ДОКЛАДЫ АКАДЕМИИ НАУК, 2010, том 433, № 2, с. 154–157

МАТЕМАТИКА

УДК 511.6

О НОВОМ ЛОКАЛЬНО-ГЛОБАЛЬНОМ ПРИНЦИПЕ ДЛЯ КВАДРАТИЧНЫХ ФУНКЦИОНАЛЬНЫХ ПОЛЕЙ

© 2010 г. В. В. Беняш-Кривец, академик В. П. Платонов

Поступило 03.03.2010 г.

Пусть K – поле алгебраических чисел, $[K:\mathbb{Q}]<\infty$, V^K – множество всех попарно неэквивалентных нормирований поля K.

Пусть $f(x)=x^{2n}+a_{2n-1}x^{2n-1}+\ldots+a_0\in K[x]$ – свободный от квадратов многочлен. Обозначим

$$D_f = K[x](\sqrt{f}) = \{\alpha+\beta\sqrt{f}\,|\,\alpha,\beta\in K[x]\}.$$

Элемент $u\in D_f$ называется единицей, если u обратим в D_f. Если $u\in K^*$, то u называется тривиальной единицей. Предположим, что D_f обладает нетривиальными единицами. Тогда $D_f^* = K^*\times\langle u_1\rangle$, где $\langle u_1\rangle$ – бесконечная циклическая группа. Элемент u_1 называется фундаментальной единицей в D_f.

Проблема существования нетривиальных единиц в D_f является трудной и имеет глубокие связи с кручением в якобиевых многообразиях кривых $y^2=f(x)$ и с непрерывными дробями в функциональных полях (см. [1]).

Пусть $v\in V^K$, $\mathbf{O}_v$ – кольцо нормирования для неархимедова v, $\mathbf{p}_v$ – максимальный идеал в $\mathbf{O}_v$, $k_v=\mathbf{O}_v/\mathbf{p}_v$ – поле вычетов, являющееся конечным полем. Для почти всех $v\in V^K$ все коэффициенты многочлена $f(x)$ принадлежат $\mathbf{O}_v$. Мы можем рассмотреть многочлен $f_v(x)$, получающийся из $f(x)$ редукцией его коэффициентов по модулю $\mathbf{p}_v$: $f_v(x)\in k_v[x]$.

Нетрудно показать, что для почти всех v многочлен $f_v(x)$ свободен от квадратов. Рассмотрим

$$D_{f_v} = \{\alpha_v+\beta_v\sqrt{f_v(x)}\,|\,\alpha_v,\beta_v\in k_v[x]\}.$$

Хорошо известно, что D_{f_v} имеет нетривиальные единицы, так что $D_{f_v}^* = k_v^*\times u_v$, где u_v – фундаментальная единица в D_{f_v}. Если $u_v=\alpha_v+\beta_v\sqrt{f_v}$, то определим $\deg u_v=\deg\alpha_v$. В [1] установлен следующий локально-глобальный принцип нового типа.

Белорусский государственный университет, Минск
Научно-исследовательский институт системных исследований Российской Академии наук, Москва

Т е о р е м а 1. *D_f обладает нетривиальной единицей тогда и только тогда, когда существует такая константа C, что $\deg u_v<C$ для почти всех $v\in V^K$.*

Доказательство использует свойства якобиева многообразия кривой $y^2=f(x)$ и ее локализаций. В конце статьи [1] было замечено, что, возможно, методы работ [2, 3] могут быть применены к проблеме существования нетривиальных единиц.

Цель настоящего сообщения – дать принципиально новое доказательство теоремы 1 с помощью методов работы [2] (полное изложение содержится в [4]), а также для широкого класса многочленов f, где $\deg f=4$, решить проблему существования и вычисления фундаментальных единиц. При этом мы не используем якобиевы многообразия.

