ISSN 1064–5624, Doklady Mathematics, 2007, Vol. 76, No. 3, pp. 886–890. © Pleiades Publishing, Ltd., 2007.
Original Russian Text © V.V. Benyash-Krivets, V.P. Platonov, 2007, published in Doklady Akademii Nauk, 2007, Vol. 417, No. 4, pp. 446–450.

MATHEMATICS

Groups of *S*-units in Hyperelliptic Fields

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

Received August 1, 2007

DOI: 10.1134/S106456240706021X

In this paper, we calculate groups of S-units in hyperelliptic fields.

Let $k = F_q(x)$ be the field of rational functions of one variable over a finite field F_q of characteristic $p > 2$, and let

$$d(x) = a_0x^{2n+1} + a_1x^{2n} + \ldots + a_{2n+1}$$

be a square-free polynomial with $a_0 \neq 0$. Consider $K = k(\sqrt{d})$. For an irreducible polynomial $v \in F_q[x]$, by $|\cdot|_v$ we denote the corresponding valuation on k, by $O_v = \{z \in k \mid |z|_v \geq 0\}$ the ring of the valuation $|\cdot|_v$, and by $p_v = \{z \in k \mid |z|_v > 0\}$ the ideal of the valuation $|\cdot|_v$. The residue field $k_v = O_v/p_v$ coincides with $F_p[x]/(v)$ and is a finite extension of F_p. Let $\bar{x}$ be the image of x in residue field k_v. If $d(\bar{x}) = \beta^2$ for some $0 \neq \beta \in k_v$ (this means that $(\beta, \bar{x})$ is a k_v-point of the hyperelliptic curve $y^2 = d(x)$), then the valuation $|\cdot|_v$ admits two nonequivalent extensions to the field K. We denote these valuations by $|\cdot|_{v'}$ and $|\cdot|_{v''}$. Otherwise, the valuation $|\cdot|_v$ has a unique extension to the field K, which we denote by the same symbol $|\cdot|_v$. The non-Archimedean valuation $|\cdot|_\infty$ admits a unique extension to K; we denote it by $|\cdot|_\infty$.

Let S be an arbitrary finite set of nonequivalent valuations of the field K containing $|\cdot|_\infty$, and let $S_1 = \{|\cdot|_\infty, |\cdot|_{v_1}, \ldots, |\cdot|_{v_t}\}$ be the set of restrictions of valuations from S to the field k. We use O_S to denote the ring of S-integer elements in K, i.e., of all $z \in K$ such that $|z|_v \geq 0$ for all valuations $|\cdot|_v$ of K not belonging to S. The set U_S of invertible elements of the ring O_S is called the group of S-units of the field K. By virtue of the generalized Dirichlet theorem about units (see [1, Chapter IV, Theorem 9]), the group U_S is the direct product of the group F_q^* and the free Abelian group G of rank $|S| - 1$. Independent generators of the group G are called fundamental S-units.

In the classical case of the quadratic extension $L = Q(\sqrt{d})$ of the field Q, a fundamental unit of the field L can be found by expanding $\sqrt{d}$ into a continued fraction [2]. However, for functional fields, the method of continued fractions does not always yield a fundamental unit. The purpose of this paper is to construct an algorithm for calculating fundamental S-units of a hyperelliptic field K.

The first proposition is of technical character.

Proposition 1. *Let $y = f + g\sqrt{d}$, where $f, g \in F_q[x]$; $f \neq 0$; $g \neq 0$; and $(f, g) = 1$, and let $v \in F_q[x]$ be an irreducible polynomial.*

Then, the following assertions hold.

(i) *If $|\cdot|_v$ admits two extensions $|\cdot|_{v'}$ and $|\cdot|_{v''}$ to K, then either $|y|_{v'} = 0$ or $|y|_{v''} = 0$.*

(ii) *If $v \nmid d$ and $|\cdot|_v$ admits a unique extension $|\cdot|_v$ to K, then $|y|_v = 0$.*

(iii) *If $v \mid d$ and $v \nmid f$, then $|\cdot|_v$ admits a unique extension to K, and $|y|_v = 0$.*

(iv) *If $v \mid d$ and $v \mid f$, then $|\cdot|_v$ admits a unique extension to K, and $|y|_v = \frac{1}{2}$.*

The following proposition characterizes S-integer elements in K.

