УДК 511.238.4

ГЕНЕРИРУЮЩИЙ ПОЛИНОМ ДЛЯ A_4 НАД ПОЛЕМ ХАРАКТЕРИСТИКИ 3[1]

***Сергеев Э. А.*[2], *Авадов К. С.*[3]**

GENERATING POLYNOMIAL FOR A_4 GROUP OVER CHARACTERISTIC 3 FIELDS

Sergeev E. A., Avadov K. S.

In this work we construct a generic polynomial for A_4 alternative group over characteristic 3 fields.

Известно, что генерирующий полином для группы A_4 существует над любым полем. В работе [1] A. Ledet построил генерирующий полином с двумя параметрами для группы A_4 над полем, характеристика которого не равна 2,3. Аналогичный результат для поля характеристики 2 получен в [2], а для случая поля характеристики 3 соответствующий генерирующий полином найден в данной работе. Таким образом, A_4 — генерирующие полиномы построены для всех случаев.

Определение. Пусть K — поле, а G — конечная группа. Сепарабельный полином $g(t_1,\dots,t_m,X) \in K(t_1,\dots,t_m)[X]$ с коэффициентами из поля рациональных функций $K(t_1,\dots,t_m)$ и единичным старшим коэффициентом называется генерирующим для G над K, если выполнены следующие два условия:

1. Группа Галуа g (как многочлена от X) изоморфна G;

2. Если L — бесконечное поле, содержащее K, а N/L — расширение Галуа с группой Галуа G, то существуют $\lambda_1,\dots,\lambda_m \in L$ такие, что N — поле расщепления $g(\lambda_1,\dots,\lambda_m,X)$ над L.

Теорема 1 [3]. Пусть G — конечная группа и V — точное m-мерное линейное представление G над полем K. Предположим, что $K(V)^G = K(\varphi_1,\dots,\varphi_m)$ — чисто трансцендентно над K (т. е. φ_i — трансцендентные над K и образуют минимальный базис) и выберем конечное G-стабильное подмножество $M \subset K(V)$ такое, что $K(V) = K(V)^G(M)$. Положим

$$f(X) = \prod_{y\in M}(X-y) \in K(V)^G[X],$$

тогда $f(X) = g(\varphi_1,\dots,\varphi_m,X)$ для $g \in K(\varphi_1,\dots,\varphi_m)[X]$ и g — генерирующий для G над K.

Лемма. Пусть k — поле, $char\ k = 3, \sigma$ — автоморфизм расширения $k(s,t)/k$, действующий следующим образом:

$$\sigma : s \mapsto t, \quad t \mapsto 1/st,$$

тогда порядок σ равен 3 и поле неподвижных элементов $k(s,t)^{C_3}$ чисто трансцендентно над k, а именно

$$k(s,t)^{C_3} = k\left(\frac{st^2+t+st}{s^2t^2+t^2+1+2st^2+2t+2st}, \frac{s^2t^3+t^2+st}{s^3t^3+t^3+1}\right).$$

Доказательство. Пусть $C_3 = \langle\sigma\rangle$, σ действует на $k(x,y,z)$

$$\sigma : x \mapsto y, \quad y \mapsto z, \quad z \mapsto x.$$

Известно, что

$$k(x,y,z)^{S_3} = k(s_1,s_2,s_3),$$

где

$$s_1 = x+y+z, \quad s_2 = xy+yz+xz, \quad s_3 = xyz.$$

[1]Работа выполнена при поддержке РФФИ_р_юг (06-01-96645).

[2]Сергеев Эдуард Александрович, канд. физ.-мат. наук, доцент кафедры высшей алгебры и геометрии Кубанского государственного университета.

[3]Авадов Константин Сергеевич, аспирант кафедры вычислительной математики и информатики Кубанского государственного университета.

Пусть

$$l_1 = x^2y + y^2z + z^2x, \quad l_2 = xy^2 + yz^2 + zx^2.$$

Легко убедиться, что

$$(\alpha - l_1)(\alpha - l_2) \equiv \alpha^2 + 2s_1s_2\alpha + (s_2^3 + s_1^3s_3) (\mod 3).$$

Все вычисления проводятся над полем характеристики 3.

