УДК 519.642.8

**КОРНЕВЫЕ МНОГОЧЛЕНЫ**

Сергеев Александр Эдуардович
к.ф.-м.н, доцент

Сергеев Эдуард Александрович
к.ф.-м.н, доцент
*Кубанский Государственный Университет, Краснодар, Россия*

В статье получен явный вид корневых многочленов для циклических многочленов третьей степени над полями характеристики 2. Приводится также обзор известных результатов по корневым многочленам над произвольными полями

Ключевые слова: НОРМАЛЬНЫЙ МНОГОЧЛЕН, КОРНЕВОЙ МНОГОЧЛЕН, ЦИКЛИЧЕСКИЙ МНОГОЧЛЕН

UDC 519.642.8

**ROOT POLYNOMIALS**

Sergeev Alexander Eduardovich
Cand.Phys.-Math.Sci., associate professor

Sergeev Eduard Alexandrovich
Cand.Phys.-Math.Sci., associate professor
*Kuban State University, Krasodar, Russia*

The article obtained the explicit form of root polynomials for cyclic polynomials of degree three over fields of characteristic 2. We also give an overview of known results on the root polynomials over arbitrary fields

Keywords: NORMAL POLYNOMIAL, ROOT POLYNOMIAL, CYCLIC POLYNOMIAL

## Корневые многочлены

Пусть $K$ – поле и $\overline{K}$ – алгебраическое замыкание поля $K$. Унитарный многочлен (многочлен со старшим коэффициентом, равным 1) $f(x)$ из $K[x]$ называется нормальным над $K$, если все его корни рациональным образом выражаются над $K$ через любой корень многочлена $f(x)$.

Пусть $f(x)$ – нормальный многочлен над $K$, т.е.

$$f(x)=(x-q_1)\cdot\ldots\cdot(x-q_n),$$

где $q_i\in\overline{K}$ и $q_i=g_i(q_1)$ для всех $i=1,2,\ldots,n,$ где $g_i(x)$ – многочлены из $K[x]$ степени, меньшей $n$.

Многочлены $g_i(x)$ однозначно определены многочленом $f(x)$. Если он неприводим в $K[x]$, то их называют корневыми многочленами для $f(x)$.

Заметим, что $g_1(x)=x,$ образуем множество корневых многочленов $S=\{g_1=x,g_2,\ldots,g_n\}$. Пусть степень $f(x),$ равная $n,$ будет больше двух и $K$ – формально вещественное поле. В этом случае H. Kleiman [3] доказал следующие теоремы.

**Теорема 1.** Нормальный многочлен $f = x^n + \sum_{j=0}^{n-1} a_{(n-1)-j} x^{(n-1)-j}$ с коэффициентами в формально вещественном поле $K$ однозначно определяется множеством $T = \{S, a_{n-2}\}$, где $S$ – множество корневых многочленов для $f(x)$. Кроме того, множество $S$ содержит по крайней мере один нелинейный многочлен, при условии что $n > 2$. Если множество $S$ содержит корневой многочлен степени два, то нормальный многочлен $f(x)$ однозначно определяется множеством $S$.

Пусть $\Phi_n(x)$ – круговой многочлен порядка $n$, $n > 6$, следовательно, степень многочлена $\Phi_n(x)$ больше или равна 4.

**Теорема 2.** Каждый многочлен в классе круговых многочлен степени $\geq 4$ однозначно определяется своими корневыми многочленами.

**Теорема 3.** Пусть $K$ – поле характеристики 0. Пусть $f(x) \in K[x]$ – неприводимый над $K$ многочлен и все корни многочлена $f(x)$ являются линейными функциями от одного корня $a$. Тогда поле разложения многочлена $f(x)$ есть циклическое расширение поля $K$ и поле $K$ содержит первообразный корень $n$-ой степени из единицы.

