Записки научных
семинаров ПОМИ
Том 330, 2006 г.

А. Э. Сергеев, А. В. Яковлев

ГЕНЕРИРУЮЩИЕ МНОГОЧЛЕНЫ НАД ПОЛЯМИ ХАРАКТЕРИСТИКИ ДВА ДЛЯ ТРАНЗИТИВНЫХ ПОДГРУПП ГРУППЫ S_4

1. Введение

Пусть k – поле и G – конечная группа. Напомним (см. [2]), что сепарабельный многочлен

$$g(x;t_1,\dots,t_m) = x^n + a_{n-1}(t_1,\dots,t_m)x^{n-1} + \dots \\ + a_1(t_1,\dots,t_m)x + a_0(t_1,\dots,t_m)$$

с коэффициентами из поля $k(t_1,\dots,t_m)$ рациональных над k функций от независимых переменных $t_1,\dots,t_m$ называется *генерирующим* для группы G над k, если выполняются условия:

(1) Группа Галуа многочлена g (как многочлена от x над $k(t_1,\dots,t_m)$) есть G.
(2) Если K – бесконечное поле, содержащее k, и M/K – расширение Галуа с группой G, тогда существуют $\lambda_1,\dots,\lambda_m \in K$, такие, что M является полем разложения многочлена $g(x;\lambda_1,\dots,\lambda_m)$ над K.

Проблема построения генерирующих многочленов нетривиальна уже для небольших групп; так, для циклической группы порядка 8 над полем рациональных чисел генерирующий многочлен вообще не существует. Генерирующие многочлены над полем рациональных чисел $\mathbb{Q}$ построены для многих групп, в частности, для всех транзитивных подгрупп групп S_4 и S_5 (см. [3], [4]). Однако, использованные методы неприменимы в случае полей характеристики 2.

Целью настоящей работы является построение генерирующих многочленов над полями характеристики два для транзитивных подгрупп группы S_4, а именно, для симметрической группы S_4, знакопеременной группы A_4, диэдральной группы D_4, нециклической группы V_4 порядка 4 (группы Клейна) и циклической группы $\mathbb{Z}_4$. Мы доказываем следующую теорему.

Теорема. *Пусть k – поле характеристики 2. Следующие многочлены являются генерирующими над k:*

- $x^4 + t_1 x^3 + t_2 x^2 + t_3 x + t_4$ *– для симметрической группы S_4;*
- $x^4 + (1 + t_1)x^2 + t_1 x + t_1 t_2 + t_2^2$ *– для группы Клейна V_4;*
- $x^4 + (1 + t_1)x^2 + t_1 x + t_1^3 + t_2^2 + t_1 t_2$ *– для циклической группы $\mathbb{Z}_4$ порядка 4;*
- $x^4 + (1 + t_1)x^2 + t_1 x + t_2$ *– для диэдральной группы D_4;*
- $x^4 + (t_1^2 + t_1 + 1)x^2 + (t_1^2 + t_1 + 1)x + t_2(t_1^2 + t_1 + 1)^2$ *– для знакопеременной группы A_4.*

Заметим, что первые два утверждения теоремы тривиальны и справедливы для любого основного поля k (не обязательно имеющего характеристику 2). Общеизвестно, что многочлен общего вида $x^n + t_1 x^{n-1} + \ldots + t_{n-1}x + t_n$ является генерирующим для симметрической группы S_n для любого n. Далее, группа Галуа многочлена

$$x^4 + (1 + t_1)x^2 + t_1 x + t_1 t_2 + t_2^2 = (x^2 + x + t_2)(x^2 + x + t_1 + t_2)$$

над полем $k(t_1, t_2)$ является прямым произведением групп Галуа сомножителей, а каждая из этих групп – циклическая группа порядка 2. С другой стороны, если поле K содержит поле k и M/K – расширение Галуа с группой Галуа V_4, то M является композитом двух квадратичных расширений M_1/K и M_2/K, которые для полей любой характеристики, включая 2, являются полями разложения многочленов $x^2 + x + a_1$, $x^2 + x + a_2$ при некоторых $a_1, a_2 \in K$; таким образом, M – поле разложения многочлена $(x^2 + x + a_1)(x^2 + x + a_2) \in K[x]$, а этот многочлен представляет собой специализацию многочлена $(x^2 + x + t_2)(x^2 + x + t_1 + t_2)$ при $t_1 = a_2 - a_1$, $t_2 = a_1$.

