Sbornik: *Mathematics* **200**:11 1587–1615 © 2009 RAS(DoM) and LMS

Matematicheskiĭ Sbornik **200**:11 15–44 DOI 10.1070/SM2009v200n11ABEH004052

Groups of S-units in hyperelliptic fields and continued fractions

V. V. Benyash-Krivets and V. P. Platonov

Abstract. New methods for calculating fundamental S-units in hyperelliptic fields are found. Continued fractions in function fields are investigated. As an application, it is proved that if a valuation is defined by a linear polynomial, then a fundamental S-unit in a hyperelliptic field can be found by expanding certain elements into continued fractions.

Bibliography: 11 titles.

Keywords: S-units, valuations, hyperelliptic fields, continued fractions, best approximations.

§ 1. Introduction

In [1]–[4] several results were presented related to solving the problem of calculating the groups of S-units in hyperelliptic fields, developing the theory of continued fractions in function fields, and their connections with the calculation of fundamental S-units. The present paper contains an extended exposition of the results announced in [1]–[4].

Two new methods for calculating fundamental S-units in hyperelliptic fields are proposed. The first method is based on a new effective procedure of linearization of the search for solutions of the natural norm equation. In the elliptic case, which is important for applications, where the valuations in S are induced by points on an elliptic curve, a new interesting connection with Hankel matrices is discovered.

The second method is of a different nature. First we obtain some results on continued fractions in function fields, which are of a certain independent interest, and then we apply them for solving the norm equation. In the case where the valuations in S are defined by linear polynomials, the method of continued fractions gives the fastest algorithms for calculating fundamental S-units. However, in contrast to the first method, the method of continued fractions loses its effectiveness in the case where S contains valuations of a more general nature.

Let $k = \mathbb{F}_q(x)$ be the field of rational functions in one variable over a finite field $\mathbb{F}_q$ of characteristic $p > 2$. For an irreducible polynomial $v \in \mathbb{F}_q[x]$, we denote by $|\cdot|_v$ the valuation of the field k given by the equation

$$\left| v^m \frac{a}{b} \right|_v = m,$$

This research was carried out with the financial support of the Russian Foundation for Basic Research (grant nos. 09-01-00287 and 09-01-12169).

AMS 2000 *Mathematics Subject Classification.* Primary 11R58; Secondary 11A55, 11R27.

where $a,b \in \mathbb{F}_q[x]$, $v \nmid a$, $v \nmid b$. We denote by $|\cdot|_\infty$ the valuation $|a/b|_\infty = \deg b - \deg a$.

We denote by $\mathscr{O}_v = \bigl\{z \in k \bigm| |z|_v \geqslant 0\bigr\}$ the valuation ring of $|\cdot|_v$, and by $\mathfrak{p}_v = \bigl\{z \in k \bigm| |z|_v > 0\bigr\}$ the valuation ideal of $|\cdot|_v$. Then the residue field $k_v = \mathscr{O}_v/\mathfrak{p}_v$ coincides with $\mathbb{F}_p[x]/(v)$ and is a finite extension of $\mathbb{F}_p$. Let $\overline{k}$ be the completion of the field k with respect to the valuation $|\cdot|_v$. We denote the extension of the valuation $|\cdot|_v$ to $\overline{k}$ as before by $|\cdot|_v$. We choose in $\mathbb{F}_q[x]$ a fixed system Σ of representatives of cosets of the ideal (v) consisting of all the polynomials of degree less than $\deg v$. Then each element $z \in \overline{k}$ can be uniquely represented as a formal power series:

$$z = \sum_{i=s}^{\infty} a_i v^i,$$

where $a_i \in \Sigma$. If $\deg v = 1$, then the field $\overline{k}$ can be identified with the field of formal power series $\mathbb{F}_q((v))$.

Let

$$d(x) = a_0 x^{2n+1} + a_1 x^{2n} + \dots + a_{2n+1} \in \mathbb{F}_q[x]$$

be a square-free polynomial with $a_0 \neq 0$, let $K = k(\sqrt{d})$, and let $\overline{x}$ be the image of x in the residue field k_v. If $d(\overline{x}) = \beta^2$ for some $0 \neq \beta \in k_v$ (and this means that the point $(\overline{x}, \beta)$ is a k_v-point of the hyperelliptic curve $y^2 = d(x)$), then the valuation $|\cdot|_v$ has two non-equivalent extensions to the field K. We denote these valuations by $|\cdot|_{v'}$ and $|\cdot|_{v''}$. Note that in this case $v \nmid d$, $\sqrt{d} \in \overline{k}$, and $|f + g\sqrt{d}|_{v'} = |f - g\sqrt{d}|_{v''}$ for an element $f + g\sqrt{d} \in K$. But if $d(\overline{x}) = 0$ or $d(\overline{x}) \neq 0$ and $d(\overline{x})$ is not a square in k_v, then the valuation $|\cdot|_v$ has a unique extension to the field K. In order not to complicate the notation, we denote this extension by $|\cdot|_v$, as before. In this case we have $|f + g\sqrt{d}|_v = (1/2)|f^2 - g^2 d|_v$ for an element $f + g\sqrt{d} \in K$. Since the polynomial $d(x)$ has odd degree, the valuation $|\cdot|_\infty$ has a unique extension to K, and we also denote it by $|\cdot|_\infty$.

Let S be an arbitrary finite set of non-equivalent valuations of the field K containing $|\cdot|_\infty$, and $S_1 = \{|\cdot|_\infty, |\cdot|_{v_1}, \dots, |\cdot|_{v_t}\}$ the set of restrictions of valuations in S to the field k. We denote by $\mathscr{O}_S$ the ring of S-integer elements in K, that is, elements $z \in K$ such that $|z|_v \geqslant 0$ for all the valuations $|\cdot|_v$ of the field K that do not belong to the set S. The set of invertible elements U_S of the ring $\mathscr{O}_S$ is called the *group of S-units of the field K*. By the generalized Dirichlet unit theorem (see [5], Ch. IV, Theorem 9), the group U_S is the direct product of the group $\mathbb{F}_q^*$ and a free Abelian group G of rank $|S| - 1$. Independent generators of the group G are called *fundamental S-units*.

§ 2. Some properties of S-units

Let S be an arbitrary finite set of non-equivalent valuations of the field K containing $|\cdot|_\infty$, let $s = |S| - 1$, and let $S_1 = \{|\cdot|_\infty, |\cdot|_{v_1}, \dots, |\cdot|_{v_t}\}$ be the set of restrictions of valuations in S to the field k.

Proposition 2.1. *Let $y = f + g\sqrt{d}$, where $f, g \in \mathbb{F}_q[x]$, $f \neq 0$, $g \neq 0$, $(f,g) = 1$, and let $v \in \mathbb{F}_q[x]$ be an irreducible polynomial. Then the following assertions hold.*

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

2. *If* $v \nmid d$ *and* $|\cdot|_v$ *has a unique extension to* K, *then* $|y|_v = 0$.

3. *If* $v \mid d$, *then* $|\cdot|_v$ *has a unique extension to* K. *In this case, if* $v \nmid f$, *then* $|y|_v = 0$. *If* $v \mid f$, *then* $|y|_v = 1/2$.

Proof. 1. Since $|\cdot|_v$ has two extensions to K, we have $v \nmid d$ and $\sqrt{d} \in \overline{k}$. Let the elements f, g, and $\sqrt{d}$ be represented in the completion $\overline{k}$ as formal power series:

$$f = \sum_{i=0}^{r} f_i v^i, \qquad g = \sum_{i=0}^{s} g_i v^i, \qquad \sqrt{d} = \sum_{i=0}^{\infty} d_i v^i, \tag{2.1}$$

where $f_i, g_i, d_i \in \Sigma$. Suppose that $|y|_{v'} > 0$ and $|y|_{v''} > 0$. Since $|f + g\sqrt{d}|_{v''} = |f - g\sqrt{d}|_{v'}$, we obtain

$$|f + g\sqrt{d}|_{v'} > 0, \qquad |f - g\sqrt{d}|_{v'} > 0. \tag{2.2}$$

We observe that

$$f + g\sqrt{d} = \sum_{i=0}^{\infty} h_i v^i, \qquad f - g\sqrt{d} = \sum_{i=0}^{\infty} t_i v^i,$$

where $h_i, t_i \in \Sigma$ and h_0, t_0 are the remainders after division of $f_0+g_0d_0$ and $f_0-g_0d_0$ by v. It follows from inequalities (2.2) that $h_0 = t_0 = 0$. Therefore v divides f_0. Since $\deg f_0 < \deg v$, it follows that $f_0 = 0$. We now obtain that v divides g_0d_0. Since $v \nmid d$, it follows that $d_0 \neq 0$ and v does not divide d_0. Therefore v divides g_0, whence $g_0 = 0$. Thus, $v \mid f$ and $v \mid g$, which contradicts the fact that f and g are coprime.

2. Let $d = \sum_{i=0}^{m} h_i v^i$, where $h_i \in \Sigma$ and $h_0 \neq 0$ by hypothesis. Since $|\cdot|_v$ has a unique extension to K, the image of h_0 in the residue field k_v is not a square. Then

$$|y|_v = \frac{1}{2}|f^2 - g^2 d|_v.$$

Let the elements f, g, $\sqrt{d}$ be represented in the completion $\overline{k}$ in the form of the formal power series (2.1). We write

$$f^2 - g^2 d = \sum_{i=0}^{m} q_i v^i,$$

where $q_i \in \Sigma$ and q_0 is the remainder after division of $f_0^2 - g_0^2 h_0$ by v. We observe that $q_0 \neq 0$, since otherwise h_0 would be a square in the residue field k_v. Thus, v does not divide $f^2 - g^2 d$ and $|y|_v = 0$.

3. Since $v \mid d$ and d is a square-free polynomial, it follows that $|\cdot|_v$ has a unique extension to K. Then

$$|y|_v = \frac{1}{2}|f^2 - g^2 d|_v.$$

If v does not divide f, then v does not divide $f^2 - g^2 d$ and, consequently, $|y|_v = 0$.