H. Muthsam доказал следующее утверждение [4].

**Теорема 4.** Пусть $K$ – формально вещественное поле, $f(x)$ – неприводимый нормальный многочлен степени $n > 1$ из $K[x]$, корни которого линейно независимы над $K$. Тогда множество $S$ корневых многочленов для $f(x)$ однозначно определяет $f(x)$.

K. Girstmair [1] исследовал нормальные многочлены третьей степени (т.е. циклические многочлены) над полями $K$ характеристики неравной 2 и 3.

Пусть $f(z) = z^3 + a_1 z^2 + a_2 z + a_3$ – циклический многочлен из $K[x]$ с дискриминантом $D(f)$ и корневыми многочленами:

$$w_1 = z, \quad w_2 = w_{22} z^2 + w_{21} z + w_{20}, \quad w_3 = w_{32} z^2 + w_{31} z + w_{30},$$

где $w_2, w_3 \in K[x], \quad w_{22} \neq 0, \; w_{32} \neq 0$. Тогда справедлива теорема [3]:

**Теорема 5.** Циклический кубический многочлен $f(z) \in K[z]$ однозначно определяется своими корневыми многочленами.

Если для простоты обозначим нетривиальный корневой многочлен $w_2$ в виде

$$w_2 = w_2 z^2 + w_1 z + w_0,$$

то коэффициенты циклического многочлена $f(z) = z^3 + a_1 z^2 + a_2 z + a_3$ можно найти из соотношений:

$$a_1 = -(w_{20} + w_{30}),$$

$$a_2 = \frac{a_1^2 w_2 + a_1(1 - w_1) + 3w_0}{2w_2},$$

$$a_3 = a_1 a_2 - \frac{a_1^3}{3} + \frac{a_1^2 w_1 - a_2(1 + 2w_1) - a_1 w_0}{3w_2}.$$

С этими условиями справедлива теорема [3].

**Теорема 6.** Пусть $K$ – поле характеристики, неравной 2 и 3, и не содержащее корней третьей степени из единицы. Тогда квадратный многочлен $w = w_2 z^2 + w_1 z + w_0$, где $w_2 \neq 0, \quad w_2, w_1, v_0 \in K$, является корневым многочленом некоторого циклического кубического многочлена $f(x)$ только если элемент

$$r(w) = (w_1 - 1)^2 - 4w_0 w_2 - 8$$

есть квадрат в поле $K$: $r(w) = q^2, \; q \in K$. В этом случае существуют два многочлена $f_i(z) = z^3 + a_{i1} z^2 + a_{i2} z + a_{i3}, \quad i = 1, 2$ с корневым многочленом $w$:

$$a_{11} = \frac{3w_1 + 1 + q}{2w_2}, \quad a_{21} = \frac{3w_1 + 1 - q}{2w_2}$$

и коэффициенты $a_{i2}, \; a_{i3}, \; i = 1, 2$ определяются с помощью $a_{11}, \; a_{21}$ и $w$ из соотношений (теорема 5).

# Построение корневых многочленов для некоторого кубического циклического многочлена над полем $K$ характеристики 2

Пусть $K$ – поле и $f(x)=x^3+ax+b$ – неприводимый многочлен над $K$ с циклической группой Галуа $C_3$, то есть любые два корня этого многочлена рациональным образом выражаются над полем $K$ через третий оставшийся корень. Пусть $a, b, g$ – корни $f(x)$, тогда:

$$b=r_2(a)=A+Ba+Ca^2, \quad g=r_3(a)=A_1+B_1a+C_1a^2, \tag{1}$$

где $A, B, C, A_1, B_1, C_1$ из поля $K$.

Нетрудно доказать, что в случае неприводимости многочлена $f(x)$ коэффициенты $C$ и $C_1$ неравны нулю, при этом многочлены $r_2(x)$ и $r_3(x)$ имеют вид:

$$r_2(x)=A+Bx+Cx^2, \quad r_3(x)=A_1+B_1x+C_1x^2, \tag{2}$$

и их называют корневыми многочленами для циклического многочлена $f(x)$.