Замечание. Генерирующий многочлен для нециклической группы порядка 4, указанный выше, приводим и поэтому, строго говоря, не является генерирующим для группы V_4 как транзитивной подгруппы S_4. Однако, это легко исправляется: искомым генерирующим многочленом будет также минимальный многочлен для примитивного элемента расширения. Если α – корень многочлена $x^2 + x + t_2$, а β – корень многочлена $x^2 + x + t_1 + t_2$, то примитивным элементом расширения $(k(t_1, t_2))(\alpha, \beta)$ будет, например, элемент $\alpha\beta$, а его минимальным многочленом – неприводимый многочлен $x^4 + x^3 + t_1 x^2 + (t_1 t_2 + t_2^2)x + t_1^2 t_2^2 + t_2^4$.

В следующих параграфах будут доказаны остальные утверждения теоремы (предложения 1, 2, 3).

2. Генерирующий многочлен для группы $\mathbb{Z}_4$

В случае, когда $\operatorname{char} K = 0$, известно, что не всякое циклическое расширение L/K степени p^{f-1} погружаемо в циклическое расширение N/K степени p^f над K. Напротив, если K – поле характеристики $p \neq 0$, то, как показал Витт [1], для любого эпиморфизма $G \to F$ конечных p-групп любое расширение Галуа L/K с группой Галуа F погружается в расширение Галуа с группой Галуа G. Более того, Витт указал явную конструкцию, позволяющую строить все расширения N/K поля K характеристики $p \neq 0$ с циклической группой Галуа порядка p^f, содержащие данное расширение L/K степени p^{f-1}.

Теорема (Витт). *Пусть p – простое число, K – поле характеристики $p \neq 0$, L/K – циклическое расширение степени p^{f-1} $(f > 1)$, σ – порождающий элемент циклической группы Галуа расширения L/K. Существуют такие элементы $\delta, \gamma \in L$, что $\operatorname{Sp}_{L/K} \delta = 1$, $\sigma(\gamma) - \gamma = \delta^p - \delta$. Для любого $u \in K$ поле M, полученное присоединением к L корня θ уравнения $x^p - x = u + \gamma$, является расширением Галуа поля K с циклической группой Галуа порядка p^f, и так может быть получено любое циклическое расширение степени p^f, содержащее поле L.*

Отсюда сразу следует описание всех циклических расширений степени 4 для полей характеристики 2.

Лемма 1. *Пусть K – поле характеристики 2. Расширение M/K тогда и только тогда является циклическим расширением степени 4, когда существуют такие элементы $a, b \in K$, что многочлен $x^2 + x + a$ неприводим над K, а M является полем разложения многочлена $f(x; a, b) = x^4 + (1 + a)x^2 + ax + a^3 + b^2 + ab$.*

Доказательство. Пусть $a, b \in K$ и пусть $L \supseteq K$ – поле, полученное присоединением к K корня α многочлена $x^2 + x + a$, а M – поле, полученное присоединением к L корня β многочлена $h(x) = x^2 + x + a\alpha + b$ (быть может, $L = K$ или $M = L$). Покажем, что поле M является полем разложения многочлена

$f(x;a,b) = x^4 + (1+a)x^2 + ax + a^3 + b^2 + ab$. Действительно,

$$f(x;a,b) = x^4 + (1+a)x^2 + ax + a^3 + b^2 + ab =$$
$$= x^4 + (1+a)x^2 + ax + a^2(\alpha^2 + \alpha) + b^2 + ab$$
$$= (x^2 + x + a\alpha + b)(x^2 + x + a\alpha + a + b) = h(x)h_1(x),$$

