
Лекция №5 (08.10.20)

---

2. Явное построение конечных полей.

2.3. Расширения степени, делящей $q-1$.

В этом параграфе мы покажем, как можно построить расширения $F = \mathbb{F}_q$ степени $n|q-1$. Как мы увидим далее, существует неприводимый двучлен степени n над $\mathbb{F}_q$, в этом случае: если ω – примитивный элемент в $\mathbb{F}_q$, то $X^n - \omega$ – неприводим.

Теорема 1. *Пусть $f_1(X), \dots, f_N(X)$ – различные, унитарные, неприводимые многочлены степени m порядка e над полем $\mathbb{F}_q$ и пусть $t \geq 2$ – произвольное целое число, удовлетворяющее условию: если p – простой делитель t, то p делит e, но не делит $\frac{q^m-1}{e}$. Также предположим, что $q^m \equiv 1 \pmod 4$, если $t \equiv 0 \pmod 4$. Тогда $f_1(X^t), \dots, f_N(X^t)$ – различные унитарные неприводимые многочлены степени mt порядка et над $\mathbb{F}_q$.*

Теорема 2. *Пусть $t \geq 2$ – целое и $c \in \mathbb{F}_q^\times$ – элемент порядка e. Тогда двучлен $g(X) = X^t - c$ является неприводимым над $\mathbb{F}_q$ тогда и только тогда, когда выполняются следующие условия:*

1. *Если p – простой делитель t, то $p|e$, но $p \not| \frac{q^m-1}{e}$.*
2. *$q \equiv 1 \pmod 4$, если $t \equiv 0 \pmod 4$.*

Отметим два специальных случая этой теоремы.

Следствие 1. *Пусть ω – примитивный элемент поля $\mathbb{F}_q$ и пусть t – делитель $q-1$. Тогда $X^t - \omega$ – неприводимый многочлен порядка $(q-1)t$ над $\mathbb{F}_q$.*

Следствие 2. *Пусть r – простое число, $c \in \mathbb{F}_q^\times$ – элемент, не являющийся r-й степенью. Кроме того, предположим $q \equiv 1 \pmod 4$, если $r = 2$ и $n \geq 2$. Тогда $X^{r^n} - c$ – неприводимый многочлен над $\mathbb{F}_q$ для любого положительного целого n.*

2.4. Расширения произвольной степени.

Теперь мы приступим к решению задачи построения расширения произвольной степени n над $F = \mathbb{F}_q$, где q – произвольная степень простого числа. Как уже было сказано, мы всегда можем построить $\mathbb{F}_{q^n}$ с помощью последовательности расширений простой степени. Таким образом, достаточно рассмотреть случай, когда $n = r$ для некоторого простого r. Мы используем индукцию по r. В предыдущих двух параграфах мы рассматривали случаи, когда $r|(q-1)$ или r равно характеристики поля $\mathbb{F}_q$, то есть $r = p$. В частности, мы решили проблему для $r = 2$. Соответственно, будем предполагать, что $r \geq 3$ – простое, отличное от p, не делящее $q - 1$. Построение расширения F степени $s = r^a$, где a – произвольное целое > 0, я расскажу на паре.

Лемма 1. *Пусть f – неприводимый многочлен степени m над F, α – его корень. Пусть g – неприводимый многочлен степени n над F, β – его корень. Предположим, что m и n – взаимно просты. Тогда $E = F(\alpha, \beta) = F(\alpha + \beta)$ и $h = m_{\alpha+\beta}$ – неприводимый многочлен степени mn над F.*