ISSN 1064-5624, Doklady Mathematics, 2010, Vol. 82, No. 1, pp. 531–534. © Pleiades Publishing, Ltd., 2010.
Original Russian Text © V.V. Benyash-Krivets, V.P. Platonov, 2010, published in Doklady Akademii Nauk, 2010, Vol. 433, No. 2, pp. 154–157.

MATHEMATICS

A New Local-Global Principle for Quadratic Functional Fields

V. V. Benyash-Krivets[a] and Academician V. P. Platonov[b]

Received March 3, 2010

DOI: 10.1134/S1064562410040083

Let K be a field of algebraic numbers with $[K:\mathbb{Q}] < \infty$, and let V^K be the set of all pairwise nonequivalent valuations of the field K.

Consider a square-free polynomial $f(x) = x^{2n} + a_{2n-1}x^{2n-1} + \ldots + a_0 \in K[x]$. We set

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

An element $u \in D_f$ is called a unit if u is invertible in D_f. If $u \in K^*$, then u is called a trivial unit. Suppose that D_f has nontrivial units. Then, $D_f^* = K^* \times \langle u_1 \rangle$, where $\langle u_1 \rangle$ is the infinite cyclic group. The element u_1 is called the fundamental unit of D_f.

The problem of the existence of nontrivial units in D_f is difficult; it is deeply related to torsion in the Jacobian varieties of curves $y^2 = f(x)$ and to continuous fractions in function fields (see [1]).

Suppose that $v \in V^K$, $\mathbf{O}_v$ is a valuation ring for non-Archimedean v, $\mathbf{p}_v$ is a maximal ideal in $\mathbf{O}_v$, and $k_v = \mathbf{O}_v/\mathbf{p}_v$ is the residue field, being a finite field. For almost every $v \in V^K$, all coefficients of the polynomial $f(x)$ belong to $\mathbf{O}_v$. Consider the polynomial $f_v(x)$, obtained from $f(x)$ by reducing its coefficients modulo $\mathbf{p}_v$: $f_v(x) \in k_v[x]$.

It is easy to show that the polynomial $f_v(x)$ is square-free for almost all v. Consider the ring

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

It is well known that D_{f_v} contains nontrivial units, so that $D_{f_v}^* = k_v^* \times u_v$, where u_v is the fundamental unit of D_{f_v}. If $u_v = \alpha_v + \beta_v\sqrt{f_v}$, then we set $\deg u_v = \deg\alpha_v$. In [1], the following local-global principle of a new type was established.

Theorem 1. *The ring D_f has a nontrivial unit if and only if there exists a constant C such that $\deg u_v < C$ for almost all $v \in V^K$.*

The proof of this theorem uses properties of the Jacobian variety of the curve $y^2 = f(x)$ and it localizations. At the end of paper [1], it was mentioned that, possibly, the methods of [2, 3] can be applied to the problem of the existence of nontrivial units.

The purpose of this paper is to present a fundamentally new proof of Theorem 1 using methods of [2] (a complete exposition is contained in [4]) and solve the problem of the existence and the determination of fundamental units for a large class of polynomials f with $\deg f = 4$. We do not employ Jacobian varieties.

The following assertion is valid for any field K of characteristic different from 2. We keep the notation for the polynomial $f(x)$ and the ring D_f introduced above. Let $|\cdot|_\infty$ be an infinite valuation on $K(x)$, and let $\overline{K(x)}$ be the completion of $K(x)$ with respect to $|\cdot|_\infty$. Any element $z \in K(x)$ can be expanded in a Laurent series $z = z_m x^m + z_{m-1}x^{m-1} + \ldots$, where $z_i \in K$ and $z_m \neq 0$; we have $|z|_\infty = -m$. Since the valuation $|\cdot|_\infty$ admits two extensions to $K(x)(\sqrt{f})$, it follows that $\sqrt{f} \in \overline{K(x)}$. Consider $\sqrt{f}$ the Laurent expansion

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

and the matrix

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

This matrix has r columns and $r + s - 2$ rows. The following theorem is valid.

Theorem 2. *The ring D_f has a fundamental unit $u = \alpha + \beta\sqrt{f}$, where $\alpha, \beta \in K[x]$ and $\deg\beta = r$, if and only if the rank of the matrix H_{r+1} is less than $r + 1$ and $\operatorname{rank} H_m = m$ if $m < r + 1$. In this case, $\deg u = r + s$.*

[a] *Belarussian State University, pr. Nezavisimosti 4, Minsk, 220030 Belarus*
e-mail: benyash@bsu.by
[b] *Research Institute for System Studies, Russian Academy of Sciences, Nakhimovskii pr. 36, korp. 1, Moscow, 117218 Russia*
e-mail: platonov@niisi.ras.ru

Proof. Suppose that $u = \alpha + \beta\sqrt{f}$ is a nontrivial unit in D_f and let

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

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

where $f_m \neq 0$ and $g_r \neq 0$. Since $\alpha^2 - \beta^2 f \in K^*$, it follows that $m = r + s$ and