где через $h_1(x)$ обозначен многочлен $x^2 + x + a\alpha + a + b$. Другим корнем многочлена $h(x)$ является элемент $\beta + 1 \in M$, а корнями многочлена $h_1(x)$ служат элементы $\beta + \alpha, \beta + \alpha + 1 \in M$; таким образом, M содержит все корни многочлена $f(x;a,b)$, а потому и его поле разложения. С другой стороны, поле разложения многочлена $f(x;a,b)$ содержит его корни β, $\alpha+\beta$; следовательно, оно содержит поле $(K(\alpha))(\beta) = M$.

Если многочлен x^2+x+a неприводим над K, то поле $L = K(\alpha)$ является квадратичным расширением поля K. Единственный нетождественный автоморфизм σ этого расширения действует по правилу: $\sigma(\alpha) = \alpha + 1$; поэтому

$$\mathrm{Sp}_{L/K}(\alpha) = \alpha + \sigma\alpha = \alpha + \alpha + 1 = 1, \quad \sigma(a\alpha) - (a\alpha) = a = \alpha^2 - \alpha.$$

По теореме Витта поле M, полученное присоединением к L корня многочлена $h(x) = x^2+x+a\alpha+b$, является для поля K циклическим расширением степени 4.

Обратно, пусть M/K – циклическое расширение степени 4. Обозначим через L единственное квадратичное расширение поля K, содержащееся в M; как и для любого квадратичного расширения поля характеристики 2, найдется элемент $a \in K$, такой что поле L получается присоединением к K корня α многочлена x^2+x+a, и единственный нетождественный автоморфизм σ этого расширения отображает α в $\alpha+1$. Поскольку

$$\mathrm{Sp}_{L/K}(\alpha) = \alpha + \sigma\alpha = \alpha + \alpha + 1 = 1, \qquad \sigma(a\alpha) - (a\alpha) = a = \alpha^2 - \alpha,$$

по теореме Витта существует такой элемент $b \in K$, что поле M получается присоединением к L корня многочлена $h(x) = x^2 + x + a\alpha + b$. Как мы видели в начале доказательства леммы, M совпадает с полем разложения многочлена $f(x;a,b)$. Лемма полностью доказана.

Предложение 1. *Многочлен* $x^4 + (1 + t_1)x^2 + t_1 x + t_1^3 + t_2^2 + t_1 t_2 \in (k(t_1, t_2))[x]$ *является генерирующим многочленом для группы* $\mathbb{Z}_4$ *над полем* k *характеристики* 2.

Доказательство. Трехчлен $x^2 + x + t_1$ неприводим над полем $k(t_1, t_2)$ рациональных функций от независимых переменных t_1, t_2, и потому по лемме 1 группа Галуа многочлена $x^4 + (1 + t_1)x^2 + t_1 x + t_1^3 + t_2^2 + t_1 t_2$ над полем $k(t_1, t_2)$ является циклической группой порядка 4. По той же лемме, если K – поле, содержащее k, а M/K – циклическое расширение степени 4, то существуют такие элементы $a, b \in K$, что M – поле разложения над K многочлена $x^4 + (1 + a)x^2 + ax + a^3 + b^2 + ab$.

3. Генерирующий многочлен для группы D_4

Лемма 2. *Пусть* K – *поле характеристики* 2, $a, b \in K$ *и* M – *поле разложения многочлена* $x^4 + (1 + a)x^2 + ax + b$ *над полем* K. *Тогда степень* $(M : K)$ *расширения* M/K *является делителем числа* 8.