Следующий результат справедлив для произвольного поля K характеристики, отличной от 2. Сохраним введенные выше обозначения для многочлена $f(x)$ и кольца D_f. Обозначим через $|\cdot|_\infty$ бесконечное нормирование на $K(x)$ и пусть $\overline{K(x)}$ – пополнение $K(x)$ относительно $|\cdot|_\infty$. Произвольный элемент $z\in K(x)$ можно разложить в ряд Лорана $z=z_mx^m+z_{m-1}x^{m-1}+\ldots$, где $z_i\in K$, $z_m\neq 0$, и тогда $|z|_\infty=-m$. Поскольку нормирование $|\cdot|_\infty$ имеет два продолжения на $K(x)(\sqrt{f})$, то $\sqrt{f}\in\overline{K(x)}$. Разложим $\sqrt{f}$ в ряд Лорана:

$$\sqrt{f} = x^s+d_{s-1}x^{s-1}+d_{s-2}x^{s-2}+\ldots \qquad (1)$$

и рассмотрим матрицу

$$H_r=\begin{pmatrix} d_{-1} & d_{-2} & \ldots & d_{-r} \\ d_{-2} & d_{-3} & \ldots & d_{-r-1} \\ \vdots & \vdots & \ddots & \vdots \\ d_{-r-s+2} & d_{-r-s+1} & \ldots & d_{-2r-s+3}\end{pmatrix}. \qquad (2)$$

Эта матрица имеет r столбцов и $r+s-2$ строки. Справедлива

Т е о р е м а 2. *Кольцо D_f имеет фундаментальную единицу $u=\alpha+\beta\sqrt{f}$, где $\alpha,\beta\in K[x]$ и $\deg\beta=r$, тогда и только тогда, когда ранг матрицы H_{r+1}*

меньше, чем $r+1$, *и* $\operatorname{rank} H_m = m$ *при* $m < r+1$. *При этом* $\deg u = r+s$.

Доказательство. Пусть $u = \alpha + \beta\sqrt{f}$ – нетривиальная единица в D_f, и пусть

$$\alpha(x) = f_m x^m + f_{m-1}x^{m-1} + \ldots + f_0,$$

$$\beta(x) = g_r x^r + g_{r-1}x^{r-1} + \ldots + g_0,$$

где $f_m \neq 0$, $g_r \neq 0$. Поскольку $\alpha^2 - \beta^2 f \in K^*$, то $m = r+s$ и

$$|\alpha + \beta\sqrt{f}|_\infty + |\alpha - \beta\sqrt{f}|_\infty = 0. \qquad (3)$$

Разложим $\beta\sqrt{f}$ в ряд Лорана:

$$\beta\sqrt{f} = h_m x^m + h_{m-1}x^{m-1} + \ldots,$$

где $h_i = \sum_{j+t=i} g_j d_t \in K$, $h_m \neq 0$. Поскольку $f_m + h_m$ и $f_m - h_m$ одновременно не обращаются в нуль, то не может быть одновременно $|\alpha + \beta\sqrt{f}|_\infty = |\alpha - \beta\sqrt{f}|_\infty = 0$. Пусть для определенности $|\alpha + \beta\sqrt{f}|_\infty > 0$, $|\alpha - \beta\sqrt{f}|_\infty < 0$. Тогда мы должны иметь

$$f_m = h_m, \quad f_{m-1} = h_{m-1}, \ldots, f_0 = h_0. \qquad (4)$$

Кроме того, из (3) следует, что $|\alpha + \beta\sqrt{f}|_\infty = m$, $|\alpha - \beta\sqrt{f}|_\infty = -m$. Следовательно,

$$h_{-1} = h_{-2} = \ldots = h_{-m+1} = 0,$$

откуда получаем систему уравнений

$$\begin{aligned} d_{-1}g_0 + d_{-2}g_1 + \ldots + d_{-r-1}g_r &= 0,\\ d_{-2}g_0 + d_{-3}g_1 + \ldots + d_{-r-2}g_r &= 0,\\ &\vdots\\ d_{-m+1}g_0 + d_{-m}g_1 + \ldots + d_{-m-r+1}g_r &= 0. \end{aligned} \qquad (5)$$

Пусть $\mathbf{g} = (g_0, g_1, \ldots, g_r)^t$. Тогда (5) можно записать в матричном виде:

$$H_{r+1}\mathbf{g} = 0. \qquad (6)$$

Таким образом, однородная система линейных уравнений (6) с матрицей H_{r+1} имеет ненулевое решение $\mathbf{g}$. Значит, ранг матрицы H_{r+1} меньше, чем $r+1$.