Proposition 2. *Any element $y \in O_S$ has the form*

$$y = \frac{f + g\sqrt{d}}{v_1^{m_1} v_2^{m_2} \ldots v_t^{m_t}},$$

where $f, g \in F_q[x]$ and $m_i \geq 0$. If some m_i is positive, then $v_i \nmid f$ and $v_i \nmid g$.

[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

To prove Proposition 2, it suffices to note that if the denominator of y is divisible by an irreducible polynomial $v \neq v_i$, where $i = 1, 2, \ldots, t$, then, by Proposition 1, we have $|y|_{v'} < 0$ for some extension $|\cdot|_{v'}$ of the valuation $|\cdot|_v$.

Note that not every element of the form $y = \dfrac{f + g\sqrt{d}}{v_1^{m_1} v_2^{m_2} \ldots v_t^{m_t}}$ is an S-integer. For what follows, it is important to know what values a valuation mapping can take at S-units.

Proposition 3. *If* $\varepsilon \in U_s$ *and* $\varepsilon \notin F_q^*$, *then*

$$N_{K/k}(\varepsilon) = a v_1^{m_1} v_2^{m_2} \ldots v_t^{m_t},$$

where $a \in F_q^*$, $m_i \in \mathbf{Z}$, *and* $m_1, m_2, \ldots, m_t$ *are not all zero.*

As in the case of S-integer elements, an element $\varepsilon \in K$ satisfying the condition $N_{K/k}(\varepsilon) = a v_1^{m_1} v_2^{m_2} \ldots v_t^{m_t}$ is not necessarily an S-unit.

If $\varepsilon = \dfrac{f + g\sqrt{d}}{v_1^{m_1} v_2^{m_2} \ldots v_t^{m_t}} \in U_S \backslash F_q^*$, then it follows from Proposition 3 that

$$f^2 - g^2 d = a v_1^{k_1} v_2^{k_2} \ldots v_t^{k_t}, \qquad (1)$$

where $k_1, k_2, \ldots, k_t$ are nonnegative integers. The following proposition shows that if the valuation equation (1) with fixed $k_1, k_2, \ldots, k_t$ has a solution in polynomials f, $g \in F_q[x]$, then we can easily construct an S-unit.

Proposition 4. *Suppose that* $z = f + g\sqrt{d} \in K$, *where* $f, g \in F_q[x]$, *and*

$$N_{K/k}(z) = f^2 - g^2 d = a v_1^{m_1} v_2^{m_2} \ldots v_t^{m_t},$$

where $a \in F_q^*$, $m_i \in \mathbf{Z}$, *and* $m_1, m_2, \ldots, m_t$ *are not all zero. Let* $S_2 = \{|\cdot|_{v_1}, |\cdot|_{v_2}, \ldots, |\cdot|_{v_r}\}$ *be the set of those valuations* $|\cdot|_{v_i}$ *from* S_1 *for which the following conditions hold*: (i) $|\cdot|_{v_i}$ *admits two extensions* $|\cdot|_{v_i'}$ *and* $|\cdot|_{v_i''}$ *to* K; (ii) $|\cdot|_{v_i''} \notin S$; (iii) $|z|_{v_i''} > 0$.

Then, $\dfrac{z}{v_1^{m_1} v_2^{m_2} \ldots v_r^{m_r}} \in U_S$.

Now, consider the natural question of how a system of independent fundamental S-units expands when the set S is augmented with a new valuation $|\cdot|_v$. It is answered by the following theorem.

Theorem 1. *Suppose that* $f = |S| - 1$, $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_f$ *are independent fundamental S-units of the field K and* $v \in F_q[x]$ *is an irreducible polynomial.*

Then, the following assertions hold.