Доказательство. Пусть $L \supseteq K$ – поле, полученное присоединением к K корня α многочлена $x^2 + ax + b$. Над полем L многочлен $x^4 + (1 + a)x^2 + ax + b$ раскладывается в произведение двух квадратичных сомножителей:

$$x^4 + (1 + a)x^2 + ax + b = x^4 + (1 + a)x^2 + ax + \alpha^2 + a\alpha =$$
$$= (x^2 + x + \alpha)(x^2 + x + \alpha + a);$$

пусть $\beta, \gamma \in M$ – какие-то корни первого и второго сомножителей, и пусть $N = L(\beta)$. Тогда $N(\gamma) = LM$; все расширения LM/N, N/L, L/K являются квадратичными или тривиальными, и потому степень $(LM : K) = (LM : N)(N : L)(L : K)$ делит 8. Тем более делит 8 степень над K подполя M поля LM.

Лемма 3. *Пусть* k – *поле характеристики* 2. *Многочлен* $x^4 + (1 + t_1)x^2 + t_1 x + t_2$ *сепарабелен над полем* $k(t_1, t_2)$ *рациональных функций от независимых переменных* t_1, t_2, *и его группой Галуа над полем* $k(t_1, t_2)$ *является диэдральная группа* D_4.

Доказательство. То, что $x^4 + (1 + t_1)x^2 + t_1 x + t_2$ – сепарабельный многочлен, очевидно. Его группа Галуа G является подгруппой симметрической группы S_4; с другой стороны, порядок группы G равен степени поля разложения многочлена $x^4 + (1 + t_1)x^2 +$

$t_1x + t_2$, которая по лемме 2 является делителем числа 8. Мы видели выше, что группы Галуа специализаций $x^4 + (1 + t_1)x^2 + t_1x + t_1^3 + t_2^2 + t_1t_2$, $x^4 + (1 + t_1)x^2 + t_1x + t_1t_2 + t_2^2$ многочлена $x^4 + (1 + t_1)x^2 + t_1x + t_2$ равны соответственно $\mathbb{Z}_4$ и V_4. Но группа Галуа любой специализации является подгруппой G. Итак, группа G обладает следующими свойствами: она является подгруппой S_4; у нее есть подгруппы, изоморфные $\mathbb{Z}_4$ и V_4; ее порядок делит 8. Этим условиям удовлетворяет только диэдральная группа D_4.

Лемма 4. *Пусть K – поле характеристики 2, и пусть M/K – расширение Галуа с диэдральной группой Галуа D_4. Тогда существуют такие элементы $a, b \in K$, что M является полем разложения над K многочлена $x^4 + (1 + a)x^2 + ax + b$.*

Доказательство. Диэдральная группа Галуа расширения M/K порождена автоморфизмами σ, τ, такими что $\sigma^2 = \tau^4 = 1$, $\sigma\tau = \tau^3\sigma$. Пусть L – подполе, состоящее из всех элементов поля M, инвариантных относительно τ^2 и σ, а $M_1 \supset L$ – поле всех σ-инвариантных элементов поля M. Поле L является квадратичным расширением поля K, а поле M_1 – квадратичным расширением поля L (но поле M_1 не является нормальным расширением поля K).

Поскольку M_1 – расширение Галуа степени 2 поля L, существует такой элемент $\alpha \in L$, что M_1 получается присоединением к L корня β многочлена $x^2 + x + \alpha$. Но α – элемент квадратичного расширения L/K; поэтому существуют такие $a, b \in K$, что $\alpha^2 = a\alpha + b$. Произведение многочленов

$$\begin{aligned}(x^2 + x + \alpha)(x^2 + x + \alpha + a) &= x^4 + x^2 + \alpha^2 + ax^2 + ax + a\alpha \\ &= x^4 + (1 + a)x^2 + ax + b\end{aligned}$$

является многочленом с коэффициентами из K, и β – корень этого многочлена, поскольку β – корень первого сомножителя.

Заметим, что $K(\beta) = M_1$; в самом деле, $\beta \in M_1$, и если бы элемент β не порождал M_1, то он порождал бы квадратичное над K подполе M_1, а такое поле только одно – это поле L, которому элемент β не принадлежит. Единственным нормальным расширением K, содержащим $M_1 = K(\beta)$ и содержащимся в M, является само поле M. Но мы видели, что β принадлежит полю разложения M' многочлена $x^4 + (1 + a)x^2 + ax + b$, и потому $K(\beta) \subseteq M'$, а тогда и нормальное замыкание M поля $K(\beta)$ содержится в M'.

