10.1. Расширения степени p^k.

Пусть $F = \mathbb{F}_q$ - поле характеристики *p*. В этом параграфе мы покажем, как построить расширения *F* степени p^k. Функция следа может быть использована для того, чтобы найти неприводимые многочлены степени p^k над *F*.

Сперва рассмотрим случай, когда *k* = 1. Отметим следующий результат теории Галуа: пусть *E*/*F* – расширение Галуа простой степени *p* поля *F* характеристики *p*. Тогда существует элемент $b \in E$, такой, что *E* = *F*(*b*), где $a := b^p - b \in F$. Это влечет, что минимальный многочлен элемента *a* есть $X^p - X - a$, который даст нам желаемый неприводимый многочлен.

Лемма: Пусть *a* – элемент поля $F = \mathbb{F}_q$, где *q* – степень простого числа *p*. Тогда многочлен $X^p - X - a$ приводим над *F* тогда и только тогда, когда имеет корень в *F*.

Теорема: Пусть *a* – элемент поля $F = \mathbb{F}_q$, где *q* – степень простого числа *p*. Тогда многочлен $X^p - X - a$ неприводим над *F* тогда и только тогда, когда абсолютный след $\mathrm{Tr}_{\mathbb{F}_p}(a) \neq 0$.

Таким образом, мы можем построить расширение $\mathbb{F}_p$ степени *p*. Если нам необходимо построить расширение степени $n = p^k$ для некоторого целого $k \geq 2$, то мы можем использовать данную теорему рекурсивно.

Теорема: Пусть $F = \mathbb{F}_q$ - поле характеристики *p*, $a \in F$ - элемент с абсолютным следом, отличным от нуля, и пусть α - корень многочлена $f = X^p - X - a$. Тогда $a\alpha^{p-1}$ - элемент в $E = F(\alpha)$ с абсолютным следом, отличным от нуля. Следовательно, $X^p - X - a\alpha^{p-1}$ - неприводимый многочлен над *E*.

Теорема: Пусть $f = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ - неприводимый многочлен над $F = \mathbb{F}_q$, где *q* – степень простого числа *p*, пусть *b* – элемент *F*. Тогда многочлен $g = f(X^p - X - b)$ неприводим над *F* тогда и только тогда, когда $\mathrm{Tr}_{\mathbb{F}_p}(nb - a_{n-1}) \neq 0$.

Пример: Построим неприводимый многочлен степени 2*p* над $\mathbb{F}_p$, где $p \equiv 3 \pmod 4$. Так как -1 является квадратичным невычетом по модулю *p*, то многочлен $f = X^2 + 1$ - неприводим над $\mathbb{F}_p$. По предыдущей теореме многочлен $g = f(X^p - X - b)$ будет неприводим над $\mathbb{F}_p$, если $\mathrm{Tr}(2b) \neq 0$. Мы всегда можем выбрать *b* = -1, и тогда

$$g = (X^p - X + 1)^2 + 1 = X^{2p} - 2X^{p+1} + 2X^p + X^2 - 2X + 2$$

Неприводимый многочлен степени 2*p* над $\mathbb{F}_p$.

10.2. Расширения степени, делящей *q* – 1.

В этом параграфе мы покажем, как можно построить расширения $F = \mathbb{F}_q$ степени $n \mid q - 1$. 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: Пусть $f_1(X),..., f_N(X)$ - 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 $(q^m - 1)/e$. Также предположим, что $q^m \equiv 1 \pmod 4$, если $t \equiv 0 \pmod 4$. Тогда $f_1(X^t),..., f_N(X^t)$ - различные унитарные неприводимые многочлены степени mt и порядка et над $\mathbb{F}_q$.

Пример: Рассмотрим случай, когда $q = 2$, $m = 4$ и $e = 15$. Круговой многочлен Φ_{15} расщепляется над $\mathbb{F}_2$ на два неприводимых множителя $f_1 = 1 + X + X^4$ и $f_2 = 1 + X^3 + X^4$. Теорема показывает, что $1 + X^t + X^{4t}$ и $1 + X^{3t} + X^{4t}$ являются унитарными неприводимыми многочленами степени $4t$ и порядка $15t$ над $\mathbb{F}_2$ для любого t вида $t = 3^a 5^b$, в частности, для $t = 3, 5, 9, 15, 25$.

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

1. Если p – простой делитель t, то $p|e$, но $p \nmid (q^m - 1)/e$.
2. $q \equiv 1 \pmod 4$, если $t \equiv 0 \pmod 4$.

Отметим два специальных случая этой теоремы.

Следствие: 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: Пусть r – простое число, $c \in \mathbb{F}_q^*$ - элемент, не являющийся r-ой 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.