(i) *Suppose that the valuation* $|\cdot|_v$ *admits two extensions* $|\cdot|_{v'}$ *and* $|\cdot|_{v''}$ to K *and, moreover,* $|\cdot|_{v'} \in S$ *and* $|\cdot|_{v''} \notin S$. *Let* $S' = S \cup \{|\cdot|_{v''}\}$. *Then,* $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_f$, v *form a system of independent fundamental S'-units.*

(ii) *Suppose that the valuation* $|\cdot|_v$ *admits two extensions* $|\cdot|_{v'}$ *and* $|\cdot|_{v''}$ *to K and, moreover,* $|\cdot|_{v'} \notin S$ *and* $|\cdot|_{v''} \notin S$. *Let* $S' = S \cup \{|\cdot|_{v''}\}$, *and let* ε_{f+1} *be an S'-unit for which*

$$N_{K/k}(\varepsilon_{f+1}) = a v_1^{m_1} v_2^{m_2} \ldots v_f^{m_f} v_{f+1}^{m_{f+1}},$$

where m_{f+1} *is the minimum possible positive integer exponent. Then,* $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_f, \varepsilon_{f+1}$ *form a system of independent fundamental S'-units.*

(iii) *Let* $v \mid d$. *Then, the valuation* $|\cdot|_v$ admits a *unique extension to K. Suppose that* $|\cdot|_v \notin S$ *and* $S' = S \cup \{|\cdot|_v\}$. *If* $\dfrac{d}{v} \notin F_q$, *then* $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_f$, v *form a system of independent fundamental S'-units. If* $\dfrac{d}{v} \in F_q$, *then* $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_f$, $\sqrt{d}$ *form a system of independent fundamental S'-units.*

It follows from Theorem 1 that the key case in finding a system of independent fundamental S-units is as follows. Let $v_1, v_2, \ldots, v_t \in F_q[x]$ be irreducible polynomials such that each valuation $|\cdot|_{v_i}$ admits two extensions $|\cdot|_{v_i'}$ and $|\cdot|_{v_i''}$ to K. We set $S = \{|\cdot|_\infty, |\cdot|_{v_1'}, \ldots, |\cdot|_{v_t'}\}$, i.e., include precisely one of the two extensions of $|\cdot|_{v_i}$ to K in S.

First, consider the minimal case, in which $S = \{|\cdot|_\infty, |\cdot|_{v'}\}$. If $\varepsilon \in U_S$, then, by Proposition 3, we have $N_{K/k}(\varepsilon) = a v^m$. Therefore, to calculate a fundamental S-unit, we must find the minimum positive integer m for which the valuation equation

$$f^2 - g^2 d = a v^m, \qquad (2)$$

where $a \in F_q^*$, has a solution in polynomials f, $g \in F_q[x]$. By virtue of Proposition 4, either $f + g\sqrt{d}$ or $f - g\sqrt{d}$ is a fundamental S-unit.

The most complete result is obtained when $v = x - a$ is a first-degree polynomial. Let $\bar{k}_v$ be the completion of k with respect to the valuation $|\cdot|_v$. The field $\bar{k}_v$ can be identified with the field $F_q((v))$ of formal power series. Since $|\cdot|_v$ admits two extension to K, it follows that $\sqrt{d} \in F_q((v))$. The following theorem provides an algorithm for finding fundamental S-units.

Theorem 2. *Suppose that* $\sqrt{d} = \sum_{i=0}^{\infty} d_i v^i \in F_q((v))$, $n = \frac{\deg d - 1}{2}$, *$r \geq n$ is an integer, and*

$$D_r = \begin{pmatrix} d_{n+1} & d_{n+2} & \dots & d_{r+1} \\ d_{n+2} & d_{n+3} & \dots & d_{r+2} \\ & & \ddots & \\ d_{n+r} & d_{n+r+1} & \dots & d_{2r} \end{pmatrix}$$

and

$$H_r = \begin{pmatrix} d_{n+2} & d_{n+3} & \dots & d_{r+2} \\ d_{n+3} & d_{n+4} & \dots & d_{r+3} \\ & & \ddots & \\ d_{n+r+1} & d_{n+r+2} & \dots & d_{2r+1} \end{pmatrix}$$

are matrices. Then, the valuation equation (2) *with odd* $m = 2r + 1$ *has a solution in polynomials* $f, g \in F_q[x]$ *if and only if* $r \geq n$ *and* $\operatorname{rank} D_r < r - n + 1$, *and the valuation equation* (2) *with even* $m = 2r$ *has such a solution if and only if* $r \geq n + 1$ *and* $\operatorname{rank} H_{r-1} < r - n$.