С другой стороны, по лемме 2 степень расширения M'/K делит степень 8 расширения M/K; поэтому поле M совпадает с полем разложения M' многочлена $x^4+(1+a)x^2+ax+b$.

Леммы 3, 4 в точности означают, что справедливо

Предложение 2. *Многочлен $x^4+(1+t_1)x^2+t_1x+t_2 \in (k(t_1,t_2))[x]$ является генерирующим многочленом для группы D_4 над полем k характеристики 2.*

4. Генерирующие многочлены для знакопеременной группы A_4

Лемма 5. *Пусть K – поле характеристики 2, M/K – расширение Галуа с группой Галуа A_4, $L \supset K$ – подполе M степени 3 над K. Предположим, что поле L является полем разложения многочлена z^3+dz+e, где $d,e \in K$. Тогда существует такой элемент $a \in K$, что M – поле разложения многочлена*

$$f(x;a,d,e) = (x^2+x)^3 + a^2d^2(x^2+x) + a^3e^2.$$

Доказательство. Пусть η_1,η_2,η_3 – корни многочлена z^3+dz+e; по теореме Виета их сумма $\eta_1+\eta_2+\eta_3$ равна 0. Корнями многочлена $q(z) = z^3+a^2d^2z+a^3e^2$ будут элементы $a\eta_i^2$:

$$q(a\eta_i^2) = a^3\eta_i^6 + a^3d^2\eta_i^2 + a^3e^2 = a^3(\eta_i^3+d\eta_i+e)^2 = 0;$$

поэтому $q(z) = (z+a\eta_1^2)(z+a\eta_2^2)(z+a\eta_3^2)$, и значит,

$$f(x;a,d,e) = q(x^2+x) = ((x^2+x)+a\eta_1^2)((x^2+x)+a\eta_2^2)((x^2+x)+a\eta_3^2).$$

Таким образом, нам достаточно доказать, что при некотором $a \in K$ существуют элементы $\alpha_i \in M$, не принадлежащие L и являющиеся корнями квадратичных трехчленов $x^2+x+a\eta_i^2$ $(i=1,2,3)$; действительно, тогда поле разложения многочлена $f(x;a,d,e)$ содержит элемент $\alpha_1 \in M$, не принадлежащий L, и, поскольку в M нет нормальных над K подполей, кроме K, L, M, оно совпадает с M.

В поле M есть три сопряженных над K подполя $N_1,N_2,N_3 \supset L$, степень каждого из которых над L равна 2. Как и всякое квадратичное расширение, поле N_1 является полем разложения многочлена $h_1(x) = x^2+x+\mu$, где μ – какой-то элемент из L. Но элементы η_1^2, η_1, 1, составляют базис L над K, поэтому существуют такие $a', b, c \in K$, что $\mu = a'\eta_1^2 + b\eta_1 + c$. Поля N_2, N_3 являются полями разложения многочленов

$$h_2(x) = x^2 + x + a'\eta_2^2 + b\eta_2 + c, \quad h_3(x) = x^2 + x + a'\eta_3^2 + b\eta_3 + c,$$

сопряженных с $h_1(x)$ над K. Пусть $\delta_2 \in N_2$, $\delta_3 \in N_3$ – какие-то корни многочленов $h_2(x)$, $h_3(x)$. Положим $a = a' + b^2$ и покажем, что элементы $\alpha_1 = \delta_2 + \delta_3 + b\eta_1$, $\alpha_2 = \delta_1 + \delta_3 + b\eta_2$, $\alpha_3 = \delta_1 + \delta_2 + b\eta_3$ не принадлежат L и являются корнями многочленов $x^2 + x + a\eta_i^2$. Если бы элемент α_1 принадлежал L, то и элемент $\alpha_1 - b\eta_1 = \delta_2 + \delta_3$ принадлежал бы L, а тогда элемент $\delta_3 = \alpha_1 - b\eta_1 - \delta_2$ содержался бы и в поле N_3, и в поле N_2, а значит, и в их пересечении L, что неверно, так как $L \neq N_3 = L(\delta_3)$. Далее,