Пусть $D(f)$ – дискриминант многочлена $f(x)=x^3+ax+b$, то есть:

$$D(f)=-4a^3-27b^2.$$

В случае циклического многочлена $f(x)$ дискриминант $D(f)=d^2$, $d\in K$, и для поля $K$ характеристики неравной 2 и 3, Girstmair [1] доказал, что в равенствах (1) и (2) имеем:

$$r_2(x)=-\frac{2a^2}{d}+\left(\frac{9b}{2d}-\frac{1}{2}\right)x-\frac{3a}{d}x^2, \qquad r_3(x)=\frac{2a^2}{d}+\left(\frac{9b}{2d}-\frac{1}{2}\right)x+\frac{3a}{d}x^2. \tag{3}$$

Формулы (3) дают явный вид корневых многочленов для $f(x)$, но эти формулы не имеют смысла, если поле $K$ имеет характеристику 2 или 3.

Рассмотрим далее случай, когда поле $K$ имеет характеристику 2 и в $K[x]$ существуют циклические многочлены третьей степени.

Всякий многочлен 3-ей степени над полем $K$ с помощью соответствующей линейной подстановки может быть приведен к виду:

$$f(x) = x^3 + ax + b. \quad (4)$$

В работе [2] было доказано, что неприводимый над $K$ многочлен вида (4) имеет циклическую группу Галуа над полем $K$ характеристики 2, только если уравнение (5):

$$y^2 + by + a^3 + b^2 = 0 \quad (5)$$

имеет корни в поле $K$.

Найдем в этом случае явный вид корневых многочленов. Пусть $a$ – произвольный корень многочлена $f(x) = x^3 + ax + b \in K[x]$, характеристика поля $K$ равна 2 и группа Галуа многочлена $f(x)$ – циклическая третьего порядка. Тогда многочлен $f(x)$ примет вид:

$$f(x) = x^3 + ax + b = (x - a)(x^2 + ax + a + a^2). \quad (6)$$

Пусть остальные два корня $a_2$ и $a_3$ многочлена $f(x)$ представляются в виде:

$$a_2 = A + Ba + Ca^2, \quad a_3 = M + Na + Sa^2, \quad (7)$$

где коэффициенты $A, B, C, M, N, S \in K$, а $a_2$ и $a_3$ являются корнями многочлена $g(x) = x^2 + ax + a + a^2$. Поэтому, справедливы следующие соотношения:

$$a_2 + a_3 = a, \quad a_2 \cdot a_3 = a + a^2. \quad (8)$$

Из (8) ввиду неприводимости многочлена $f(x)$ над полем $K$ имеем: $B + N = 1, \quad A + M = 0, \quad C + S = 0,$ откуда $A = M, \quad N = B + 1, \quad C = S.$ Таким образом:

$$a_2 = A + Ba + Ca^2, \quad a_3 = A + (B + 1)a + Ca^2.$$

Так как $g(a_2) = (A + Ba + Ca^2)^2 + a \cdot (A + Ba + Ca^2) + a + a^2 = 0$, то, имеем:

$$A^2 + B^2a^2 + C^2a^4 + Aa + Ba^2 + Ca^3 + a + a^2 = 0.$$

Учитывая соотношения

$$a^3 = aa + b, \quad a^4 = aa^2 + ba,$$

получаем следующее равенство:

$$A^2 + B^2a^2 + C^2(aa^2 + ba) + Aa + Ba^2 + C(aa + b) + a + a^2 = 0.$$

Отсюда имеем систему уравнение:

$$\begin{cases} A^2 + Cb + a = 0, \\ C^2 b + A + Ca = 0, \\ B^2 + C^2 a + B + 1 = 0. \end{cases} \quad (9)$$