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

Consider $\beta\sqrt{f}$ the Laurent expansion

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

where $h_i = \sum_{j+t=i} g_j d_t \in K$ and $h_m \neq 0$. Since $f_m + h_m$ and $f_m - h_m$ do not vanish simultaneously, it follows that the equalities $|\alpha + \beta\sqrt{f}|_\infty = |\alpha - \beta\sqrt{f}|_\infty = 0$ cannot hold simultaneously either. For definiteness, suppose that $|\alpha + \beta\sqrt{f}|_\infty > 0$ and $|\alpha - \beta\sqrt{f}|_\infty < 0$. Then, we have

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

Moreover, (3) implies that $|\alpha + \beta\sqrt{f}|_\infty = m$ and $|\alpha - \beta\sqrt{f}|_\infty = -m$. Therefore,

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

This gives the system of equations

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

Let $\mathbf{g} = (g_0, g_1, \ldots, g_r)^t$. Then, (5) can be written in the matrix form

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

Thus, the homogeneous system of linear equations (6) with matrix H_{r+1} has a nonzero solution $\mathbf{g}$, and the rank of the matrix H_{r+1} is less than $r + 1$.

Conversely, suppose that the rank of the matrix H_{r+1} is less than $r + 1$. Then, the homogeneous system of linear equations (6) has a nonzero solution $\mathbf{g}$, and $g_r \neq 0$ for this solution. Let us calculate the coefficients of the polynomial f by formulas (4). By construction, we have $|\alpha + \beta\sqrt{f}|_\infty = m$ and $|\alpha - \beta\sqrt{f}|_\infty = -m$. Therefore,

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

Since $\alpha^2 - \beta^2 f \in K[x]$, it follows that $\alpha^2 - \beta^2 f \in K^*$, and hence, $u = \alpha + \beta\sqrt{f}$ is a nontrivial unit of the ring D_f. By construction, $\deg\beta = r$; thus, $\deg u = r + s$.

Note that, to obtain the fundamental unit of the ring D_f, it suffices to find the least positive integer r for which the rank of the matrix H_r is less than r.

In what follows, we again assume that K is a field of algebraic numbers. Let us derive Theorem 1 from Theorem 2.

Suppose that $u = \alpha + \beta\sqrt{f}$ is a nontrivial unit in D_f. Let S denote the set of valuations $v \in V^K$ such that all coefficients of the polynomials $f(x)$, $\alpha(x)$, and $\beta(x)$ belong to $\mathbf{O}_v$, the polynomial $f_v(x)$ is square-free, and the characteristic of the field k_v is different from 2. Clearly, the set $V^K \setminus S$ is finite. Since $\alpha^2 - \beta^2 f \in K^*$, it follows that $\alpha_v^2 - \beta_v^2 f_v \in k_v^*$ for any $v \in S$. This means that the element $u'_v = \alpha_v + \beta_v\sqrt{f_v}$ is a unit of the ring D_{f_v}. Clearly, $\deg u'_v \leq \deg u$. The fundamental unit u_v of the ring D_{f_v} satisfies the relations $\deg(u_v) \leq \deg(u'_v) \leq \deg(u)$; thus, for the constant C we can take $\deg(u)$.

Let us prove the converse. Suppose that $\deg u_v < C$ for all $v \in S$. Take an arbitrary $v \in S$. Let $\overline{k_v(x)}$ be the completion of the field $k_v(x)$ with respect to the infinite valuation $|\cdot|_\infty$. Since $\sqrt{f_v} \in \overline{k_v(x)}$, we can expand $\sqrt{f_v}$ in a Laurent series as

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

where the coefficients $(d_i)_v$ are the reductions of the coefficients d_i in decomposition (1) modulo $\mathbf{p}_v$. Let $H_{r,v}$ denote the matrix obtained from the matrix H_r by reducing its elements modulo $\mathbf{p}_v$. Since the ring D_{f_v} has the nontrivial fundamental unit u_v, Theorem 2 implies the existence of a positive integer $r = r(v)$ for which the rank of the matrix $H_{r,v}$ is less than r. This means that all minors of order r in the matrix $H_{r,v}$ vanish. Moreover, we have $\deg(u_v) = r(v) + s - 1$. Using the assumptions of the theorem, we obtain $r(v) \leq C - s + 1$.

Since the set S infinite, it contains an infinite subset $S_1 \subset S$ such that $r(v_1) = r(v_2)$ for any $v_1, v_2 \in S_1$. Let $v \in S_1$. Consider any minor T of order r in the matrix H_r and the corresponding minor T_v in the matrix $H_{r,v}$. Clearly, T_v is obtained from T by reduction modulo $\mathbf{p}_v$. As mentioned above, $T_v = 0$ for all $v \in S_1$. By virtue of the infinity of S_1, this implies $T = 0$. Thus, all minors of order r in the matrix H_r vanish. Therefore, the rank of this matrix is less than r, and Theorem 2 implies the existence of a nontrivial unit in the ring D_f. This completes the proof of Theorem 2.