$$\alpha_1^2 + \alpha_1 + a\eta_1^2 = \delta_2^2 + \delta_3^2 + b^2\eta_1^2 + \delta_2 + \delta_3 + b\eta_1 + a'\eta_1^2 + b^2\eta_1^2 = (a'\eta_2^2 + b\eta_2 + c) +$$
$$+ (a'\eta_3^2 + b\eta_3 + c) + a'\eta_1^2 + b\eta_1 = a'(\eta_2 + \eta_3 + \eta_1)^2 + b(\eta_2 + \eta_3 + \eta_1) = 0,$$

и точно так же показывается, что элементы α_2 и α_3 не принадлежат L и удовлетворяют соотношениям $\alpha_2^2 + \alpha_2 + a\eta_2^2 = 0$, $\alpha_3^2 + \alpha_3 + a\eta_3^2 = 0$.

Лемма 6. *Пусть K – поле характеристики 2 и пусть $a, d, e \in K$, причем $a \neq 0$, $e \neq 0$. Тогда многочлены*

$$f(x; a, d, e) = (x^2 + x)^3 + a^2 d^2 (x^2 + x) + a^3 e^2,$$
$$g(x; a, d, e) = x^4 + dx^2 + ex + ae^2$$

имеют общее поле разложения M. Если группа Галуа поля разложения L многочлена $z^3 + dz + e$ является циклической группой порядка 3, а многочлен $g(x; a, d, e)$ неприводим над K, то группа Галуа расширения M/K изоморфна A_4.

Доказательство. До конца доказательства мы будем обозначать многочлены $f(x; a, d, e)$ и $g(x; a, d, e)$ через $f(x)$ и $g(x)$. Обозначим через M поле разложения многочлена $g(x)$, а через η_1, η_2, η_3 – корни многочлена $z^3 + dz + e$.

Напомним, что кубическая резольвента многочлена общего вида $x^4 + \bar{a}x^3 + \bar{b}x^2 + \bar{c}x + \bar{d}$ равна $z^3 - \bar{b}z^2 + (\bar{a}\bar{c} - 4\bar{d})z + 4\bar{b}\bar{d} - \bar{d}\bar{a}^2 - \bar{c}^2$. В частности, учитывая, что характеристика поля равна 2, находим, что кубическая резольвента многочлена $g(x) = x^4 + dx^2 + ex + ae^2$

равна $z^3+dz^2+e^2$. Корнями резольвенты являются элементы e/η_i $(i=1,2,3)$; действительно,

$$(e/\eta_i)^3 + d(e/\eta_i)^2 + e^2 = e^2(\eta_i^3 + d\eta_i + e)/\eta_i^3 = 0.$$

Обозначим через $\beta, \beta_1, \beta_2, \beta_3 \in M$ корни многочлена $g(x)$; тогда $\beta\beta_1 + \beta_2\beta_3$, $\beta\beta_2 + \beta_1\beta_3$, $\beta\beta_3 + \beta_1\beta_4$ – корни резольвенты, так что при надлежащей нумерации корней

$$\beta\beta_1 + \beta_2\beta_3 = e/\eta_1, \quad \beta\beta_2 + \beta_1\beta_3 = e/\eta_2, \quad \beta\beta_3 + \beta_2\beta_4 = e/\eta_3$$

(отсюда, в частности, следует, что элементы η_i принадлежат полю M). Поскольку произведение всех корней $\beta, \beta_1, \beta_2, \beta_3$ многочлена $g(x)$ равно его свободному члену ae^2, предыдущие равенства можно переписать так:

$$(\beta\beta_i)^2 + e(\beta\beta_i)/\eta_i = ae^2 \qquad (i=1,2,3).$$

Обозначим через α_i элемент $\beta\beta_i\eta_i/e$; тогда

$$\alpha_i^2 + \alpha_i = \eta_i^2((\beta\beta_i)^2 + e(\beta\beta_i)/\eta_i)/e^2 = \eta_i^2 \cdot ae^2/e^2 = a\eta_i^2.$$