Обратно, предположим, что ранг матрицы H_{r+1} меньше, чем $r+1$. Тогда однородная система линейных уравнений (6) имеет ненулевое решение $\mathbf{g}$, причем в этом решении $g_r \neq 0$. Вычислим по формулам (4) коэффициенты многочлена f. Тогда по построению имеем, что $|\alpha + \beta\sqrt{f}|_\infty = m$, $|\alpha - \beta\sqrt{f}|_\infty = -m$. Следовательно,

$$|\alpha^2 - \beta^2 f|_\infty = |\alpha + \beta\sqrt{f}|_\infty + |\alpha - \beta\sqrt{f}|_\infty = 0.$$

Поскольку $\alpha^2 - \beta^2 f \in K[x]$, то мы должны иметь $\alpha^2 - \beta^2 f \in K^*$, а значит, $u = \alpha + \beta\sqrt{f}$ – нетривиальная единица кольца D_f. Поскольку по построению $\deg\beta = r$, то $\deg u = r+s$.

Отметим, что если мы найдем наименьшее натуральное r, такое что ранг матрицы H_r меньше, чем r, то получим фундаментальную единицу кольца D_f.

Далее снова будем считать, что K – поле алгебраических чисел. Покажем, что теорема 1 следует из теоремы 2.

Предположим, что $u = \alpha + \beta\sqrt{f}$ – нетривиальная единица в D_f. Обозначим через S множество таких нормирований $v \in V^K$, что все коэффициенты многочленов $f(x)$, $\alpha(x)$, $\beta(x)$ принадлежат $\mathbf{O}_v$, многочлен $f_v(x)$ свободен от квадратов и характеристика поля k_v отлична от 2. Ясно, что $V^K \setminus S$ – конечное множество. Поскольку $\alpha^2 - \beta^2 f \in K^*$, то для любого $v \in S$ имеем $\alpha_v^2 - \beta_v^2 f_v \in k_v^*$. Это означает, что элемент $u'_v = \alpha_v + \beta_v\sqrt{f_v}$ является единицей кольца D_{f_v}. Ясно, что $\deg u'_v \leq \deg u$. Поскольку для фундаментальной единицы u_v кольца D_{f_v} $\deg(u_v) \leq \deg(u'_v) \leq \deg(u)$, то в качестве константы C можно взять $\deg(u)$.

Докажем обратное утверждение. Предположим, что $\deg u_v < C$ для всех $v \in S$. Возьмем произвольное $v \in S$. Пусть $\overline{k_v(x)}$ – пополнение поля $k_v(x)$ относительно бесконечного нормирования $|\cdot|_\infty$. Так как $\sqrt{f_v} \in \overline{k_v(x)}$, то мы можем разложить $\sqrt{f_v}$ в ряд Лорана:

$$\sqrt{f_v} = x^s + (d_{s-1})_v x^{s-1} + (d_{s-2})_v x^{s-2} + \ldots,$$

где коэффициенты $(d_i)_v$ являются редукцией коэффициентов d_i из разложения (1) по модулю $\mathbf{p}_v$. Обозначим через $H_{r,v}$ матрицу, которая получается из матрицы H_r редукцией ее элементов по модулю $\mathbf{p}_v$. Поскольку в кольце D_{f_v} есть нетривиальная фундаментальная единица u_v, то по теореме 2 найдется натуральное число $r = r(v)$, такое что ранг матрицы $H_{r,v}$ меньше, чем r. Это означает, что все миноры порядка r в матрице $H_{r,v}$ равны 0. При этом $\deg(u_v) = r(v) + s - 1$. Учитывая условия теоремы, получаем, что $r(v) \leq C - s + 1$.