Proof. Suppose that $m = 2r + 1$ (the case of even m is considered similarly). Let $f, g \in F_q[x]$ be a solution to (2). Then, $\deg f \leq r$ and $\deg g = r - n$. Expanding f and g in powers of v, we obtain

$$f = f_0 + f_1 v + \dots + f_r v^r,$$
$$g = g_0 + g_1 v + \dots + g_{r-n} v^{r-n},$$

where $f_i, g_j \in F_q$. Thus,

$$g\sqrt{d} = \sum_{i=0}^{\infty} P_i v^i,$$

where $P_i = \sum_{j=0}^{i} g_j d_{i-j}$ (we assume that $g_j = 0$ for $j > r - n$). The valuation equation (2) is equivalent to $f + g\sqrt{d} = \sum_{i=m}^{\infty} P_i v^i$, which gives the following systems of linear equations for the coefficients f_i and g_j:

$$f_i = -P_i, \quad i = 0, 1, \dots, r-1, \tag{3}$$

$$P_j = 0, \quad j = r, r+1, \dots, m-1. \tag{4}$$

Setting $G = (g_{r-n}, g_{r-n-1}, \dots, g_0)^t$, we can rewrite (4) in the matrix form

$$D_r G = 0. \tag{5}$$

Since the homogeneous system (5) of linear equations with matrix D_r has a nonzero solution G, it follows that $\operatorname{rank} D_r < r - n + 1$.

Conversely, if $\operatorname{rank} D_r < r - n + 1$, then (5) has a nonzero solution G. Formulas (3) give the coefficients f_i; thus, we obtain polynomials f and g such that $v^m \mid f^2 - g^2 d$. By construction, $\deg(f^2 - g^2 d) \leq \deg v^m$ and, obviously, $f^2 - g^2 d \neq 0$; hence, $f^2 - g^2 d = a v^m$, where $a \in F_q^*$.

Thus, to find a fundamental S-unit of the field K, we expand $\sqrt{d}$ in a power series in the field $k_v((v))$. Then, successively calculating the ranks of the matrices D_r and H_r, we find a minimum positive integer r for which either $\operatorname{rank} D_r < r - n + 1$ or $\operatorname{rank} H_{r-1} < r - n$. After that, solving the homogeneous system of linear equations (5), we obtain a nonzero polynomial g, and formulas (3) give a polynomial f. The required fundamental S-unit has the form $f + g\sqrt{d}$.

If K is the function field of an elliptic curve, i.e., $\deg d = 3$, then the matrices D_r and H_r are square, and Theorem 2 acquires the following form.

Corollary. *Suppose that* $\deg d = 3$. *Then, the valuation equation* (2) *with odd* $m = 2r + 1$ *has a solution in polynomials* $f, g \in F_q[x]$ *if and only if* $\det D_r = 0$, *and the valuation equation* (2) *with even* $m = 2r$ *has such a solution if and only if* $\det H_{r-1} = 0$.