Now suppose that $f = vf_1$ and $d = vd_1$. Then v does not divide d_1 and by hypothesis v does not divide g. Then

$$|y|_v = \frac{1}{2}|f^2 - g^2 d|_v = \frac{1}{2}|v(f_1^2 v - g^2 d_1)|_v = \frac{1}{2},$$

since v does not divide $f_1^2 v - g^2 d_1$.

Proposition 2.1 is proved.

The following proposition characterizes the S-integer elements in K.

Proposition 2.2. *Any element $y \in \mathscr{O}_S$ has the form*

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

where $f, g \in \mathbb{F}_q[x]$, $v_j \in S_1$, and $m_j \geqslant 0$. Furthermore, if $m_j > 0$ and the valuation $|\cdot|_{v_j}$ has two extensions to K one of which does not belong to S, then v_j does not divide f and v_j does not divide g.

Proof. Let $y = (f + g\sqrt{d})/h$, where $f, g, h \in \mathbb{F}_q[x]$. Suppose that $h = v^r h_1$, where v is an irreducible polynomial that does not belong to S_1 and $r > 0$. We can assume without loss of generality that v does not divide both f and g. By Proposition 2.1,

$$|y|_{v'} = |f + g\sqrt{d}|_{v'} - r < 0$$

for some extension $|\cdot|_{v'}$ of the valuation $|\cdot|_v$. Consequently, $h \notin \mathscr{O}_S$.

Now suppose that $m_j > 0$ and the valuation $|\cdot|_{v_j}$ has two extensions $|\cdot|_{v_j'}$ and $|\cdot|_{v_j''}$ to K of which $|\cdot|_{v_j'}$ does not belong to S. Then $v_j \nmid d$. We can assume without loss of generality that v_j does not divide both f and g (otherwise the numerator and denominator can be divided by v_j). Suppose that $v_j \mid f$ and $v_j \nmid g$. Then v_j does not divide $f^2 - g^2 d$. Consequently,

$$0 = |f^2 - g^2 d|_{v_j} = |f^2 - g^2 d|_{v_j'} = |f + g\sqrt{d}|_{v_j'} + |f - g\sqrt{d}|_{v_j'},$$

whence $|f + g\sqrt{d}|_{v_j'} = 0$. Thus, $|y|_{v_j'} = -m_j < 0$; a contradiction with the fact that $y \in \mathscr{O}_S$.

Proposition 2.2 is proved.

We point out that not every element of the form $y = (f + g\sqrt{d})/(v_1^{m_1} \cdots v_t^{m_t})$ is an S-integer. For example, if the valuation $|\cdot|_{v_j} \in S_1$ has two extensions to K and $|\cdot|_{v_j'}$ does not belong to S, then the element $1/v_j$ is not an S-integer.

We denote by $N_{K/k}$ the norm map from K into k. For what follows it is important for us to know which values the norm map can take on S-units.

Proposition 2.3. *If $\varepsilon \in U_S$, then $N_{K/k}(\varepsilon) = a v_1^{r_1} \cdots v_t^{r_t}$, where $a \in \mathbb{F}_q^*$ and $r_i \in \mathbb{Z}$.*

Proof. By Proposition 2.2,

$$\varepsilon = \frac{f + g\sqrt{d}}{v_1^{m_1} \cdots v_t^{m_t}}.$$

Then $N_{K/k}(\varepsilon) = (f^2 - g^2 d)v_1^{-2m_1} \cdots v_t^{-2m_t}$. Suppose that $f^2 - g^2 d = u^s h$, where $u, h \in \mathbb{F}_q[x]$, $u \notin S_1$ is an irreducible polynomial, $s > 0$, and u does not divide h. Then

$$\varepsilon^{-1} = \frac{(f - g\sqrt{d})v_1^{m_1} \cdots v_t^{m_t}}{u^s h}.$$

Since $\varepsilon^{-1} \in \mathscr{O}_S$, it follows by Proposition 2.2 that u^s divides f and g. But then u^{2s} divides $f^2 - g^2 d$; a contradiction.

Proposition 2.3 is proved.

As in the case of S-integer elements, if an element $\varepsilon \in K$ has the property $N_{K/k}(\varepsilon) = av_1^{m_1} \cdots v_t^{m_t}$, then it does not follow that ε is an S-unit. For example, if the valuation $|\cdot|_{v_j}$ has two extensions to K and $|\cdot|_{v_j'}$ does not belong to S, then $N_{K/k}(v_j) = v_j^2$ but v_j is not an S-unit.

If $\varepsilon = (f + g\sqrt{d})/(v_1^{r_1} \cdots v_t^{r_t}) \in U_S$, then it follows from Proposition 2.3 that

$$f^2 - g^2 d = av_1^{m_1} \cdots v_t^{m_t}, \tag{2.3}$$

where $a \in \mathbb{F}_q^*$ and $m_1, \dots, m_t$ are non-negative integers. The following proposition shows that if the norm equation (2.3) for fixed $m_1, \dots, m_t$ has a solution in polynomials $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, then we can easily construct some S-unit.

Proposition 2.4. *Let $z = f + g\sqrt{d} \in K$, where $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, and suppose that*

$$N_{K/k}(z) = f^2 - g^2 d = av_1^{m_1} \cdots v_t^{m_t},$$

where $a \in \mathbb{F}_q^*$ and $m_i \geqslant 0$. Let $S_2 = \{|\cdot|_{v_1}, \dots, |\cdot|_{v_r}\}$ denote the set of valuations in S_1 satisfying the following conditions:

1) *$|\cdot|_{v_i}$ has two extensions $|\cdot|_{v_i'}$ and $|\cdot|_{v_i''}$ to K;*
2) *$|\cdot|_{v_i''} \notin S$;*
3) *$|z|_{v_i''} > 0$.*

Then $\varepsilon = z/(v_1^{m_1} \cdots v_r^{m_r}) \in U_S$. If S_2 is the empty set, then z is an S-unit.

Proof. Let us prove that $\varepsilon \in \mathscr{O}_S$. For an arbitrary valuation $|\cdot|_{v_i}$, $1 \leqslant i \leqslant r$, we have

$$|f^2 - g^2 d|_{v_i''} = |f - g\sqrt{d}|_{v_i''} + |f + g\sqrt{d}|_{v_i''} = m_i > 0 \tag{2.4}$$

by the construction of the set S_2. Since $|f + g\sqrt{d}|_{v_i''} > 0$, by Proposition 2.1 we have $|f - g\sqrt{d}|_{v_i''} = 0$, and then $|f + g\sqrt{d}|_{v_i''} = m_i$. Consequently, $|\varepsilon|_{v_i''} = m_i - m_i = 0$, $i = 1, \dots, r$. Therefore, $\varepsilon \in \mathscr{O}_S$.

Next,

$$\varepsilon^{-1} = \frac{f - g\sqrt{d}}{v_{r+1}^{m_{r+1}} \cdots v_t^{m_t}}.$$

Suppose that a valuation $|\cdot|_{v_i}$ for $r + 1 \leqslant i \leqslant t$ has two extensions to K and $|\cdot|_{v_i''} \notin S$. Then $|z|_{v_i''} = 0$ by hypothesis, and from (2.4) we obtain $|f - g\sqrt{d}|_{v_i''} = m_i$. Consequently, $|\varepsilon^{-1}|_{v_i''} = m_i - m_i = 0$ and $\varepsilon^{-1} \in \mathscr{O}_S$.

Proposition 2.4 is proved.

We now consider the following natural question: how will a system of independent fundamental S-units expand if we add a new valuation $|\cdot|_v$ to the set S? The answer to this question is given by the following theorem.

Theorem 2.5. *Let $\varepsilon_1, \dots, \varepsilon_s$ be independent fundamental S-units of the field K, and suppose that $v \in \mathbb{F}_q[x]$ is an irreducible polynomial such that at least one of the extensions of the valuation $|\cdot|_v$ to K does not belong to S. Then the following assertions hold.*

1. *Suppose that the valuation $|\cdot|_v$ has two extensions $|\cdot|_{v'}$ and $|\cdot|_{v''}$ to K. Furthermore, suppose that $|\cdot|_{v'} \in S$ and $|\cdot|_{v''} \notin S$. Let $S' = S \cup \{|\cdot|_{v''}\}$. Then $\varepsilon_1, \dots, \varepsilon_s, v$ is a system of independent fundamental S'-units.*

2. *Suppose that the valuation $|\cdot|_v$ has two extensions $|\cdot|_{v'}$ and $|\cdot|_{v''}$ to K which do not belong to S. Let $S' = S \cup \{|\cdot|_{v'}\}$. Suppose that ε is an S'-unit such that*

$$N_{K/k}(\varepsilon) = a v_1^{m_1} \cdots v_t^{m_t} v^{m_{t+1}}$$

with the least possible positive integer exponent m_{t+1}. Then $\varepsilon_1, \dots, \varepsilon_s, \varepsilon$ is a system of independent fundamental S'-units.

3. *Suppose that the valuation $|\cdot|_v$ has a unique extension to K. Let $S' = S \cup \{|\cdot|_v\}$. If $d/v \notin \mathbb{F}_q$, then $\varepsilon_1, \dots, \varepsilon_s, v$ is a system of independent fundamental S'-units. But if $d/v \in \mathbb{F}_q$, then $\varepsilon_1, \dots, \varepsilon_s, \sqrt{d}$ is a system of independent fundamental S'-units.*

Proof. 1. Suppose that the units $\varepsilon_1, \dots, \varepsilon_s, v$ are dependent. Then

$$\varepsilon_1^{m_1} \cdots \varepsilon_s^{m_s} v^m = 1,$$

where $m_i \in \mathbb{Z}$ and $m \neq 0$. Consequently, $v^m \in U_S$, but $|v^m|_{v''} = m \neq 0$; a contradiction.