Поскольку множество S бесконечно, то для бесконечного подмножества $S_1 \subset S$ должно быть $r(v_1) = r(v_2)$ для любых $v_1, v_2 \in S_1$. Пусть $v \in S_1$, T – произвольный минор порядка r матрицы H_r и T_v – соответствующий минор матрицы $H_{r,v}$. Ясно, что T_v получается из T редукцией по модулю $\mathbf{p}_v$. Как отмечено выше, $T_v = 0$ для всех $v \in S_1$. В силу бесконечности S_1 отсюда следует, что $T = 0$. Таким образом, все миноры порядка r в матрице H_r равны 0. Следовательно, ее ранг меньше r и по

теореме 2 в кольце D_f существует нетривиальная единица. Теорема 2 доказана.

Алгоритмическое решение проблемы существования нетривиальных единиц в кольце D_f для многочленов f, $\deg f \le 4$, получено в [1] на основе редукции к проблеме кручения в эллиптических кривых. Для случая $K = \mathbb{Q}$ в [1] сделано важное наблюдение: степень фундаментальной единицы не превосходит 12 и не может быть равна 11. Это открывает путь к быстрому прямому вычислению нетривиальных единиц. В случае $\deg f = 4$ матрица H_r, определенная в (2), является ганкелевой и условие $\operatorname{rank} H_r < r$ эквивалентно тому, что $\det H_r = 0$.

В [1] дан ответ на вопрос, поставленный Ф. Груневальдом: для многочлена $f(x) = x^4 + x + 1$ кольцо D_f не содержит нетривиальных единиц. Также в [1] отмечено, что если $f(x) = x^4 + c$ либо $f(x) = x^4 + x$, то соответствующее кольцо D_f обладает нетривиальными единицами.

Используя развитые в настоящем сообщении методы, можно дать полный ответ на вопрос, для каких многочленов $f(x) = x^4 + bx + c$ кольцо D_f обладает нетривиальными единицами.

Теорема 3. *Для многочлена $f(x) = x^4 + bx + c$ кольцо D_f обладает фундаментальной единицей степени n при следующих значениях n, b и* c:

1) $n = 2$, $b = 0$, $c \in \mathbb{Q}^*$, $u = x^2 + \sqrt{f}$;

2) $n = 3$, $c = 0$, $b \in \mathbb{Q}^*$, $u = x^3 + \dfrac{b}{2} + x\sqrt{f}$;

3) $n = 4$, $b = t^3$, $c = \dfrac{t^4}{2}$, где $t \in \mathbb{Q}^*$, $u = x^4 - tx^3 + \dfrac{t^2}{2}x^2 + \dfrac{t^3}{2}x - \dfrac{t^4}{4} + \left(x^2 - tx + \dfrac{t^2}{2}\right)\sqrt{f}$.

Доказательство. Разложение $\sqrt{f}$ в ряд Лорана имеет вид

$$\sqrt{f} = x^2 + \frac{1}{2}bx^{-1} + \frac{1}{2}cx^{-2} - \frac{1}{8}b^2x^{-4} - \frac{1}{4}bcx^{-5} - \frac{1}{8}c^2x^{-6} + \frac{1}{16}b^3x^{-7} + \frac{3}{16}b^2cx^{-8} + \ldots,$$

где коэффициенты d_{-i} при x^{-i} вычисляются по рекуррентным формулам

$$d_{-(2m+1)} = -d_{-1}d_{-2m} - \ldots - d_{-m}d_{-m-1},$$

$$d_{-2m} = -d_{-1}d_{-2m+1} - \ldots - d_{-m+1}d_{-m-1} - \frac{1}{2}d_{-m}^2.$$

По теореме 2 кольцо D_f имеет нетривиальную единицу u степени $r + 1$ тогда и только тогда, когда $\det H_r = 0$.

При $r = 1$ имеем $\det H_r = \dfrac{b}{2} = 0$, следовательно, $f(x) = x^4 + c$. Этот случай рассмотрен в [1]. Очевидно, элемент $u = x^2 + \sqrt{f}$ является фундаментальной единицей кольца D_f.

При $r = 2$ имеем $\det H_r = -\dfrac{c^2}{4} = 0$. Следовательно, $f(x) = x^4 + bx$. В этом случае фундаментальная единица кольца D_f имеет вид $u = x^3 + \dfrac{b}{2} + x\sqrt{f}$.