In the case where $\deg v \geq 2$, the problem of finding a fundamental S-unit also reduces to solving a homogeneous system of linear equations. However, the matrix of this system is hard to write out explicitly. In this case, to solve the valuation equation (2), we write

$$f = f_0 + f_1 x + \dots + f_r x^r$$

and

$$g = g_0 + g_1 x + \dots + g_e x^e,$$

where $r = \left[\frac{m \deg v}{2}\right]$ and $e = \left[\frac{m \deg v - \deg d}{2}\right]$ ($[z]$ denotes the integer part of z). Since $\sqrt{d} \in \bar{k}_v$, it follows that the elements f and $g\sqrt{d}$ can be represented as the formal power series

$$f = f'_0 + f'_1 v + \dots + f'_{r'} v^{r'} \quad \text{and} \quad g\sqrt{d} = \sum_{i=0}^{\infty} L_i v^i,$$

where the coefficients f'_i and L_i are polynomials from $F_q[x]$ of degree < deg v; moreover, the coefficients of f'_i are linear forms in $f_0, f_1, \dots, f_r$ and the coefficients of L_i are linear forms in $g_0, g_1, \dots, g_e$. Let us require that $f + g\sqrt{d} = \sum_{i=m}^{\infty} L_i v^i$, i.e.,

$$f'_0 = -L_0, \quad f'_1 = -L_1, \dots, f'_{r'} = -L_{r'}, \tag{6}$$

$$L_{r'+1} = L_{r'+2} = \dots = L_{m-1} = 0. \tag{7}$$

Relations (7) give a homogeneous system of linear equations with respect to $g_0, g_1, \dots, g_e$ with some matrix A_v:

$$A_v(g_0, g_1, \dots, g_e)^t = 0. \tag{8}$$

System (8) has a nonzero solution if and only if rank$A_v \le e$. If this condition holds, then we find the polynomial g from (8) and the polynomial f from (6). By construction, $v^m \mid f^2 - g^2d$, $\deg(f^2 - g^2d) \le \deg v^m$, and, obviously, $f^2 - g^2d \ne 0$. Therefore, $f^2 - g^2d = av^m$, where $a \in F_q^*$.

Now, let $S = \{|\cdot|_\infty, |\cdot|_{v'_1}, \dots, |\cdot|_{v'_t}\}$. According to assertion 2 of Theorem 1, a system of independent fundamental S-units can be constructed by induction. Let $S_i = \{|\cdot|_\infty, |\cdot|_{v'_1}, \dots, |\cdot|_{v'_i}\}$. Using Theorem 2, we find a fundamental S_1-unit. Suppose that $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_i$ are independent fundamental S_i-units and

$$N_{K/k}(\varepsilon_j) = a_j v_1^{m_{j1}} v_2^{m_{j2}} \dots v_j^{m_{jj}}, \quad a_j \in F_q^*,$$
$$j = 1, 2, \dots, i.$$

Adding an S_{i+1}-unit ε_{i+1} with minimum possible positive integer exponent $m_{i+1,i+1}$, we obtain independent fundamental S_{i+1}-units.

Let $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_t$ be independent fundamental S-units thus constructed. Consider the valuation matrix

$$H(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_t) = \begin{pmatrix} m_{11} & 0 & \dots & 0 \\ m_{21} & m_{22} & \dots & 0 \\ & & \ddots & \\ m_{t1} & m_{t2} & \dots & m_{tt} \end{pmatrix}.$$

If $\varepsilon'_1, \varepsilon'_2, \dots, \varepsilon'_t$ for another system of independent fundamental S-units, then

$$\varepsilon'_i = \varepsilon_1^{b_{i1}} \varepsilon_2^{b_{i2}} \dots \varepsilon_t^{b_{it}}, \quad i = 1, 2, \dots, t$$

and $B = (b_{ij}) \in GL_t(\mathbf{Z})$. It is easy to see that

$$H(\varepsilon'_1, \varepsilon'_2, \dots, \varepsilon'_t) = BH(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_t).$$

Therefore, multiplying $H(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_t)$ by a suitable matrix $B \in GL_t(\mathbf{Z})$ if necessary, we can assume that $0 \le m_{ir} < m_{rr}$ for $i = r + 1, r + 2, \dots, t$. Let $T_i = \{|\cdot|_\infty, |\cdot|_{v'_i}\}$, and let δ_i be the corresponding fundamental T_i-unit. Then, $N_{K/k}(\delta_i) = b_i v_i^{m_i}$, where $b_i \in F_q^*$. Since δ_i is an S_i-unit, it follows that $\delta_i = c_i \varepsilon_1^{f_1} \varepsilon_2^{f_2} \dots \varepsilon_i^{f_i}$, where $c_i \in F_q^*$. Comparing the values of the left- and right-hand sides, we obtain $f_i m_{ii} = m_i$, i.e., $m_{ii} \mid m_i$.