Let $\varepsilon_1, \dots, \varepsilon_s, \varepsilon_{s+1}$ be a system of independent fundamental S'-units. Then

$$v = a\varepsilon_1^{r_1} \cdots \varepsilon_s^{r_s} \varepsilon_{s+1}^{r_{s+1}}, \tag{2.5}$$

where $a \in \mathbb{F}_q^*$, $r_i \in \mathbb{Z}$, and $r_{s+1} \neq 0$, since $v \notin U_S$. Since $\varepsilon_i \in U_S$ for $i = 1, \dots, s$, it follows that $|\varepsilon_i|_{v''} = 0$. From (2.5) we obtain $1 = |v|_{v''} = r_{s+1}|\varepsilon_{s+1}|_{v''}$, whence $r_{s+1} = \pm 1$. Thus, in view of (2.5), the fundamental S'-unit ε_{s+1} can be replaced by v.

2. We now show that the units $\varepsilon_1, \dots, \varepsilon_s, \varepsilon$ are independent. If $\varepsilon_1^{r_1} \cdots \varepsilon_s^{r_s} v^r = 1$, where $r_i \in \mathbb{Z}$ and $r \neq 0$, then $\varepsilon^r \in U_S$. Therefore, $|\varepsilon^r|_{v'} = r|\varepsilon|_{v'} = 0$, whence $|\varepsilon|_{v'} = 0$. Similarly, $|\varepsilon|_{v''} = 0$. Consequently, $\varepsilon \in U_S$; a contradiction with Proposition 2.3.

Let $\varepsilon_1, \dots, \varepsilon_s, \varepsilon_{s+1}$ be a system of independent fundamental S'-units. We claim that ε_{s+1} can be replaced by ε. Let

$$\varepsilon = a\varepsilon_1^{r_1} \cdots \varepsilon_s^{r_s} \varepsilon_{s+1}^{r_{s+1}}, \tag{2.6}$$

where $a \in \mathbb{F}_q^*$, $m_i \in \mathbb{Z}$, and $m_{s+1} \neq 0$. Let $N_{K/k}(\varepsilon_{s+1}) = bv_1^{k_1} \cdots v_t^{k_t} v^{k_{t+1}}$, where $b \in \mathbb{F}_q$. We observe that by Proposition 2.3 we have $N_{K/k}(\varepsilon_i) = cv_1^{i_1} \cdots v_t^{i_t}$ for $i = 1, \dots, s$. We now calculate the norms of the left- and right-hand sides in (2.6) and compare the exponents with which v occurs on the left- and right-hand sides. We obtain

$$m_{t+1} = r_{s+1}k_{t+1}.$$

Since $|k_{t+1}| \geqslant m_{t+1}$ by hypothesis, $r_{s+1} = \pm 1$ and we can use (2.6) to replace ε_{s+1} by ε.

3. If $d/v \notin \mathbb{F}_q$, then the proof is completely similar to part 1. Let $d/v \in \mathbb{F}_q$. As in part 1, it is easy to show that $\varepsilon_1, \dots, \varepsilon_s, \sqrt{d}$ are independent S'-units. Suppose that $\varepsilon_1, \dots, \varepsilon_s, \varepsilon_{s+1}$ is a system of independent fundamental S'-units. As in part 2, we prove that ε_{s+1} can be replaced by $\sqrt{d}$.

Theorem 2.5 is proved.

It follows from Theorem 2.5 that the key case for finding a system of independent fundamental S-units is the following. Let $v_1, \dots, v_t \in \mathbb{F}_q[x]$ be irreducible polynomials such that each of the valuations $|\cdot|_{v_i}$ has two extensions $|\cdot|_{v_i'}$ and $|\cdot|_{v_i''}$ to K. As the set S we take the following set of valuations: $S = \{|\cdot|_\infty, |\cdot|_{v_1'}, \dots, |\cdot|_{v_t'}\}$, that is, we include into S exactly one of the two extensions of the valuation $|\cdot|_{v_i}$ to K. In what follows we consider separately the cases where S contains two elements and where S contains more than two elements.

§ 3. Case $|S| = 2$

3.1. The general case. Let $S=\{|\cdot|_\infty, |\cdot|_{v'}\}$ and $\varepsilon \in U_S$. Then $\varepsilon = (f+g\sqrt{d})/v^k$ by Proposition 2.2 and $N_{K/k}(\varepsilon) = av^s$, where $a \in \mathbb{F}_q^*$, by Proposition 2.3. Consequently, $N_{K/k}(f+g\sqrt{d}) = f^2 - g^2 d = av^m$ for some positive integer m.

Proposition 3.1. *Suppose that m is the minimal positive integer such that the norm equation*

$$f^2 - g^2 d = av^m, \tag{3.1}$$

where $a \in \mathbb{F}_q^*$, has a solution in polynomials $f, g \in \mathbb{F}_q[x]$, $g \neq 0$. Then either $f+g\sqrt{d}$ or $f-g\sqrt{d}$ is a fundamental S-unit.

Proof. By Proposition 2.1, either $|f+g\sqrt{d}|_{v''} = 0$ or $|f-g\sqrt{d}|_{v''} = 0$. This means that either $f+g\sqrt{d}$ or $f-g\sqrt{d}$ is an S-unit. For example, suppose that $f+g\sqrt{d} \in U_S$, and let ε be a fundamental S-unit. Then by Proposition 2.3 $N_{K/k}(\varepsilon) = bv^k$, where $b \in \mathbb{F}_q^*$. Furthermore, we can assume that $k > 0$, if necessary replacing ε by ε^{-1}. Then $k \geqslant m$ by the hypothesis of the proposition. We have

$$f + g\sqrt{d} = c\varepsilon^r,$$

where $c \in \mathbb{F}_q^*$. By considering the norms of both parts, we obtain the equation $v^m = v^{rk}$, whence $m = rk$. Consequently, $r = 1$ and $f + g\sqrt{d} = c\varepsilon$.

Proposition 3.1 is proved.

In what follows we propose a method for solving the norm equation (3.1). Each element in the completion $\overline{k}$ can be represented as a formal power series with coefficients in Σ. However, in the case $\deg v > 1$, corresponding to the product of two elements in the completion $\overline{k}$ we do not have the ordinary product of the corresponding formal power series. The fact is that when formal power series are multiplied, the coefficients of the product may be polynomials of degree $\geqslant \deg v$. Therefore we need to rewrite the resulting formal power series in such a form that all the coefficients belong to Σ (that is, perform the operation of 'shift of digits'). We introduce the following notation. If $f(x) = f_0 + f_1x + \dots + f_rx^r \in \mathbb{F}_q[x]$, then we denote by $\widehat{f} = (f_0, \dots, f_r)^t$ the column vector of coefficients of f. We have the following proposition.

Proposition 3.2. *Let $v(x) = v_0 + v_1x + \dots + v_hx^h$, $v_h \neq 0$, be a fixed irreducible polynomial, and let $a(x) = a_0 + a_1x + \dots + a_{h-1}x^{h-1}$ and $b(x) = b_0 + b_1x + \dots + b_{h-1}x^{h-1}$ be polynomials in $\mathbb{F}_q[x]$. We divide ab by v with remainder: $ab = gv + r$, where $g = g_0 + g_1x + \dots + g_{h-2}x^{h-2}$ and $r = r_0 + r_1x + \dots + r_{h-1}x^{h-1}$. Then there exist $(h \times h)$-matrices $A_v(a)$ and $B_v(a)$ whose coefficients are linear functions of $a_0, \dots, a_{h-1}$ with coefficients in $\mathbb{F}_q$ such that*

$$\widehat{r} = A_v(a)\widehat{b}, \qquad \begin{pmatrix} \widehat{g} \\ 0 \end{pmatrix} = B_v(a)\widehat{b}. \tag{3.2}$$

Remark. In equation (3.2) we add 0 to the column $\widehat{g}$ in order that the matrices $A_v(a)$ and $B_v(a)$ have the same size, which is convenient for further calculations.

Proof of Proposition 3.2. Let $\overline{a}$, $\overline{b}$, $\overline{r}$, $\overline{x}$ be the images of a, b, r, x in the residue field k_v. Then $\overline{a}\overline{b} = \overline{r}$. Let φ be the linear operator on k_v given by $z \mapsto az$, and let $A_v(a)$ be the matrix of the operator φ in the basis $1, \overline{x}, \dots, \overline{x}^{h-1}$. Then $\widehat{r} = A_v(a)\widehat{b}$.

In order to find the matrix $B_v(a)$ we consider the equation $ab = gv + r$. By comparing the coefficients of $x^h, \dots, x^{2h-2}$ on the left- and right-hand sides of this equation we obtain

$$\sum_{l+e=h+j} g_lv_e = \sum_{l'+e'=h+j} a_{l'}b_{e'}, \qquad j = 0, 1, \dots, h-2.$$

This system of $h-1$ equations can be written in the matrix form

$$T_1\widehat{g} = T_2\widehat{b}, \tag{3.3}$$

where

$$T_1 = \begin{pmatrix} v_h & v_{h-1} & \dots & v_2 \\ 0 & v_h & \dots & v_3 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & v_h \end{pmatrix}, \qquad T_2 = \begin{pmatrix} a_{h-1} & a_{h-2} & \dots & a_1 \\ 0 & a_{h-1} & \dots & a_2 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{h-1} \end{pmatrix}.$$

Consequently, $\widehat{g} = T_1^{-1}T_2\widehat{b}$. By setting $B_v(a) = \begin{pmatrix} 0 & T_1^{-1}T_2 \\ 0 & 0 \end{pmatrix}$ we obtain the second of equations (3.2).

Proposition 3.2 is proved.

The matrix $B_v(a)$ in Proposition 3.2 is responsible for the 'shift of digits' when formal power series are multiplied. From Proposition 3.2 it is easy to obtain the following proposition.