Таким образом, элементы $\alpha_1, \alpha_2, \alpha_3 \in M$ являются корнями многочлена

$$\begin{aligned}((x^2+x)+a\eta_1^2)&((x^2+x)+a\eta_2^2)((x^2+x)+a\eta_3^2)\\ &= (x^2+x)^3 + a^2d^2(x^2+x) + a^3e^2 = f(x);\end{aligned}$$

остальными его корнями являются элементы $\alpha_1+1, \alpha_2+1, \alpha_3+1 \in M$. Мы видим, что поле разложения $K(\alpha_1, \alpha_2, \alpha_3)$ многочлена $f(x)$ содержится в поле разложения M многочлена $g(x)$.

Докажем обратное включение. Заметим что элементы

$$\eta_i^2 = (\alpha_i^2 + \alpha_i)/a, \quad \eta_i = e/(\eta_i^2 + d), \quad \beta\beta_i = e\alpha_i/\eta_i \ \ (i=1,2,3)$$

принадлежат $K(\alpha_1, \alpha_2, \alpha_3)$. Остается показать,
что $\beta \in K(\alpha_1, \alpha_2, \alpha_3)$. Мы имеем:

$$\begin{aligned}\beta^2 &= \beta^2 \cdot ae^2 \cdot e/(ae^3) = \beta^2(\beta\beta_1\beta_2\beta_3)\eta_1\eta_2\eta_3/(ae^3)\\ &= \alpha_1\alpha_2\alpha_3/a \in K(\alpha_1, \alpha_2, \alpha_3),\end{aligned}$$

откуда и следует, что $\beta = (\beta^4 + d\beta^2 + ae^2)/e \in K(\alpha_1, \alpha_2, \alpha_3)$.

Пусть теперь поле разложения $L = K(\eta_1, \eta_2, \eta_3)$ многочлена $z^3 + dz + e$ является расширением Галуа поля K с циклической группой порядка 3 и многочлен $g(x)$ неприводим над K. Мы видели, что элементы η_i принадлежат M, так что $L = K(\eta_1, \eta_2, \eta_3) \subseteq M$. Поскольку многочлен $g(x)$ неприводим, группа Галуа расширения M/K является транзитивной подгруппой группы S_4; в то же время у нее есть факторгруппа $\mathrm{Gal}(L/K)$, порядка 3. Единственной такой подгруппой S_4 является группа A_4.

Лемма 6 полностью доказана.

Предложение 3. *Многочлен* $x^4 + (t_1^2 + t_1 + 1)x^2 + (t_1^2 + t_1 + 1)x + t_2(t_1^2 + t_1 + 1)^2 \in (k(t_1, t_2))[x]$ *является генерирующим для группы* A_4 *над полем* k *характеристики* 2.

Доказательство. В обозначениях леммы 6 многочлен, указанный в формулировке предложения, равен $g(x; t_2, v, v)$, где через v для краткости обозначен многочлен $1 + t_1 + t_1^2$. Сначала докажем две леммы.

Лемма 7. *Многочлен* $z^3 + (t_1^2 + t_1 + 1)z + (t_1^2 + t_1 + 1) \in k[z, t_1]$ *является генерирующим над* k *многочленом для циклических расширений степени* 3.

Доказательство. Над полем любой характеристики многочлен $z^3 - t_1 z^2 + (t_1 - 3)z + 1$ является генерирующим многочленом для циклической группы порядка 3 (см. [5]). Для полей характеристики 2 он приобретает вид $q(z) = z^3 + t_1 z^2 + (t_1 + 1)z + 1$. Вместе с ним генерирующим является и многочлен

$$q(z + t_1) = z^3 + (t_1^2 + t_1 + 1)z + (t_1^2 + t_1 + 1).$$

Лемма 8. *Многочлен* $g(x; t_2, v, v)$ *неприводим над* K.