Suppose that the units $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{i-1}$ are already found. To find ε_i, we must determine the minimum positive integer divisor m_{ii} of m_i and integers $0 \le m_{ij} < m_{jj}$, where $j = 1, 2, \dots, i-1$, for which the valuation equation

$$f^2 - g^2 d = a v_1^{m_{i1}} v_1^{m_{i2}} \dots v_i^{m_{ii}}, \tag{9}$$

where $a \in F_q^*$, has a solution in polynomials $f, g \in F_q[x]$. As in the case of one valuation, solving (9) reduces to solving a homogeneous system of linear equations. It follows from (9) that

$$\deg f = \left[\frac{1}{2}\sum_{j=1}^{i} m_{ij} \deg v_j\right] = l$$

and

$$\deg g = \left[\frac{1}{2}\left(\sum_{j=1}^{i} m_{ij} \deg v_j - \deg d\right)\right] = e.$$

Suppose that $f = f_0 + f_1x + \dots + f_lx^l$ and $g = g_0 + g_1x + \dots + g_ex^e$. Choose one of the valuations $|\cdot|_{v_j}$, where $1 \le j \le i$. Let us represent $f + g\sqrt{d}$ as a formal power series in v_j:

$$f + g\sqrt{d} = \sum_{s=0}^{\infty} L_s v_j^s,$$

where $L_s \in F_q[x]$ and $\deg L_s < \deg v_j$; the coefficients of the polynomial L_s are linear forms in $f_0, f_1, \dots, f_l, g_0, g_1, \dots, g_e$. We require that

$$L_0 = L_1 = \dots = L_{m_{ij}-1} = 0. \tag{10}$$

Then, (10) yields a homogeneous system of linear equations with respect to $f_0, f_1, \dots, f_l, g_0, g_1, \dots, g_e$ with matrix A_{v_j} such that

$$A_{v_j}(f_0, f_1, \dots, f_l, g_0, g_1, \dots, g_e)^t = 0. \tag{11}$$

After performing this construction for all valuations $|\cdot|_{v_j}$ with $j = 1, 2, \dots, i$, we see that $f_0, f_1, \dots, f_l, g_0, g_1, \dots, g_e$ are a solution to the homogeneous system of linear equations

$$A(f_0, f_1, \dots, f_l, g_0, g_1, \dots, g_e)^t = 0, \tag{12}$$

where A is a block matrix of the form $A = (A_{v_1}, A_{v_2}, \dots, A_{v_i})^t$.

Conversely, if $f_0, f_1, \dots, f_l, g_0, g_1, \dots, g_e$ are a solution to (12) and not all of the g_j vanish, then the nonzero polynomial $f^2 - g^2d$ is divisible by the product $v_1^{m_{i1}} v_2^{m_{i2}} \dots v_i^{m_{ii}}$. By construction, we have $\deg f^2 - g^2d \le \deg v_1^{m_{i1}} v_2^{m_{i2}} \dots v_i^{m_{ii}}$; therefore, $f^2 - g^2d = a v_1^{m_{i1}} v_2^{m_{i2}} \dots v_i^{m_{ii}}$, where $a \in F_q^*$. Thus, we have proved the following theorem.

Theorem 3. *The valuation equation* (9) *has a solution in nonzero polynomials* $f, g \in F_q[x]$ *if and only if the homogeneous system of linear equations* (12) *has a solution* $f_0, f_1, \dots, f_l, g_0, g_1, \dots, g_e$ *in which not all of the* g_j *vanish.*

REFERENCES

1. A. Weil, *Basic Number Theory* (Springer-Verlag, Heidelberg, 1967; Mir, Moscow, 1972).
2. Z. I. Borevich and I. R. Shafarevich, *Number Theory* (Nauka, Moscow, 1964) [in Russian].