
Лекция №2 (10.09.20)

---

1. Предварительные сведения из теории конечных полей.

1.3. Круговые многочлены.

В этом параграфе мы отметим основные факты о корнях из единицы и круговых многочленах.

Корни многочлена $X^n - 1 \in K[X]$ (в его поле разложения) называются корнями *n-ой степени из единицы над* K. Так как $(X^n - 1)' = nX^{n-1}$, то корни $X^n - 1$ являются простыми тогда и только тогда, когда $\mathrm{char}K \nmid n$.

Лемма 1. *Пусть* K *— поле конечной характеристики* p *и пусть* n *— положительное целое, такое, что* $p|n$*, то есть* $n = p^a m$*, где* $p^a||n$ *(то есть* p^a *– наивысшая степень* p*, делящая* n*). Тогда корни* $X^n - 1$ *есть* m *различные корни* m*-й степени из единицы, каждый кратности* p^a*.*

Теорема 1. *Пусть* K *– поле,* n *– положительное целое, такое, что* $charK \nmid n$*. Тогда* n*-различные корни* n*-й степени из единицы образуют циклическую подгруппу* U_n *в* $E^\times$*, где* E *– поле разложения* $X^n - 1$ *над* K*.*

$\varphi(n)$ порождающих элементов группы U_n являются *примитивными корнями степени* n *из единицы над* K. Многочлен

$$\Phi_n = \prod_{\zeta, \langle\zeta\rangle = U_n} (X - \zeta)$$

называется *n-м круговым многочленом над* K. Очевидно, имеет место равенство:

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Кроме того, благодаря функции Мёбиуса, имеем

$$\Phi_n = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}.$$

Теорема 2. *Пусть* K *— поле,* $charK \nmid n$*. Тогда коэффициенты* Φ_n *лежат в простом подполе поля* K*.*

Теорема 3. *Пусть q – степень простого числа, n – положительное целое, НОД$(q,n)=1$. Обозначим $d := \mathrm{ord}_n q$ – порядок q по $\bmod n$, то есть d – наименьшее положительное целое, такое, что $q^d \equiv (\bmod n)$. Тогда $\mathbb{F}_{q^d}$ – поле разложения многочлена Φ_n, и Φ_n представляет собой произведение $\varphi(n)/d$ различных унитарных неприводимых многочленов степени d над $\mathbb{F}_q$.*

Следствие 1. *Φ_n неприводим над $\mathbb{F}_q$ тогда и только тогда, когда $\mathrm{ord}_n q = \varphi(n)$.*

Пусть f – неприводимый многочлен степени n над $F = \mathbb{F}_q$ и α – корень многочлена f в расширении $E = \mathbb{F}_{q^n}$. Тогда ordα в $E^\times$ также называется *порядком многочлена* f и обозначается ord$f$. В частности, примитивные многочлены степени n являются многочленами порядка $q^n - 1$. Пусть $\mathrm{ord}f = \mathrm{ord}\alpha = m$. Тогда α – примитивный корень степени m из единицы над $\mathbb{F}_q$, следовательно, его минимальный многочлен $f = m_\alpha$ является множителем Φ_m, тогда $\mathrm{ord}_m q = n$ и Φ_m – произведение неприводимых многочленов степени n порядка m над $\mathbb{F}_q$.

Теорема 4. *Пусть q – степень простого числа и n – положительное целое. Тогда*

$$I_{n,q}(X) = \prod \Phi_m(X),$$

где $m | q^n - 1$ и $\mathrm{ord}_m q = n$.

Пусть $f(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ – многочлен над $\mathbb{F}_q$. *Двойственным к f* называется многочлен $f^*(X)$ следующего вида:

$$f^*(X) = X^n f(X^{-1}) = a_0 X^n + a_1 X^{n-1} + \ldots + a_{n-1}X + a_n.$$

Если $f(X) = f^*(X)$, то f называется *самодвойственным* (или *палиндромом*).

Теорема 5. *Пусть $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ – неприводимый, унитарный многочлен порядка e над $\mathbb{F}_q$. Тогда $\tilde{f} = f^*/a_0$ – унитарный, неприводимый многочлен степени n порядка e. Кроме того, если f – минимальный многочлен элемента α, то $\tilde{f}$ – минимальный многочлен элемента α^{-1}. Исключая многочлены $X+1$ и $X-1$, каждый неприводимый многочлен, удовлетворяющий условию $f = \tilde{f}$, является самодвойственным и имеет четную степень $n = 2m$. В этом случае $\alpha^{q^m} = \alpha^{-1}$.*

Следствие 2. *Пусть q – степень простого числа, n – положительное целое, такое, что НОД$(q,n)=1$. Тогда Φ_n – произведение $\varphi(n)/\mathrm{ord}_n q$ различных унитарных неприводимых многочленов степени $\mathrm{ord}_n q$ над $\mathbb{F}_q$. Пусть f – неприводимый множитель Φ_n степени, по крайней мере, 2, тогда либо f – самодвойственный ($\mathrm{ord}_n q$ – четный), либо $\tilde{f} \nmid f$.*