Proposition 3.3. *Let* $u_1 = \sum_{i=s_1}^{\infty} a_i v^i$ *and* $u_2 = \sum_{i=s_2}^{\infty} b_i v^i$ *be two elements in the completion* $\overline{k}$. *We set* $C_v(a_{s_1}) = A_v(a_{s_1})$ *and* $C_v(a_i) = A_v(a_i) + B_v(a_{i-1})$ *for* $i > s_1$. *Then* $u_1u_2 = \sum_{j=s_1+s_2}^{\infty} L_j v^j$, *where*

$$\widehat{L}_j = \sum_{i+s=j} C_v(a_i)\widehat{b}_s. \tag{3.4}$$

Proof. We write the product u_1u_2 in the form

$$u_1u_2 = \sum_{j=s_1+s_2}^{\infty} M_j v^j,$$

where $M_j = \sum_{i+s=j} a_i b_s$. We divide a_ib_s by v with remainder: $a_ib_s = g_{is}v + r_{is}$. Then

$$M_j = M_j'v + M_j'',$$

where $M_j' = \sum_{i+s=j} g_{is}$ and $M_j'' = \sum_{i+s=j} r_{is}$. Consequently,

$$u_1u_2 = M''_{s_1+s_2}v^{s_1+s_2} + \sum_{j=s_1+s_2+1}^{\infty} (M'_{j-1} + M''_j)v^j,$$

where $M''_{s_1+s_2}, M'_{j-1} + M''_j \in \Sigma$. Therefore,

$$L_j = \begin{cases} M''_{s_1+s_2} & \text{if } j = s_1+s_2, \\ M'_{j-1} + M''_j & \text{if } j > s_1+s_2. \end{cases}$$

It follows from Proposition 3.2 that

$$\begin{pmatrix} \widehat{g}_{is} \\ 0 \end{pmatrix} = B_v(a_i)\widehat{b}_s, \qquad \widehat{r}_{is} = A_v(a_i)\widehat{b}_s.$$

For $j = s_1 + s_2$ we obtain

$$\widehat{L}_{s_1+s_2} = \widehat{r}_{s_1s_2} = A_v(a_{s_1})\widehat{b}_{s_2} = C_v(a_{s_1})\widehat{b}_{s_2},$$

since $A_v(a_{s_1}) = C_v(a_{s_1})$ by hypothesis. If $j > s_1 + s_2$, then

$$L_j = M'_{j-1} + M''_j = \sum_{i+s=j-1} g_{is} + \sum_{i+s=j} r_{is}.$$

Consequently,

$$\begin{aligned}\widehat{L}_j &= \sum_{i+s=j-1} \begin{pmatrix} \widehat{g}_{is} \\ 0 \end{pmatrix} + \sum_{i+s=j} \widehat{r}_{is} = \sum_{i+s=j-1} B_v(a_i)\widehat{b}_s + \sum_{i+s=j} A_v(a_i)\widehat{b}_s \\ &= \sum_{i+s=j} (B_v(a_{i-1}) + A_v(a_i))\widehat{b}_s = \sum_{i+s=j} C_v(a_i)\widehat{b}_s.\end{aligned}$$

Proposition 3.3 is proved.

Suppose that for a given m the norm equation (3.1) has a solution in polynomials $f, g \in \mathbb{F}_q[x]$, $g \neq 0$. Since the valuation $|\cdot|_v$ has two extensions to K, we have $\sqrt{d} \in \overline{k}$. We represent f, g, $\sqrt{d}$ as formal power series:

$$f = f_0 + f_1 v + \dots + f_r v^r, \qquad g = g_0 + g_1 v + \dots + g_e v^e, \qquad \sqrt{d} = \sum_{i=0}^{\infty} d_i v^i, \tag{3.5}$$

where $f_i, g_i, d_i \in \Sigma$. A comparison of the degrees of the left- and right-hand sides in (3.1) shows that

$$m \geqslant \frac{\deg d}{\deg v}, \qquad r = \left[\frac{m}{2}\right], \qquad e = \left[\frac{m \deg v - \deg d}{2 \deg v}\right], \tag{3.6}$$

where $[z]$ denotes the integer part of a number z. Furthermore, the degrees of the polynomials f_r and g_e must satisfy the following relations:

$$r_1 = \deg f_r = \left[\left(\frac{m}{2} - r\right) \deg v\right] = \begin{cases} 0 & \text{if } m \text{ is even,} \\ \left[\frac{\deg v}{2}\right] & \text{if } m \text{ is odd,} \end{cases} \tag{3.7}$$

$$e_1 = \deg g_e = \left[\frac{1}{2} R\right], \tag{3.8}$$

where R is the remainder after division of $m \deg v - \deg d$ by $2 \deg v$. We set $C_v(d_i) = C_i$ and consider the matrix

$$\overline{D}_m = \begin{pmatrix} C_{r-e} & C_{r-e+1} & \dots & C_r \\ C_{r-e+1} & C_{r-e+2} & \dots & C_{r+1} \\ \dots & \dots & \dots & \dots \\ C_{m-e-1} & C_{m-e} & \dots & C_{m-1} \end{pmatrix}. \tag{3.9}$$

Let D_m be the matrix obtained from $\overline{D}_m$ by crossing out the first $r_1 + 1$ rows and the columns with numbers $e_1 + 2, \dots, \deg v$ (if $e_1 + 2 > \deg v$, then columns are not crossed out). The following theorem gives an algorithm for finding a fundamental S-unit.

Theorem 3.4. *For a positive integer $m \geqslant \deg d / \deg v$, the norm equation (3.1) has a solution in polynomials $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, if and only if the rank of the matrix D_m is less than $e \deg v + e_1 + 1$.*

Proof. Suppose that for a given m the norm equation (3.1) has a solution in polynomials $f, g \in \mathbb{F}_q[x]$, $g \neq 0$. Then by Proposition 2.1 either $|f + g\sqrt{d}|_{v''} = m$ or $|f - g\sqrt{d}|_{v''} = m$. Consequently, one of the elements $f + g\sqrt{d}$ or $f - g\sqrt{d}$ when expanded into a formal power series has the form $\sum_{i=m}^{\infty} L_i v^i$, where $L_i \in \Sigma$. Suppose that $f + g\sqrt{d} = \sum_{i=m}^{\infty} L_i v^i$. By using Proposition 3.3 for calculating the coefficients L_i we obtain the following equations:

$$\widehat{L}_i = \widehat{f}_i + \sum_{j+j'=i,\, j' \leqslant e} C_j \widehat{g}_{j'} = 0, \qquad 0 \leqslant i \leqslant r, \tag{3.10}$$

$$\widehat{L}_i = \sum_{j=0}^{e} C_{i-j} \widehat{g}_j = 0, \qquad r < i < m. \tag{3.11}$$

We consider equation (3.10) for $i = r$. Let $f_r = f_{r,0} + \cdots + f_{r,r_1}x^{r_1}$ and $g_e = g_{e,0} + \cdots + g_{e,e_1}x^{e_1}$. Then

$$(f_{r,0}, \dots, f_{r,r_1}, 0, \dots, 0)^t + \sum_{j=0}^{e-1} C_{r-j}\widehat{g}_j + C_{r-e}(g_{e,0}, \dots, g_{e,e_1}, 0, \dots, 0)^t = 0. \quad (3.12)$$

We set

$$\widetilde{f}_r = \begin{pmatrix} f_{r,0} \\ \dots \\ f_{r,r_1} \end{pmatrix}, \qquad \widetilde{g}_e = \begin{pmatrix} g_{e,0} \\ \dots \\ g_{e,e_1} \end{pmatrix}, \qquad F(g) = \begin{pmatrix} \widetilde{g}_e \\ \widehat{g}_{e-1} \\ \dots \\ \widehat{g}_0 \end{pmatrix}.$$

Let $\widetilde{C}_i$ be the matrix consisting of the first $r_1 + 1$ rows of the matrix C_i. We point out that $F(g)$ is a column vector of length $e \deg v + e_1 + 1$. From (3.10), (3.12) we obtain

$$\widehat{f}_i = -\sum_{j+j'=i,\, j' \leqslant e} C_j\widehat{g}_{j'}, \quad 0 \leqslant i < r, \qquad \widetilde{f}_r = -\sum_{p=0}^{e} \widetilde{C}_{r-p}\widehat{g}_p. \quad (3.13)$$

By considering the last $\deg v - r_1 - 1$ equations in (3.12) and equations (3.11) we obtain

$$D_m F(g) = 0. \quad (3.14)$$

Thus, the homogeneous system of linear equations (3.14) with matrix D_m has a nonzero solution $F(g)$. Consequently, the rank of the matrix D_m is less than $e \deg v + e_1 + 1$.

Now suppose that the rank of the matrix D_m is less than $e \deg v + e_1 + 1$. Then the homogeneous system of linear equations (3.14) with matrix D_m has a nonzero solution $F(g)$. When we know the column vector $F(g)$, we find a nonzero polynomial g. Then by formulae (3.13) we find the coefficients of the polynomial f. By construction, the polynomials f and g have the property that $\deg(f^2 - g^2 d) \leqslant \deg v^m$ and v^m divides $f^2 - g^2 d$. Consequently, $f^2 - g^2 d = av^m$, where $a \in \mathbb{F}_q^*$.

Theorem 3.4 is proved.

Thus, in order to find a fundamental S-unit of the field K, first we need to expand $\sqrt{d}$ into a formal power series. Then, calculating consecutively the rank of the matrix D_m, starting from $m \geqslant \deg d / \deg v$, we find the minimal positive integer m such that the rank of D_m is less than $e \deg v + e_1 + 1$. After that, by solving the homogeneous system of linear equations with matrix D_m we find a nonzero polynomial g, and by formulae (3.13) the polynomial f. The sought-for fundamental S-unit has the form $f + g\sqrt{d}$.

The following proposition sharpens Theorem 3.4 for the case where d is an irreducible polynomial.

