
Лекция №7 (29.10.20)

---

3. Нормальные базисы.

3.1. Фундаментальные результаты.

Как известно, любое расширение Галуа E/F допускает существование нормального базиса. *Нормальным базисом* поля $E = \mathbb{F}_{q^n}$ над $F = \mathbb{F}_q$ называется базис $B = \{\alpha_0, \ldots, \alpha_{n-1}\}$ следующего вида:

$$\alpha_0 = \alpha, \alpha_1 = \alpha^q, \ldots, \alpha_{n-1} = \alpha^{q^{n-1}}.$$

При этом α называется *образующей нормального базиса* или *свободным элементом* E/F. Таким образом, все элементы нормального базиса имеют один и тот же минимальный многочлен, который будем называть *минимальным многочленом базиса* B и обозначать m_B.

Теорема 1 (О нормальном базисе)**.** *$E = \mathbb{F}_{q^n}$ имеет нормальный базис над $F = \mathbb{F}_q$.*

Пример 1. *Буду рассматривать на паре + расскажу про обобщение.*

Теорема 2 (Орэ)**.** *Пусть q – степень простого числа p, n – положительное целое, такое, что $n = p^a m$ и $p \nmid m$. Тогда число нормальных базисов поля $\mathbb{F}_{q^n}/\mathbb{F}_q$ равно*

$$\frac{q^n}{n} \prod_{d|m} \left(1 - q^{-\mathrm{ord}_d(q)}\right)^{\frac{\varphi(d)}{\mathrm{ord}_d(q)}}.$$

Лемма 1. *Пусть $E = \mathbb{F}_{q^n}$, $F = \mathbb{F}_q$ и $\alpha \in E$. Тогда α является образующей нормального базиса E/F тогда и только тогда, когда*

$$\begin{vmatrix} \alpha & \alpha^q & \ldots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & \ldots & \alpha \\ \ldots & \ldots & \ldots & \ldots \\ \alpha^{q^{n-1}} & \alpha & \ldots & \alpha^{q^{n-2}} \end{vmatrix} \neq 0.$$

Теорема 3. *Пусть* $E = \mathbb{F}_{q^n}$, $F = \mathbb{F}_q$ *и* $\alpha \in E$. *Тогда* α *является образующей нормального базиса* E/F *тогда и только тогда, когда многочлены* $f(X) = X^n - 1$ *и* $g(X) = \alpha^{q^{n-1}} X^{n-1} + \ldots + \alpha^q X + \alpha$ *в* $E[X]$ *являются взаимно простыми.*

Следствие 1. *Пусть* $E = \mathbb{F}_{q^n}$, $F = \mathbb{F}_q$, $n = p^a$ *и* $p = \mathrm{char}F$. *Тогда элемент* α *является образующей нормального базиса* E/F *тогда и только тогда, когда* $Tr_{E/F}(\alpha) \neq 0$.

Отмечу некоторые замечания на паре.

Теорема 4. *Поле* $\mathbb{F}_{q^n}$ *имеет примитивный нормальный базис над* $\mathbb{F}_q$, *то есть существует образующая нормального базиса* ω, *которая одновременно является примитивным элементом в* $\mathbb{F}_{q^n}$.