При $r = 3$ имеем $\det H_r = \dfrac{1}{128}b(-b^4 + 9c^3) = 0$. Случай $b = 0$ рассмотрен выше. Нетрудно показать, что уравнение $-b^4 + 8c^3 = 0$ имеет следующие рациональные решения: $b = t^3$, $c = \dfrac{t^4}{2}$, где $t \in \mathbb{Q}^*$. Фундаментальная единица кольца D_f имеет вид

$$u = x^4 - tx^3 + \frac{t^2}{2}x^2 + \frac{t^3}{2}x - \frac{t^4}{4} + \left(x^2 - tx + \frac{t^2}{2}\right)\sqrt{f}.$$

Отметим, при любом $t \in \mathbb{Q}^*$ эллиптическая кривая $y^2 = f(x)$ бирегулярно изоморфна кривой $y_1^2 = f_1(x)$, где $f_1(x) = x_1^4 + x_1 + \dfrac{1}{2}$. Соответствующий изоморфизм задается формулами $x = tx_1$, $y = t^2y_1$.

При $r = 4$ имеем

$$\det H_r = \frac{1}{256}\left(c^6 + \frac{1}{2}c^3b^4 - \frac{1}{16}b^8\right) = 0. \qquad (7)$$

Сделав замену переменных $z = \dfrac{c^3}{b^4}$, уравнение (7) можно переписать в виде

$$h_r(z) = z^2 + \frac{1}{2}z - \frac{1}{16} = 0. \qquad (8)$$

Поскольку многочлен $h_r(z)$ в (8) не имеет рациональных корней, то уравнение (7) не имеет рациональных решений b, c. Таким образом, не существует многочленов $f(x)$, таких что кольцо D_f имеет фундаментальную единицу степени $n = r + 1 = 5$.

Аналогичные вычисления показывают, что при $r = 5, 6, 7, 8, 9, 11$ элемент $z = \dfrac{c^3}{b^4}$ является корнем многочлена $h_r(z)$, где

$$h_5(z) = 24z^2 - 12z + 1,$$

$$h_6(z) = z^4 + \frac{5}{2}z^3 - \frac{13}{16}z^2 + \frac{3}{32}z - \frac{1}{256},$$

$$h_7(z) = 512z^4 - 640z^3 + 16z - 1,$$

$$h_8(z) = 4096z^6 + 30720z^5 - 19200z^4 + 6528z^3 - 1152z^2 + 96z - 3,$$

$$h_9(z) = 20480z^6 - 73728z^5 + 35584z^4 -$$
$$- 7040z^3 + 720z^2 - 40z + 1,$$
$$h_{11}(z) = 32768z^8 - 18024z^7 - 225280z^6 +$$
$$+ 114688z^5 - 29440z^4 + 5440z^3 - 640z^2 + 40z - 1.$$

Поскольку данные многочлены $h_r(z)$, $r \geq 5$, неприводимы над $\mathbb{Q}$, то они не имеют рациональных корней. Следовательно, не существует многочленов $f(x) = x^4 + bx + c$, таких что кольцо D_f имеет фундаментальную единицу степени $n \geq 5$. Теорема 3 доказана.

При доказательстве теоремы 3 мы использовали систему компьютерной алгебры Maple для вычисления определителей $\det H_r$, разложения полученных многочленов на множители и доказательства неприводимости над $\mathbb{Q}$ многочленов $h_r(z)$, где $r \geq 5$.

Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (коды проектов № 09–01–00287, 09–01–12169).

СПИСОК ЛИТЕРАТУРЫ

1. *Платонов В.П.* // ДАН. 2010. Т. 430. № 3. С. 318–320.
2. *Беняш-Кривец В.В., Платонов В.П.* // ДАН. 2007. Т. 417. № 4. С. 446–450.
3. *Беняш-Кривец В.В., Платонов В.П.* // ДАН. 2008. Т. 423. № 2. С. 155–160.
4. *Беняш-Кривец В.В., Платонов В.П.* // Мат. сб. 2009. Т. 200. № 11. С. 15–44.