Proposition 3.5. *Suppose that the polynomial d is irreducible. Then the least positive integer m such that the norm equation (3.1) has a solution in polynomials $f, g \in k[x]$, $g \neq 0$, is an odd number.*

Proof. Suppose that $m = 2t$. Since a in (3.1) must be a square, it follows that after dividing both sides by a we can assume without loss of generality that $a = 1$, that is, f, g are solutions of the norm equation $f^2 - g^2 d = v^{2t}$. We write this equation in the form

$$(f - v^t)(f + v^t) = g^2 d. \tag{3.15}$$

Since d is irreducible, it divides one of the factors on the left-hand side of equation (3.15). For example, suppose that $f - v^t = df_1$. Then $f = v^t + df_1$. By substituting this expression into (3.15) we obtain

$$f_1(2v^t + df_1) = g^2, \tag{3.16}$$

whence f_1 divides g^2. Consequently, the polynomials g and f_1 can be represented in the form $g = f_2 h g_2$ and $f_1 = f_2^2 h$ for some $f_2, g_2, h \in \mathbb{F}_q[x]$. By substituting g and f_1 into (3.16) we obtain

$$2v^t + df_2^2 h = g_2^2 h. \tag{3.17}$$

It follows from (3.17) that h divides v^t and therefore $h = bv^r$ for some $b \in \mathbb{F}_q^*$. By dividing both parts of (3.17) by h we obtain that the norm equation $g_2^2 - f_2^2 d = 2b^{-1} v^{t-r}$ has a solution in polynomials $f_2, g_2 \in \mathbb{F}_q[x]$, $g_2 \neq 0$, and $t - r < 2t = m$, which contradicts the minimality of m.

Proposition 3.5 is proved.

3.2. Case of elliptic curve. We consider in more detail the case where $\deg d = 3$. We claim that then the matrix D_m in Theorem 3.4 is a square matrix.

Suppose that $m = 2m_1$ is even. Then it follows from equations (3.6)–(3.8) that

$$r = m_1, \qquad e = \left[m_1 - \frac{3}{2\deg v}\right] = \begin{cases} m_1 - 2 & \text{if } \deg v = 1, \\ m_1 - 1 & \text{if } \deg v \geqslant 2, \end{cases}$$
$$r_1 = 0, \qquad e_1 = \left[\deg v - \frac{3}{2}\right] = \deg v - 2.$$

Then

$$\overline{D}_m = \begin{pmatrix} C_1 & \dots & C_{m_1} \\ \dots & \dots & \dots \\ C_{m_1} & \dots & C_{2m_1-1} \end{pmatrix}$$

and, obviously, $\overline{D}_m$ is a square matrix. The matrix D_m is obtained from $\overline{D}_m$ by crossing out the first row and the column with number $\deg v$.

Now suppose that $m = 2m_1 - 1$ is odd. Then it follows from equations (3.6)–(3.8) that

$$r = m_1 - 1, \qquad e = \left[m_1 - \frac{\deg v + 3}{2\deg v}\right] = \begin{cases} m_1 - 2 & \text{if } \deg v \leqslant 2, \\ m_1 - 1 & \text{if } \deg v \geqslant 3, \end{cases}$$
$$r_1 = \left[\frac{\deg v}{2}\right], \qquad e_1 = \begin{cases} 0 & \text{if } \deg v = 1, \\ 1 & \text{if } \deg v = 2, \\ \left[\frac{\deg v - 3}{2}\right] & \text{if } \deg v \geqslant 3. \end{cases}$$

In the case $\deg v \leqslant 2$,

$$\overline{D}_m = \begin{pmatrix} C_1 & \dots & C_{m_1-1} \\ \dots & \dots & \dots \\ C_{m_1} & \dots & C_{2m_1-2} \end{pmatrix}.$$

The matrix D_m is obtained from $\overline{D}_m$ by crossing out the first $\deg v$ rows (no columns are crossed out). Consequently, for $\deg v \leqslant 2$,

$$D_m = \begin{pmatrix} C_2 & \dots & C_{m_1} \\ \dots & \dots & \dots \\ C_{m_1} & \dots & C_{2m_1-2} \end{pmatrix} \tag{3.18}$$

is a square matrix of order $(m_1 - 1)\deg v$.

If, however, $\deg v \geqslant 3$, then

$$\overline{D}_m = \begin{pmatrix} C_0 & \dots & C_{m_1-1} \\ \dots & \dots & \dots \\ C_{m_1-1} & \dots & C_{2m_1-2} \end{pmatrix}$$

and $\overline{D}_m$ is a square matrix. The matrix D_m is obtained from $\overline{D}_m$ by crossing out the first $[\deg v/2]+1$ rows and the columns with numbers $[(\deg v+1)/2], \dots, \deg v$. It is easy to verify that the number of rows and columns being crossed out coincide. Therefore, D_m is a square matrix.

Thus, in the case of elliptic curves we can state Theorem 3.4 as follows.

Theorem 3.6. *For a positive integer $m \geqslant 3/\deg v$ the norm equation (3.1) has a solution in polynomials $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, if and only if* $\det D_m = 0$.

Example 3.7. Let $k = \mathbb{F}_3(x)$, $v = x^2 + 1 \in k[x]$, and let

$$d = x^3 + 2x^2 + x + 1 = (x+2)v + 2 \in k[x]$$

which is an irreducible polynomial. In our case, for the polynomial $u = u_0 + u_1 x \in \Sigma$ we have

$$A_v(u) = \begin{pmatrix} u_0 & -u_1 \\ u_1 & u_0 \end{pmatrix}, \qquad B_v(u) = \begin{pmatrix} 0 & u_1 \\ 0 & 0 \end{pmatrix}.$$

Since 2 is a square in the residue field $\mathbb{F}_3[x]/(v)$, it follows that $\sqrt{d} \in \overline{k}$ and the element $\sqrt{d}$ can be represented as a formal power series:

$$\sqrt{d} = x + (x+2)v + (x+1)v^2 + xv^3 + xv^4 + 2xv^5 + (2x+1)v^6 + \cdots.$$

Then the first five matrices C_i are as follows:

$$C_0 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \qquad C_1 = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}, \qquad C_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

$$C_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad C_4 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Since the polynomial d is irreducible, by Proposition 3.5 the sought-for m is odd. We have

$$m \geqslant 2, \qquad r = \left[\frac{m}{2}\right], \qquad e = \left[\frac{2m-3}{4}\right], \qquad e_1 = r_1 = 1.$$

Since m is odd, the matrix D_m has the form (3.18).

Let $m = 3$. Then $D_3 = C_2$ is a nonsingular matrix.

Let $m = 5$. Then

$$D_5 = \begin{pmatrix} C_2 & C_3 \\ C_3 & C_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

We have $\det D_5 = 0$. The homogeneous system of linear equations $D_5 F(g) = 0$ has the solution $F(g) = (0,0,1,0)^t$, whence $g = x$. We now obtain $f = 1 - 2xv - xv^2 = 2x^5 + 2x^3 + 1$. Thus, a fundamental S-unit of the field K has the form

$$\varepsilon = 2x^5 + 2x^3 + 1 + x\sqrt{x^3 + 2x^2 + x + 1}.$$

3.3. Case $\deg v = 1$. Let $v = x - \alpha$. We can identify the completion $\overline{k}$ with the field of formal power series $\mathbb{F}_q((v))$. In this case, $A_v(f) = (0)$ and $B_v(f) = f$ for any $f \in \mathbb{F}_q$. If $\sqrt{d} = \sum_{i=0}^{\infty} d_i v^i$ is the expansion of $\sqrt{d}$ into a formal power series in $\overline{k}$, then $C_i = d_i$. From (3.6)–(3.8) we obtain that in the case of even $m = 2l$ we have $r = l$; but if $m = 2l - 1$, then $r = l - 1$. In both cases, $r_1 = e_1 = 0$ and $e = l - n - 1$. Then the matrix D_m in Theorem 3.4 has the form

$$D_{2l} = \begin{pmatrix} d_{n+2} & d_{n+3} & \dots & d_{l+1} \\ d_{n+3} & d_{n+4} & \dots & d_{l+2} \\ \dots & \dots & \dots & \dots \\ d_{l+n} & d_{l+n+1} & \dots & d_{2l-1} \end{pmatrix}, \quad D_{2l-1} = \begin{pmatrix} d_{n+1} & d_{n+2} & \dots & d_l \\ d_{n+2} & d_{n+3} & \dots & d_{l+1} \\ \dots & \dots & \dots & \dots \\ d_{l+n-1} & d_{l+n} & \dots & d_{2l-2} \end{pmatrix}. \tag{3.19}$$

We obtain the following corollary of Theorem 3.4.

Corollary 3.8. *Let $m \geqslant 2n+1$. If $m = 2l$ (respectively, $m = 2l-1$), then the norm equation (3.1) has a solution in polynomials $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, if and only if the rank of the matrix D_{2l} (respectively, D_{2l-1}) defined in (3.19) is less than $l - n$.*

If K is the field of functions of an elliptic curve, that is, $\deg d = 3$, then D_{2l} and D_{2l-1} are square matrices and we obtain the following result.

Corollary 3.9. *Suppose that $\deg d = 3$ and $m \geqslant 3$. If $m = 2l$ (respectively, $m = 2l-1$), then the norm equation (3.1) has a solution in polynomials $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, if and only if $\det D_{2l} = 0$ (respectively, $\det D_{2l-1} = 0$).*

The matrices of special form that appear in Corollary 3.9 are known as *Hankel matrices* (for a different numbering of the unknown coefficients of the polynomial g we obtain Toeplitz matrices). These matrices have numerous applications in algebra, theory of functions, harmonic analysis, probability theory, coding theory, and in many other areas (see the monograph [6] and survey [7]).

Example 3.10. Let $d = x^3+x^2+x+1 \in \mathbb{F}_5[x]$ and $v = x$. Then in the completion $\overline{k}$ we have the following expansion of $\sqrt{d}$ into a formal power series:

$$\sqrt{d} = 1 + 3x + x^2 + 0 \cdot x^3 + 2x^4 + \cdots .$$

The valuation $|\cdot|_v$ has two extensions to $k(\sqrt{d})$. Let $S = \{|\cdot|_\infty, |\cdot|_{v'}\}$. We have $D_3 = (1)$ and $D_4 = (0)$. As a solution of the homogeneous system of linear equations with matrix D_4 we take $g = 1$. Then from the conditions $|f + \sqrt{d}|_{v'} = 4$ and $\deg f \leqslant 2$ we obtain $f = -1 - 3x - x^2$. Thus, $\varepsilon = -x^2 - 3x - 1 + \sqrt{d}$ is a fundamental S-unit and $N_{K/k}(\varepsilon) = x^4$.