Отсюда следует

$$[k(s_1, s_2, s_3, l_1) : k(s_1, s_2, s_3)] = 2.$$

Ясно,

$$l_1 \in k(x, y, z)^{C_3} \Rightarrow k(s_1, s_2, s_3, l_1) \subseteq k(x, y, z)^{C_3}.$$

А поскольку

$$\left[k(s_1, s_2, s_3, l_1) : k(x, y, z)^{S_3}\right] = 2,$$

$$\left[k(x, y, z)^{C_3} : k(x, y, z)^{S_3}\right] = 2,$$

то

$$k(x, y, z)^{C_3} = k(s_1, s_2, s_3, l_1).$$

Из уравнения для l_1 по теореме Виета следует

$$\begin{cases} -l_1 - l_2 = 2s_1s_2, \\ l_1l_2 = s_2^3 + s_1^3s_3; \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} l_2 = s_1s_2 - l_1, \\ s_1s_2l_1 - l_1^2 = s_2^3 + s_1^3s_3; \end{cases} \Rightarrow$$

$$\Rightarrow s_3 = \frac{s_1s_2l_1 - l_1^2 - s_2^3}{s_1^3},$$

то есть

$$s_3 \in k(s_1, s_2, l_1) \Rightarrow$$
$$\Rightarrow k(s_1, s_2, s_3, l_1) = k(s_1, s_2, l_1) \Rightarrow$$
$$\Rightarrow k(x, y, z)^{C_3} = k(s_1, s_2, l_1).$$

Далее,

$$k(x, y, z)^{C_3} = k(s_1, s_2, l_1) = k\left(s_1, \frac{s_2}{s_1^2}, \frac{l_1}{s_1^3}\right),$$

$$\frac{s_2}{s_1^2} \in k(x, y, z)_0^{C_3},$$

$$\frac{l_1}{s_1^3} \in k(x, y, z)_0^{C_3} \Rightarrow k(x, y, z)_0^{C_3} = k\left(\frac{s_2}{s_1^2}, \frac{l_1}{s_1^3}\right),$$

поскольку $k(x, y, z)^{C_3}$ является для каждого из этих полей чисто трансцендентным расширением степени трансцендентности 1.

Известно, что $k(x, y, z)_0 = k(s, t)$, где $s = x/y$ и $t = y/z$, причем σ действует на $k(s, t)$ следующим образом:

$$\sigma : s \mapsto t, \quad t \mapsto 1/st.$$

Кроме того,

$$\frac{s_2}{s_1^2} = \frac{st^2 + t + st}{s^2t^2 + t^2 + 1 + 2st^2 + 2t + 2st},$$

$$\frac{l_1}{s_1^3} = \frac{s^2t^3 + t^2 + st}{s^3t^3 + t^3 + 1}.$$

Итак, из сказанного следует: если σ — автоморфизм $k(x, y, z)_0 = k(s, t)$, $\sigma(s) = t$, $\sigma(t) = 1/st$, то порядок σ равен 3 и

$$k(s, t)^{C_3} = k\left(\frac{st^2 + t + st}{s^2t^2 + t^2 + 1 + 2st^2 + 2t + 2st}, \frac{s^2t^3 + t^2 + st}{s^3t^3 + t^3 + 1}\right)$$

— чисто трансцендентное расширение k. □

Найдем генерирующий полином для A_4 над полем k характеристики 3.

Мы можем прийти к линейному действию A_4 на $k(x, y, z)$, рассматривая S_4 как группу вращения куба. Запись

$$A_4 = \langle \sigma, \rho_1, \rho_2 | \sigma^3 = \rho_1^2 = 1, \sigma\rho_1\sigma^{-1} = \rho_2, \sigma\rho_2\sigma^{-1} = \rho_1\rho_2 = \rho_2\rho_1 \rangle$$

дает следующее действие A_4 на $k(x, y, z)$:

$$\sigma : \quad x \mapsto y, \quad y \mapsto z, \quad z \mapsto x,$$
$$\rho_1 : \quad x \mapsto -x, \quad y \mapsto -y, \quad z \mapsto z.$$

Переходя к подполю однородных элементов нулевой степени $k(x, y, z)_0 = k(s, t)$, $s = x/y$, $t = y/z$, получим

$$\sigma : \quad s \mapsto t, \quad t \mapsto 1/st,$$
$$\rho_1 : \quad s \mapsto s, \quad t \mapsto -t.$$

Кроме того, $k(x, y, z)^{A_4}/k(s, t)^{A_4}$ рационально (т. е. чисто трансцендентно) степени трансцендентности 1 и порождается $xyz/(x^2 + y^2 + z^2)$. Ясно, что $k(s, t)^{V_4} = k(s^2, t^2)$, таким образом, приходим к расширению $k(s^2, t^2)/k(s^2, t^2)^{C_3}$ для $C_3 = \langle \sigma \rangle$.

