{N}(\alpha^q) = \mathrm{N}(\alpha)$ *для произвольного* $\alpha \in E$.
3. $\mathrm{N}(a) = a^n$ *для произвольного* $a \in F$.
4. $\mathrm{N}(\gamma) = 1$ *тогда и только тогда, когда* $\gamma = \alpha^{q-1}$ *для некоторого* $\alpha \in E$.

Предложение 4 (Формула транзитивности)**.** *Пусть E, F, K – конечные поля и $F \subseteq K \subseteq E$. Тогда для $\alpha \in E$ выполняются следующие условия:*

$$\mathrm{Tr}_{E/F}(\alpha) = \mathrm{Tr}_{K/F}(\mathrm{Tr}_{E/K}(\alpha)), \quad \mathrm{N}_{E/F}(\alpha) = \mathrm{N}_{K/F}(\mathrm{N}_{E/K}(\alpha)).$$