An algorithmic solution of the problem of the existence of nontrivial units in the ring D_f for polynomials f with $\deg f \leq 4$ was obtained in [1] by reducing the problem under consideration to the problem of torsion in elliptic curves. For the case $K = \mathbb{Q}$, an important observation was made in [1]: the degree of the fundamental unit is at most 12 and cannot equal 11. This opens a way to a fast direct calculation of nontrivial

units. In the case of $\deg f = 4$, the matrix H_r defined by (2) is Hankel, and the condition $\operatorname{rank} H_r < r$ is equivalent to $\det H_r = 0$.

In [1], a question of F. Grunewald was answered; namely, it was proved that the ring D_f for the polynomial $f(x) = x^4 + x + 1$ contains no nontrivial units. Moreover, it was mentioned in [1] that if $f(x) = x^4 + c$ or $f(x) = x^4 + x$, then the corresponding ring D_f has nontrivial units.

Using the methods developed in this paper, we can give a complete answer to the question of for what polynomials $f(x) = x^4 + bx + c$ the ring D_f has nontrivial units.

Theorem 3. *For a polynomial of the form $f(x) = x^4 + bx + c$, the ring D_f has a fundamental unit of degree n at the following n, b, and c:*

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

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

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

Proof. The Laurent expansion of $\sqrt{f}$ has the form

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

where the coefficients d_{-i} of x^{-i} are calculated by the recursive formulas

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

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

By Theorem 2, the ring D_f has a nontrivial unit u of degree $r + 1$ if and only if $\det H_r = 0$.

For $r = 1$, we have $\det H_r = \dfrac{b}{2} = 0$; therefore, $f(x) = x^4 + c$. This case was considered in [1]. Obviously, the element $u = x^2 + \sqrt{f}$ is the fundamental unit of the ring D_f.

For $r = 2$, we have $\det H_r = -\dfrac{c^2}{4} = 0$. Therefore, $f(x) = x^4 + bx$. In this case, the fundamental unit of the ring D_f has the form $u = x^3 + \dfrac{b}{2} + x\sqrt{f}$.

For $r = 3$, we have $\det H_r = \dfrac{1}{128}b(-b^4 + 9c^3) = 0$. The case $b = 0$ was considered above. It is easy to show that the equation $-b^4 + 8c^3 = 0$ has the rational solutions $b = t^3$, $c = \dfrac{t^4}{2}$, where $t \in \mathbb{Q}^*$. The fundamental unit of the ring D_f has the form

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

Note that, for any $t \in \mathbb{Q}^*$, the elliptic curve $y^2 = f(x)$ is biregularly isomorphic to the curve $y_1^2 = f_1(x)$, where $f_1(x) = x_1^4 + x_1 + \dfrac{1}{2}$. The corresponding morphism is determined by $x = tx_1$, $y = t^2y_1$.

For $r = 4$, we have

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

Making the change of variables $z = \dfrac{c^3}{b^4}$, we can rewrite Eq. (7) in the form

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

Since the polynomial $h_r(z)$ in (8) has no rational roots, it follows that Eq. (7) has no rational solutions b, c. Thus, there exist no polynomials $f(x)$ for which the ring D_f has a fundamental unit of degree $n = r + 1 = 5$.

A similar calculation shows that, for $r = 5, 6, 7, 8, 9, 11$, the element $z = \dfrac{c^3}{b^4}$ is a root of the corresponding polynomial $h_r(z)$, which is defined for these r by

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

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

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

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

$$h_9(z) = 20480z^6 - 73728z^5 + 35584z^4 - 7040z^3 + 720z^2 - 40z + 1,$$

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

The polynomials $h_r(z)$ with $r \geq 5$ are irreducible over $\mathbb{Q}$, and therefore, they have no rational roots. Hence, there exists no polynomial $f(x) = x^4 + bx + c$ for which the ring D_f has a fundamental unit of degree $n \geq 5$. This completes the proof of Theorem 3.

In the proof of Theorem 3, the calculation of the determinants $\det H_r$, the factorization of polynomials, and the proof of the irreducibility over $\mathbb{Q}$ of the polynomials $h_r(z)$ with $r \geq 5$ were performed by using the Maple computer algebra system.

ACKNOWLEDGMENTS

This work was supported by the Russian Foundation for Basic Research (project nos. 09-01-00287 and 09-01-12169).

REFERENCES

1. V. P. Platonov, Dokl. Akad. Nauk **430**, 318–320 (2010) [Dokl. Math. **81**, 55–57 (2010)].
2. V. V. Benyash-Krivets and V. P. Platonov, Dokl. Akad. Nauk **417**, 446–450 (2007) [Dokl. Math. **76**, 886–890 (2007)].
3. V. V. Benyash-Krivets and V. P. Platonov, Dokl. Akad. Nauk **423**, 155–160 (2008) [Dokl. Math. **78**, 833–838 (2008)].
4. V. V. Benyash-Krivets and V. P. Platonov, Mat. Sb. **200** (11), 15–44 (2009).