В предположении, что $u = s^2$ и $v = t^2$, возникает вопрос: если $C_3 = \langle \sigma \rangle$ действует на $k(u, v)$, $\sigma : u \mapsto v, v \mapsto 1/uv$, будет ли

$k(u,v)^{C_3}/k$ рационально? Из доказанной леммы следует, что будет и

$$k(u,v)^{C_3} = \\ = k\left(\frac{uv^2+v+uv}{u^2v^2+v^2+1+2uv^2+2v+2uv}, \frac{u^2v^3+v^2+uv}{u^3v^3+v^3+1}\right).$$

Итак, $k(s,t)/k(s,t)^{A_4}$ является A_4-расширением, $k(s,t)^{A_4}/k$ — чисто трансцендентное расширение и по теореме 1 существует генерирующий A_4-полином с двумя параметрами над k.

Можно найти генерирующий полином для A_4 над k, выражая минимальный полином для $s+t+1/st$ над $k(s,t)^{A_4}$ через найденные выше порождающие элементы, обозначая которые через a и b соответственно, приходим к теореме.

Теорема 2. Если k — поле, $char\ k=3$, то полином

$$F(a,b,X) = X^4 + \left(\frac{2a+b}{a^3+2ab+b^2}\right)X^2 + X + \\ + \frac{a^3b+b^3+2ab^2+b^2+ab+a^2}{a^6+2a^3b^2+a^4b+b^4+ab^3+a^2b^2}$$

$F(a,b,X) \in k(a,b)[X]$ является генерирующим для A_4 над k.

Замечание. Коэффициенты минимального полинома для $s+t+1/st$ можно выразить через a и b при помощи следующих рассуждений: пусть u и v из $k(x,y)$ алгебраически независимы над полем k и известно, что $f \in k(u,v)$. Как можно найти функцию $g \in k(X,Y)$ такую, что $f = g(u,v)$?

Запишем $u = \frac{u_1}{u_2}$, $v = \frac{v_1}{v_2}$, $f = \frac{f_1}{f_2}$ в виде частных полиномов из $k[x,y]$ и рассмотрим $g = \frac{g_1}{g_2}$ как частное двух полиномов g_1 и g_2 с неопределенными коэффициентами, предположив, что степени g_1 и g_2 по каждой из переменных X, Y не превосходят некоторого числа d. Нужно получить:

$$f = \frac{f_1}{f_2} = \frac{g_1(u,v)}{g_2(u,v)} = \frac{u_2^d v_2^d g_1(u,v)}{u_2^d v_2^d g_2(u,v)},$$

то есть $G = f_1 u_2^d v_2^d g_2(u,v) - f_2 u_2^d v_2^d g_1(u,v) = 0$.

Коэффициенты G — линейные комбинации коэффициентов g_1 и g_2, а значит, g_1 и g_2 могут быть найдены методами линейной алгебры. При этом, если получается лишь нулевое решение, следует увеличить d и повторить поиск. Так как g существует, он когда-нибудь будет найден. В данном случае, так как $\left[k(s,t) : k(s,t)^{A_4}\right] = 12$, то существует минимальный полином для $s+t+1/st$ над $k(s,t)^{A_4}$ степени, не превосходящей 12. Следовательно, искомый генерирующий полином существует для $d \leqslant 12$.

Коэффициенты $F(a,b,X)$ были найдены с помощью Maple 7.

Пример. Пусть $k = F_3(t)$, t — трансцендентный элемент над F_3, $a = b = t$, тогда

$$F(X) = X^4 + X + \frac{1}{t^2} \in k[X].$$

Кубическая резольвента F равна

$$g(X) = X^3 + \frac{2}{t^2}X + 2.$$

Если α — корень g, то два других корня g равны $\alpha + \frac{1}{t}$ и $\alpha - \frac{1}{t}$, т. е.

$$g(X) = (X-\alpha)\left(X - (\alpha + \frac{1}{t})\right)\left(X - \left(\alpha - \frac{1}{t}\right)\right).$$

Таким образом, $k(\alpha)$ — поле расщепления g и $[k(\alpha) : k] = 3$, а значит, $Gal_k F(X) = A_4$ (см. [4]).

Литература

1. *Ledet A.* Constructing generic polynomials // Proceedings of the Workshop on Number Theory 2001 (eds. K. Komatsu & K. Hashimoto). Tokyo, Waseda University, 2001. P. 114–118.
2. *Сергеев А.Э., Яковлев А.В.* Генерирующие многочлены над полями характеристики два для транзитивных подгрупп группы S_4 // Записки науч. сем. ПОМИ. 2006. Т. 330. С. 247–258.
3. *Kemper G., Mattig E.* Generic polynomials with few parameters // J. Symbolic Computation. 2000. Vol. 30. P. 843–857.
4. *Jensen C. U., Ledet A., Yui. N.* Generic Polynomials: Constructive Aspects of the Inverse Galois Problem. MSRI Publication Series 45. Cambridge University Press, 2002. 268 p.

Статья поступила 25 января 2007 г.
Кубанский государственный университет, г. Краснодар