§ 4. Case $|S| > 2$

Now let $S = \{|\cdot|_\infty, |\cdot|_{v'_1}, \dots, |\cdot|_{v'_t}\}$, where $t > 1$. By part 2 of Theorem 2.5, a system of independent fundamental S-units can be constructed by induction. We set $S_i = \{|\cdot|_\infty, |\cdot|_{v'_1}, \dots, |\cdot|_{v'_i}\}$ and $S'_i = \{|\cdot|_\infty, |\cdot|_{v'_i}\}$. Let δ_i be a fundamental S'_i-unit, which can be found by using Theorem 3.4. Let $N_{K/k}(\delta_i) = b_i v_i^{m_i}$, where $b_i \in \mathbb{F}_q^*$.

Now suppose that we have already constructed independent fundamental S_i-units $\varepsilon_1, \dots, \varepsilon_i$. By Theorem 2.5 we need to find an S_{i+1}-unit ε_{i+1} such that

$$N_{K/k}(\varepsilon_{i+1}) = a_{i+1} v_1^{m_{i+1,1}} \cdots v_i^{m_{i+1,i}} v_{i+1}^{m_{i+1,i+1}},$$

where $a_{i+1} \in \mathbb{F}_q^*$ and the exponent $m_{i+1,i+1} > 0$ is least possible. Then $\varepsilon_1, \dots, \varepsilon_i, \varepsilon_{i+1}$ is a system of independent fundamental S_{i+1}-units.

Let $\varepsilon_1, \dots, \varepsilon_t$ be independent fundamental S-units constructed in this way. Consider the matrix

$$H(\varepsilon_1, \dots, \varepsilon_t) = \begin{pmatrix} m_{11} & 0 & \dots & 0 \\ m_{21} & m_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ m_{t1} & m_{t2} & \dots & m_{tt} \end{pmatrix}. \tag{4.1}$$

We have the following proposition.

Proposition 4.1. *There exists a system of independent fundamental S-units $\varepsilon_1, \dots, \varepsilon_t$ such that the matrix $H(\varepsilon_1, \dots, \varepsilon_t)$ defined in* (4.1) *has the following properties:*

1) $0 \leqslant m_{ir} < m_{rr}$ *for* $r = 1, \dots, t-1$, $i = r+1, \dots, t$;

2) $\varepsilon_i = f_i + g_i\sqrt{d}$, *where* $f_i, g_i \in \mathbb{F}_q[x]$, $g_i \neq 0$, $i = 1, \dots, t$;

3) $\sum_{j=1}^{i} m_{ij} \deg v_j \geqslant \deg d$;

4) m_{ii} *divides* m_i *for* $i = 1, \dots, t$;

5) *if* $m_{ii} = m_i$, *then* $m_{i1} = \dots = m_{i,r-1} = 0$;

6) *the row* $(m_i/m_{ii})(m_{i1}, \dots, m_{i,i-1})$ *is a linear combination with integer coefficients of the rows* $(m_{11}, 0, \dots, 0)$, $\dots$, $(m_{i-1,1}, \dots, m_{i-1,i-1})$.

Proof. 1) Let $\varepsilon_1, \dots, \varepsilon_t$ be a system of independent fundamental S-units constructed by induction. If $\varepsilon'_1, \dots, \varepsilon'_t$ is another system of independent fundamental S-units, then

$$\varepsilon'_i = \varepsilon_1^{b_{i1}} \cdots \varepsilon_t^{b_{it}}, \qquad i = 1, \dots, t. \tag{4.2}$$

Furthermore, $B = (b_{ij}) \in GL_t(\mathbb{Z})$. Conversely, if $B = (b_{ij}) \in GL_t(\mathbb{Z})$ is an arbitrary matrix, then formulae (4.2) define a transition to a new system of independent fundamental S-units. It is easy to see that, furthermore,

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

Therefore, by multiplying $H(\varepsilon_1, \dots, \varepsilon_t)$ by a suitable matrix $B \in GL_t(\mathbb{Z})$ we can ensure that condition 1) holds.

2) Let $\varepsilon_i = (f_i + g_i\sqrt{d})/(v_1^{l_1} \cdots v_i^{l_i})$, where $f_i, g_i \in \mathbb{F}_q[x]$, $g_i \neq 0$, and suppose, for example, that $l_1 > 0$. Then

$$|\varepsilon_i|_{v''_1} = |f_i + g_i\sqrt{d}|_{v''_1} - l_1 = 0. \tag{4.3}$$

Since $N_{K/k}(\varepsilon_i) = (f_i^2 - g_i^2 d)/(v_1^{2l_1} \cdots v_i^{2l_i})$, we have

$$f_i^2 - g_i^2 d = v_1^{2l_1 + m_{i1}} \cdots v_i^{2l_i + m_{ii}}.$$

Since $m_{i1} \geqslant 0$ by hypothesis, we have $2l_1 + m_{i1} > 0$. Then $|f_i + g_i\sqrt{d}|_{v''_1} = 2l_1 + m_{i1}$ by Proposition 2.1. It follows from (4.3) that $2l_1 + m_{i1} = l_1$, whence we obtain the equation $m_{i1} = -l_1 < 0$; a contradiction.

3) Since $\varepsilon_i = f_i + g_i\sqrt{d}$ by condition 2), we have $f_i^2 - g_i^2 d = v_1^{m_{i1}} \cdots v_i^{m_{ii}}$. Since $g_i \neq 0$, by comparing the degrees of the left- and right-hand sides we obtain the required assertion.

4) Since δ_i is an S_i-unit, we have $\delta_i = c_i\varepsilon_1^{a_1} \cdots \varepsilon_i^{a_i}$, where $c_i \in \mathbb{F}_q^*$. Then

$$N_{K/K}(\delta_i) = N_{K/K}(c_i\varepsilon_1^{a_1} \cdots \varepsilon_i^{a_i}), \tag{4.4}$$

whence we obtain $m_i = a_i m_{ii}$, which is what proves condition 4). If $m_{ii} = m_i$, then $a_i = 1$ and we can replace ε_i by δ_i. After this replacement, condition 5) holds.

6) It follows from (4.4) that

$$\frac{m_i}{m_{ii}}(m_{i1}, \dots, m_{i,i-1}) = a_1(m_{11}, 0, \dots, 0) + \cdots + a_i(m_{i-1,1}, \dots, m_{i-1,i-1}).$$

Proposition 4.1 is proved.

Corollary 4.2. *Let $\varepsilon_1, \dots, \varepsilon_{t-1}$ be a system of independent fundamental S_{t-1}-units. Let m_{tt} be the least positive integer divisor of m_t with the following property: there exist integers $0 \leqslant m_{tj} < m_{jj}$, $j = 1, \dots, t-1$, satisfying conditions* 3), 5), 6) *of Proposition* 4.1 *such that the norm equation*

$$f^2 - g^2 d = a v_1^{m_{t1}} \cdots v_t^{m_{tt}}, \tag{4.5}$$

where $a \in \mathbb{F}_q^*$, has a solution in polynomials $f, g \in \mathbb{F}_q[x]$, $g \neq 0$. Let ε_t be an S-unit obtained from this solution by using Proposition 2.4*. Then $\varepsilon_1, \dots, \varepsilon_t$ is a system of independent fundamental S-units.*

As in the case of a single valuation, solving the norm equation (4.5) reduces to solving a certain homogeneous system of linear equations. It follows from (4.5) that

$$\deg f \leqslant \left[\frac{1}{2}\sum_{j=1}^{t} m_{ij}\deg v_j\right] = r, \qquad \deg g \leqslant \left[\frac{1}{2}\left(\sum_{j=1}^{t} m_{ij}\deg v_j - \deg d\right)\right] = l.$$

Let $f = f_0 + f_1 x + \dots + f_r x^r$ and $g = g_0 + g_1 x + \dots + g_l x^l$. We choose one of the valuations $|\cdot|_{v_j}$, $1 \leqslant j \leqslant t$, and represent $f + g\sqrt{d}$ in the form of a formal power series in v_j:

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

where $L_i \in \Sigma$; here the coefficients of the polynomial L_i are linear forms in $f_0, \dots, f_r$, $g_0, \dots, g_l$. We require that the following conditions hold:

$$L_0 = \dots = L_{m_{tj}-1} = 0. \tag{4.6}$$

Then (4.6) gives a homogeneous system of linear equations with respect to the coefficients $f_0, \dots, f_r$, $g_0, \dots, g_l$ with some matrix M_{v_j}:

$$M_{v_j}(f_0, \dots, f_r, g_0, \dots, g_l)^t = 0.$$

Having performed this construction for all the valuations $|\cdot|_{v_j}$, $j = 1, \dots, t$, we obtain that $f_0, \dots, f_r$, $g_0, \dots, g_l$ is a solution of the homogeneous system of linear equations

$$M(f_0, \dots, f_r, g_0, \dots, g_l)^t = 0, \tag{4.7}$$

where M is a block matrix of the form $M = \begin{pmatrix} M_{v_1} \\ \vdots \\ M_{v_t} \end{pmatrix}$.

Conversely, if $f_0, \dots, f_r$, $g_0, \dots, g_l$ is a solution of (4.7) such that not all the g_i are equal to zero, then by construction the nonzero polynomial $f^2 - g^2 d$ is divisible by the product $v_1^{m_{t1}} \cdots v_t^{m_{tt}}$. Furthermore, $\deg f^2 - g^2 d \leqslant \deg v_1^{m_{t1}} \cdots v_t^{m_{tt}}$. Consequently, $f^2 - g^2 d = a v_1^{m_{t1}} \cdots v_t^{m_{tt}}$, where $a \in \mathbb{F}_q^*$.

Thus, we have proved the following theorem.