Из третьего уравнения системы получаем

$$a = \frac{B^2 + B + 1}{C^2},$$

и так как $C \neq 0,$ то из второго уравнения системы (9) имеем:

$$b = \frac{A + Ca}{C^2} = \frac{A + \frac{B^2 + B + 1}{C}}{C^2} = \frac{CA + B^2 + B + 1}{C^3}.$$

Тогда, из первого уравнения системы (9) следует равенство

$$A^2 + C \cdot \frac{CA + B^2 + B + 1}{C^3} + \frac{B^2 + B + 1}{C^2} = 0.$$

Упрощая последнее равенство, получаем:

$$AC(AC + 1) = 0. \quad (10)$$

Из последнего равенства, учитывая, что $C \neq 0$ имеем только две возможности для $A$: или $A = 0,$ или $A = \frac{1}{C}.$ В первом случае $a = \frac{B^2 + B + 1}{C^2},$ $b = \frac{B^2 + B + 1}{C^3}$ и тогда, многочлен $f(x)$ имеет вид:

$$f(x) = x^3 + \frac{B^2 + B + 1}{C^2} x + \frac{B^2 + B + 1}{C^3}. \quad (11)$$

В этом случае корневыми многочленами являются:

$$r_2(x) = Bx + Cx^2, \quad r_3(x) = (B + 1)x + Cx^2. \quad (12)$$

Если многочлен $f(x)$ вида (11) при данных $B, C \in K$ неприводим над $K,$ то это – циклический многочлен.

Во втором случае, когда $A = \frac{1}{C}$ имеем $a = \frac{B^2 + B + 1}{C},$ $b = \frac{B^2 + B}{C^3}$ и многочлен $f(x)$ принимает вид:

$$f(x) = x^3 + \frac{B^2 + B + 1}{C^2}x + \frac{B^2 + B}{C^3} = x^3 + (B^2 + B + 1)A^2x + (B^2 + B)A^3. \qquad (13)$$

В этом случае корневыми многочленами являются:

$$r_2(x) = A + Bx + \frac{1}{A}x^2, \quad r_3(x) = A + (B+1)x + \frac{1}{A}x^2. \qquad (14)$$

Если многочлен $f(x)$ вида (13) при данных $B, A \in K$ неприводим над $K$, то это – циклический многочлен.

Таким образом, мы получили следующую теорему:

**Теорема 1.** Над полем $K$ характеристики 2, допускающим циклические расширения степени 3 циклические многочлены третьей степени имеют вид (11) или (13), при этом для многочленов вида (11) корневые многочлены описываются равенствами (12), а для многочленов вида (13) корневые многочлены определяются равенствами (14).

Рассмотрим некоторые примеры.

**Пример 1.** Пусть $K = Z_2(t),\ B = 1,\ C = \frac{1}{t},$ тогда

$$f(x) = x^3 + t^2x + t^3.$$

Этот многочлен неприводим над $Z_2(t),$ так как элементы $1, t, t^2, t^3$ не являются его корнями. Поэтому этот многочлен является циклическим и его корневые многочлены имеют вид:

$$r_2(x) = x + \frac{1}{t}x^2, \quad r_3(x) = \frac{1}{t}x^2.$$

Нетривиальные автоморфизмы поля разложения многочлена $f(x)$ над $K$ определяются отображениями:

$$s(m + na + ka^2) = m + n\cdot\left(a + \frac{1}{t}a^2\right) + k\cdot\left(a + \frac{1}{t}a^2\right)^2 =$$

$$= m + na + \frac{n}{t}a^2 + ka^2 + \frac{1}{t^2}ka^4 = m + na + \frac{n}{t}a^2 + ka^2 + \frac{k}{t^2}\left(t^2a^2 + t^3a\right) =$$

$$= m + na + \frac{n}{t}a^2 + ka^2 + ka^2 + kta = m + (n + kt)a + \frac{n}{t}a^2, \quad m, n, k \in K;$$

$$= m + \frac{n}{t}a^2 + ka^2 + kta = m + (kt)a + \left(\frac{n}{t} + k\right)a^2, \quad m, n, k \in K.$$