Доказательство. Если этот многочлен приводим над полем $K = k(t_1, t_2)$, то по теореме Гаусса существует разложение

$$g(x; t_2, v, v) = x^4 + vx^2 + vx + t_2 v^2 = h_1(x, t_1, t_2) h_2(x, t_1, t_2),$$

в котором $h_1(x, t_1, t_2), h_2(x, t_1, t_2) \in k[x, t_1, t_2]$ и степени обоих сомножителей относительно x положительны. При $t_1 = 0$ многочлен $v = 1 + t_1 + t_1^2$ принимает значение 1, и мы получаем разложение

$$x^4 + x^2 + x + t_2 = p_1(x, t_2) p_2(x, t_2),$$

где
$p_i(x, t_2) = h_i(x, 0, t_2) \in k[x, t_2]$, $\deg_x(p_i(x, t_2)) = \deg_x(h_i(x, t_1, t_2)) > 0$

$(i=1,2)$. Но многочлен $x^4+x^2+x+t_2$ линеен относительно t_2; поэтому в предыдущем разложении один из сомножителей $p_i(x,t_2)$ имеет относительно t_2 степень 0, т.е. $p_i(x,t_2)=h(x)\in k[x]$. Тогда коэффициент 1 при t_2 в многочлене $x^4+x^2+x+t_2$ делится в $k[x]$ на $h(x)$, и потому $\deg_x(h_i(x,t_2,t_1))=\deg_x(p_i(x,t_2))=\deg_x(h(x))=0$ вопреки предположению. Лемма доказана.

Вернемся к доказательству предложения. По лемме 7 поле разложения многочлена

$$z^3+vz+v=z^3+(1+t_1+t_1^2)z+(1+t_1+t_1^2)$$

является циклическим расширением степени 3 поля $k(t_1,t_2)$, а по лемме 8 многочлен $g(x;t_2,v,v)$ неприводим над $k(t_1,t_2)$; поэтому из леммы 6 следует, что группа Галуа многочлена $g(x;t_2,v,v)$ над полем $k(t_1,t_2)$ изоморфна A_4.

Пусть теперь K – поле, содержащее k, а M/K – расширение Галуа с группой Галуа A_4. В поле M есть подполе $L\supset K$, которое является расширением Галуа поля K с циклической группой Галуа порядка 3; по лемме 7 существует такой элемент $b\in K$, что L – поле разложения многочлена z^3+dz+e при $d=e=b^2+b+1$. Далее, по лемме 5 существует такой элемент $a\in K$, что поле M является полем разложения многочлена $f(x;a,d,e)$; наконец, по лемме 6 это же поле является полем разложения многочлена

$$g(x;a,d,e)=g(x;a,b^2+b+1,b^2+b+1).$$

Литература

1. E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f.* — J. Reine Angew. Math. **174** (1936), 237–245.
2. G. Kemper and E. Mattig, *Generic polynomials with few parameters.* — Symb. Comp. **30** (2000), 843–857.
3. G. Kemper, *Das Noethersche Problem und generische Polynome.* Dissertation, Universitat Heidelberg (1994).
4. H. Tsunogai and K. Hashimoto, *Generic polynomials over $\mathbb{Q}$ with two parameters for the transitive groups of degree five.* — Proc. Japan Acad. **79A** (2003), 148–151.
5. J.-P. Serre, *Topics in Galois theory.* Jones and Barthelett Publ., Boston (1992).

Sergeev A. E., Yakovlev A. V. Generic polynomials for transitive subgroups of the group S_4 over fields of characteristic 2.

Generic polynomials for the symmetric group S_4, the Klein group V_4, the cyclic group of order 4, the dihedral group D_4 and the alternative group A_4 over fields of characteristic 2 are explicitly described.

С.-Петербургский
государственный университет
E-mail: yakovlev@yak.pdmi.ras.ru

Поступило 31 октября 2005 г.