Theorem 4.3. *The norm equation* (4.5) *has a solution* $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, *if and only if the homogeneous system of linear equations* (4.7) *has a solution* $f_0, \dots, f_r$, $g_0, \dots, g_l$ *such that not all of the* g_k *are equal to zero.*

We also point out the following property of S-units, which holds for our choice of S.

Proposition 4.4. *Let* $\varepsilon \in U_S$. *If* $N_{K/k}(\varepsilon) \in \mathbb{F}_q^*$, *then* $\varepsilon \in \mathbb{F}_q^*$.

Proof. Let $\varepsilon = (f + g\sqrt{d})/(v_1^{m_1} \cdots v_t^{m_t})$, where $f, g \in \mathbb{F}_q[x]$. Suppose that $m_1 > 0$. Then $|f + g\sqrt{d}|_{v_1'} = m_1$. By hypothesis, $N_{K/k}(\varepsilon) = a$; consequently,

$$f^2 - g^2 d = a v_1^{2m_1} \cdots v_t^{2m_t}.$$

Hence we obtain that

$$|f + g\sqrt{d}|_{v_1'} + |f - g\sqrt{d}|_{v_1'} = 2m_1.$$

Since $|f + g\sqrt{d}|_{v_1'} > 0$, by Proposition 2.1 we have $|f + g\sqrt{d}|_{v_1'} = 2m_1$; a contradiction. Therefore, $m_1 = \dots = m_t = 0$. But then $N_{K/k}(\varepsilon) \notin \mathbb{F}_q^*$, which contradicts the hypothesis.

Proposition 4.4 is proved.

Remark. Proposition 4.4 ceases to be true in the case of an arbitrary S. Indeed, let ε be a fundamental unit in Example 3.10. We set $S_1 = S \cup \{|\cdot|_{x''}\}$. Then the element ε/x^2 is a nontrivial S_1-unit and $N_{K/k}(\varepsilon/x^2) = 1$. Note that ε/x^2 is not an S-unit (and not even an S-integer element).

Example 4.5. Suppose that the conditions of Example 3.10 hold. Let $u = x - 1$. The valuation $|\cdot|_u$ has two extensions $|\cdot|_{u'}$ and $|\cdot|_{u''}$ to $k(\sqrt{d})$. We set $S_1 = \{|\cdot|_\infty, |\cdot|_{v'}, |\cdot|_{u'}\}$. We now find a system of independent fundamental S_1-units.

First we set $T = \{|\cdot|_\infty, |\cdot|_{u'}\}$ and find a fundamental T-unit. Let k_1 be the completion of k with respect to $|\cdot|_u$. In the field k_1 we have the following expansion of $\sqrt{d}$ into a formal power series:

$$\sqrt{d} = 2 + 4(x-1) + 2(x-1)^2 + 0 \cdot (x-1)^3 + 4(x-1)^4 + \cdots .$$

We have $D_3 = (2)$ and $D_4 = (0)$. As in Example 3.10, we obtain $g = 1$ and $f = -2 - 4(x-1) - 2(x-1)^2 = 3x^2$. Thus, $\varepsilon_1 = 3x^2 + \sqrt{d}$ is a fundamental T-unit and $N_{K/k}(\varepsilon_1) = -(x-1)^4$.

If ε, ε_2 is a system of independent fundamental S_1-units, then by Proposition 4.1 the matrix $H(\varepsilon, \varepsilon_2)$ can have one of the following forms:

$$1)\ \begin{pmatrix} 4 & 0 \\ 2 & 1 \end{pmatrix}; \qquad 2)\ \begin{pmatrix} 4 & 0 \\ 3 & 1 \end{pmatrix}; \qquad 3)\ \begin{pmatrix} 4 & 0 \\ 2 & 2 \end{pmatrix}; \qquad 4)\ \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

We consider these cases consecutively, until we find a system of independent fundamental S_1-units.

1) We have the norm equation $f^2 - g^2 d = a x^2 (x-1)$. Then $\deg f = 1$ and $\deg g = 0$. Let $f = f_0 + f_1 x$. In the completion $\overline{k}$ with respect to the valuation $|\cdot|_x$ the element $f + g\sqrt{d}$ has the form

$$f_0 + g + (f_1 + 3g)x + gx^2 + \cdots .$$

Hence we obtain the equations $f_0 + g = 0$ and $f_1 + 3g = 0$.

In the completion of k_1 the element $f + g\sqrt{d}$ has the form

$$f_0 + f_1 + 2g + (f_1 + 4g)(x-1) + 2g(x-1)^2 + \cdots .$$

Hence we obtain the equation $f_0 + f_1 + 2g = 0$. Thus, we have a homogeneous system of linear equations with the matrix $\left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 3 \\ 1 & 1 & 2 \end{smallmatrix}\right)$, which is nonsingular. Therefore, $f_0 = f_1 = g = 0$, and our norm equation has no nontrivial solutions.

2) We have the norm equation $f^2 - g^2 d = a x^3 (x-1)$. Then $\deg f = 2$ and $\deg g = 0$. Let $f = f_0 + f_1 x + f_2 x_2$. In this case we obtain a homogeneous system of linear equations with the matrix $\left(\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 2 \end{smallmatrix}\right)$, which is also nonsingular. Therefore the norm equation also has no nontrivial solutions.

3) We have the norm equation $f^2 - g^2 d = a x^2 (x-1)^2$. Then, as in part 2), $\deg f = 2$ and $\deg g = 0$. We obtain a homogeneous system of linear equations with the matrix $\left(\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 3 \\ 1 & 1 & 1 & 2 \\ 0 & 1 & 2 & 4 \end{smallmatrix}\right)$, the determinant of which is equal to zero. By solving this system we obtain $f = 4 + 2x + 2x^2$ and $g = 1$. By Corollary 4.2, $\varepsilon = -x^2 - 3x - 1 + \sqrt{d}$ and $\varepsilon_2 = 2x^2 + 2x + 4 + \sqrt{d}$ is a system of independent fundamental S_1-units.

§ 5. Continued fractions in function fields

5.1. Construction and properties of continued fractions. Continued fractions in function fields in the case of the valuation $|\cdot|_\infty$ were for the first time introduced by Artin (see [8]). We consider the general case of an arbitrary valuation $|\cdot|_v$ of the field $k = L(x)$, where L is an arbitrary field. Let $\beta \in \overline{k}$. We represent β in the form of a formal power series:

$$\beta = \sum_{i=s}^{\infty} d_i v^i,$$

where $d_i \in \Sigma$, and set

$$[\beta] = \begin{cases} \displaystyle\sum_{i=s}^{0} d_i v^i & \text{if } s \leqslant 0, \\ 0 & \text{if } s > 0. \end{cases}$$

Let $a_0 = [\beta]$. If $\beta - a_0 \neq 0$, then we set

$$\beta_1 = \frac{1}{\beta - a_0} \in \overline{k}, \qquad a_1 = [\beta_1].$$

Next we define by induction elements a_i, β_i: if $\beta_{i-1} - a_{i-1} \neq 0$, then

$$\beta_i = \frac{1}{\beta_{i-1} - a_{i-1}} \in \overline{k}, \qquad a_i = [\beta_i].$$

As a result we obtain the continued fraction

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \tag{5.1}$$

Proposition 5.1. *The continued fraction* (5.1) *is finite if and only if* $\beta \in k$.

Proof. Suppose that $\beta \in k$. Let $\beta_i = b_i/c_i$, where $b_i, c_i \in L[x]$ and $(b_i, c_i) = 1$. Then $|\beta_i|_v = -s < 0$ by construction. Let

$$c_i = v^s c_{i+1}, \qquad [\beta_i] = \frac{a_0 + \cdots + a_s v^s}{v^s},$$

where $a_i \in \Sigma$. Then

$$\beta_i - [\beta_i] = \frac{b_i}{v^s c_{i+1}} - \frac{a_0 + \cdots + a_s v^s}{v^s} = \frac{b_i - c_{i+1}(a_0 + \cdots + a_s v^s)}{v^s c_{i+1}}.$$

Since $|\beta_i - [\beta_i]|_v > 0$, we have $b_i - c_{i+1}(a_0 + \cdots + a_s v^s) = v^s b_{i+1}$, where $b_{i+1} \in L[x]$. Then

$$\beta_{i+1} = \frac{c_{i+1}}{b_{i+1}}.$$

Furthermore, $\deg c_{i+1} < M_i$ and $\deg b_{i+1} < M_i$, where $M_i = \max\{\deg b_i, \deg c_i\}$. The decreasing sequence of positive integers M_i must terminate. This means that the continued fraction (5.1) is finite. The converse assertion is obvious.

Proposition 5.1 is proved.

We use the standard abbreviated notation $[a_0, a_1, a_2, \dots]$ for the continued fraction (5.1). By construction, $\beta_n = [a_n, a_{n+1}, \dots]$.

We define by induction elements $p_i, q_i \in k$. We set

$$p_{-2} = 0, \qquad p_{-1} = 1, \qquad q_{-2} = 1, \qquad q_{-1} = 0,$$

and if $n \geqslant 0$, then

$$p_n = a_n p_{n-1} + p_{n-2}, \qquad q_n = a_n q_{n-1} + q_{n-2}. \tag{5.2}$$

Then $p_n/q_n = [a_0, a_1, a_2, \dots, a_n]$ for $n \geqslant 0$. It can be shown in standard fashion (see [9]) that for $n \geqslant -1$ the following relations hold:

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n, \tag{5.3}$$

$$q_n \beta - p_n = \frac{(-1)^n}{q_n \beta_{n+1} + q_{n-1}}, \tag{5.4}$$

$$\beta = \frac{p_n \beta_{n+1} + p_{n-1}}{q_n \beta_{n+1} + q_{n-1}}. \tag{5.5}$$

We call the fraction p_n/q_n the *nth convergent to* β. By construction, $|a_n|_v = |\beta_n|_v < 0$ for $n \geqslant 1$. From (5.2) it is easy to obtain by induction the relation

$$|q_n|_v = |a_n|_v + |q_{n-1}|_v = \sum_{j=1}^{n} |a_j|_v, \tag{5.6}$$

and from (5.4) we obtain

$$|q_n \beta - p_n|_v = -|q_{n+1}|_v = -|a_{n+1}|_v - |q_n|_v > -|q_n|_v, \tag{5.7}$$

or, which is equivalent,

$$\left| \beta - \frac{p_n}{q_n} \right|_v > -2|q_n|_v. \tag{5.8}$$

Therefore, $\lim_{n\to\infty} p_n/q_n = \beta$, that is, the convergents converge to β.