**Пример 2.** Пусть поле $K = Z_2(t)$, $A = 1$, $B = t$. Тогда из (13) имеем:

$$f(x) = x^3 + (t^2 + t + 1)x + (t^2 + t).$$

Этот многочлен неприводим в $Z_2(t)$, так как элементы $1,\ t,\ t+1$ не являются корнями этого многочлена, следовательно, это – циклический многочлен с корневыми многочленами:

$$r_2(x) = 1 + tx + x^2, \quad r_3(x) = 1 + (t+1)x + x^2.$$

Если $a$ – один корень многочлена $f(x)$, то два других корня этого многочлена есть:

$$b = r_2(a) = 1 + ta + a^2, \quad g = r_3(a) = 1 + (t+1)a + a^2$$

и нетривиальные автоморфизмы поля разложения многочлена $f(x)$ над $K$ определяются отображениями:

$$s(m + na + ka^2) = m + n(r_2(a)) + k(r_2(a))^2,$$

$$s^2(m + na + ka^2) = m + n(r_3(a)) + k(r_3(a))^2,$$

где $m, n, k \in K$.

Пусть $K$ – поле характеристики 2, над которым существуют циклические расширения степени 3, т.е. существуют циклические, неприводимые над $K$ кубические многочлены с коэффициентами из поля $K$. Покажем, что при определенных условиях на поле $K$ циклические многочлены третьей степени не имеют трех линейных корневых многочленов.

Пусть $f(x) = x^3 + px + q$ – неприводимый над полем $K$ циклический многочлен и $a$, $aa + b$, $ca + d$ – его корни, т.е. $x$, $ax + b$, $cx + d$, где $a, b, c, d \in K$ его корневые многочлены.

Так как $a+(aa+b)+(ca+d)=0,$ то $a+c+1=0,\quad b+d=0,$ откуда получаем $c=a+1,\quad b=d,$ и значит, $a,\ aa+b,\ (a+1)a+b$ – корни многочлена $f(x).$ Тогда:

$$a\cdot(a+a)+a((a+1)a+b)+(aa+b)((a+1)a+b)=p. \qquad (15)$$

Упрощая равенство (15), получаем:

$$(a^2+a+1)a^2+ba+b^2=p,$$

откуда $b=0,\ \ p=0,\ \ a^2+a+1=0.$

Итак, в рассматриваемом случае (когда все три корневых многочлена у $f(x)$ циклические), имеем: $f(x)=x^3+q$ и уравнение $x^2+x+1=0$ имеет корень в поле $K.$

Поле $K=Z_2(t)$ допускает циклические расширения третьей степени и уравнение $x^2+x+1=0$, очевидно, не имеет корней в поле $Z_2(t).$ Таким образом, циклические многочлены третьей степени с коэффициентами из $Z_2(t)$ имеют один линейный корневой многочлен $x$ и два многочлена 2-ой степени, так как, очевидно, двух линейных корневых многочленов и одного 2-ой степени не может быть у циклического многочлена 3-ей степени над полем любой характеристики.

## ЛИТЕРАТУРА

1. Girstmair K. On root polynomials of cyclic cubic equation // Arch. Math. Vol. 36, 1981. p. 313 – 326.
2. Сергеев А.Э. О задаче И. Капланского // Известия вузов; Северо-кавказский регион. Естественные науки. 2001. № 1. с. 14 – 17.
3. Kleiman H. Methods for uniquely determining Galois polynomials and related theorems // Monatshefte fur Mathematik, 73, 1969, p. 63 – 68.
4. Muthsam H. Eine bemerkung uber die wurzelpolynome Galoiisscher gleichungen // Monatshefte fur Mathematik, 83, 1977, p. 155 – 157.