As in the case of the field of real numbers, one can show in standard fashion that if the continued fraction $[a_0, a_1, \dots]$ for β is periodic, then $\beta \in \overline{k}$ is a quadratic irrationality. In the case of an infinite field L and the valuation $|\cdot|_\infty$, the converse assertion is not always true (see [10]). The following proposition holds.

Proposition 5.2. *Let* $L = \mathbb{F}_q$ *be the field of* q *elements, and let* $\deg v = 1$. *If* $\beta \in \overline{k} = L((v))$ *is a quadratic irrationality, then the continued fraction for* β *is periodic.*

Proof. Let $\beta \in L((v))$ be a root of a quadratic polynomial $H(X) = rX^2 + sX + t$, where $r, s, t \in L[v]$, and let $\beta = [a_0, a_1, \dots]$ be the expansion of β into a continued fraction. We set

$$D = s^2 - 4rt, \qquad H(X, Y) = rX^2 + sXY + tY^2.$$

Then from (5.5) we obtain

$$\beta_{n+1} = \frac{B_n + r\beta}{A_n}, \tag{5.9}$$

where

$$A_n = (-1)^{n+1} H(p_n, q_n), \qquad B_n = (-1)^n (rp_{n-1}p_n + sp_{n-1}q_n + tq_{n-1}q_n).$$

Clearly, for a sufficiently large n we have $|p_n/q_n - \beta|_v > |\beta - \overline{\beta}|_v$, where $\overline{\beta}$ is the second root of $H(X)$. Then

$$\left|\frac{p_n}{q_n} - \overline{\beta}\right|_v = \left|\frac{p_n}{q_n} - \beta + \beta - \overline{\beta}\right|_v = |\beta - \overline{\beta}|_v.$$

Since $\beta - \overline{\beta} = 2\sqrt{D}/r$, we have $|\beta - \overline{\beta}|_v = (1/2)|D|_v - |r|_v$. Hence we obtain

$$|p_n - \overline{\beta} q_n|_v = |q_n|_v + \frac{1}{2}|D|_v - |r|_v.$$

Since $H(X,Y) = r(X - \beta Y)(X - \overline{\beta} Y)$, by taking into account (5.7) we find

$$|A_n|_v = \bigl|r(p_n - \beta q_n)(p_n - \overline{\beta} q_n)\bigr|_v = \frac{1}{2}|D|_v - |a_{n+1}|_v > 0. \tag{5.10}$$

Let us find a lower estimate for $|B_n|_v$. From (5.9) we find $B_n = A_n \beta_{n+1} - r\beta$. It follows from equation $\beta(r\beta + s) = -t$ that $|r\beta|_v \geqslant 0$. By taking into account (5.10) and the fact that $|\beta_{n+1}|_v = |a_{n+1}|_v$, we find

$$|A_n \beta_{n+1}|_v = |A_n a_{n+1}|_v = \frac{1}{2}|D|_v \geqslant 0.$$

Therefore,

$$|B_n|_v \geqslant \min\bigl\{|A_n \beta_{n+1}|_v, |r\beta|_v\bigr\} \geqslant 0.$$

Thus, A_n, B_n are polynomials in $L[x]$. Their degrees do not exceed $\max\{\deg r, \deg s, \deg t\}$. Since the field L is finite, there are finitely many such polynomials. This means that for some i and j we must have $A_i = A_{i+j}$ and $B_i = B_{i+j}$. Then $\beta_i = \beta_{i+j}$ and the continued fraction for β is periodic.

Proposition 5.2 is proved.

We point out that in the case $\deg v > 1$ the argument given above ceases to be valid. Although A_n, B_n will be, as before, polynomials in $L[x]$, we cannot claim that their degrees are bounded above.

5.2. Best approximations. We introduce the notion of a best approximation to an element $\beta \in \overline{k}$. If $a/b \in L(x)$, where $a, b \in L[x]$ are coprime polynomials, then we expand a and b in powers of v:

$$a = a_0 + a_1 v + \dots + a_s v^s, \qquad b = b_0 + b_1 v + \dots + b_t v^t,$$

where $a_i, b_i \in \Sigma$, $a_s \neq 0$, $b_t \neq 0$. Then, after dividing a and b by v^r, where $r = \max\{s, t\}$, we represent the fraction a/b in the form

$$\frac{a}{b} = \frac{c_{-m} v^{-m} + \dots + c_0}{d_{-r} v^{-r} + \dots + d_0}, \tag{5.11}$$

where $c_i, d_i \in \Sigma$, $c_{-m} \neq 0$, $d_{-r} \neq 0$, and c_0 and d_0 are not simultaneously equal to zero. In what follows we assume that all elements in $L(x)$ are written in the form (5.11).

Definition 5.3. An irreducible fraction $p/q \in L(x)$ is a *best approximation* to $\beta \in \overline{k}$ if for any other irreducible fraction $a/b \neq p/q$ such that $|b|_v \geqslant |q|_v$ we have the inequality

$$\left|\beta - \frac{p}{q}\right|_v > \left|\beta - \frac{a}{b}\right|_v.$$

Theorem 5.4. *A fraction p/q is a best approximation to β if and only if one of the following conditions holds.*

1. *Let* $\deg v = 1$. *The fraction p/q is a best approximation to β if and only if* $|\beta - p/q|_v > -2|q|_v$.

2. *Let* $\deg v > 1$. *If* $|\beta - p/q|_v > -2|q|_v + 1$, *then the fraction p/q is a best approximation to β. If the fraction p/q is a best approximation to β, then* $|\beta - p/q|_v > -2|q|_v$.

Proof. Suppose that the following condition holds for the fraction p/q:

$$\left|\beta - \frac{p}{q}\right|_v > \begin{cases} -2|q|_v & \text{if } \deg v = 1, \\ -2|q|_v + 1 & \text{if } \deg v > 1. \end{cases}$$

Let c/d be a fraction such that $c/d \neq p/q$ and $|d|_v \geqslant |q|_v$. Since

$$|pd - cq|_v \leqslant \begin{cases} 0 & \text{if } \deg v = 1, \\ 1 & \text{if } \deg v > 1, \end{cases}$$

we have

$$\left|\frac{p}{q} - \frac{c}{d}\right|_v = |pd - cq|_v - |q|_v - |d|_v \leqslant \begin{cases} -2|q|_v & \text{if } \deg v = 1, \\ -2|q|_v + 1 & \text{if } \deg v > 1. \end{cases}$$

From the last inequality we obtain

$$\left|\beta - \frac{c}{d}\right|_v = \left|\beta - \frac{p}{q} + \frac{p}{q} - \frac{c}{d}\right|_v = \left|\frac{p}{q} - \frac{c}{d}\right|_v < \left|\beta - \frac{p}{q}\right|_v.$$

Therefore, the fraction p/q is a best approximation to β.

Now suppose that the fraction p/q is a best approximation to β. Let $h = \deg v$. We write the elements p, q, β in the form of formal power series in v:

$$p = \sum_{i=-r}^{0} a_i v^i, \qquad q = \sum_{i=-s}^{0} b_i v^i, \qquad \beta = \sum_{i=m}^{\infty} u_i v^i, \tag{5.12}$$

where $a_i, b_i, u_i \in \Sigma$, $a_{-r} \neq 0$, $b_{-s} \neq 0$. Suppose that $|\beta - p/q|_v \leqslant -2|q|_v$. Then $l = |q\beta - p|_v \leqslant -|q|_v = s$. It is easy to obtain from the definition of a best approximation that $l > 0$. Then we must have $|p|_v = |q|_v + |\beta|_v$, that is, $r = s - m$. We set

$$C_j = \begin{cases} 0 & \text{if } j < m, \\ A_v(u_m) & \text{if } j = m, \\ A_v(u_j) + B_v(u_{j-1}) & \text{if } j > m, \end{cases}$$

where the matrices A_v, B_v are defined in (3.2). Then $q\beta = \sum_{j=m-s}^{\infty} d_j v^j$, where $\widehat{d}_j = \sum_{i+e=j} C_i \widehat{b}_e$. Since

$$|q\beta - p|_v = \left| \sum_{i=-r}^{0} (d_i - a_i) v^i + \sum_{i=1}^{\infty} d_i v^i \right|_v = l,$$

we obtain the following equations:

$$\widehat{a}_i = \widehat{d}_i, \qquad i = -r, \dots, 0, \tag{5.13}$$

$$\widehat{d}_1 = \widehat{d}_2 = \cdots = \widehat{d}_{l-1} = 0. \tag{5.14}$$

We set

$$\widehat{q} = \begin{pmatrix} \widehat{b}_0 \\ \dots \\ \widehat{b}_{-s} \end{pmatrix}, \qquad C = \begin{pmatrix} C_1 & \dots & C_{s+1} \\ \dots & \dots & \dots \\ C_{l-1} & \dots & C_{s+l-1} \end{pmatrix}.$$

It follows from (5.14) that $\widehat{q}$ is a solution of the homogeneous system of linear equations

$$CY = 0, \tag{5.15}$$

where $Y = (y_1, \dots, y_{h(s+1)})^t$ is a column vector containing $h(s+1)$ variables. The matrix C with coefficients in the field L contains $h(s+1)$ columns and $h(l-1)$ rows. Since $l \leqslant s$ by our assumption, we have $\operatorname{rank} C \leqslant h(l-1)$. Consequently, a general solution of (5.15) has the form

$$y_i = H_i(z_1, \dots, z_m), \qquad i = 1, \dots, h(s+1), \tag{5.16}$$

where H_i is some linear form in the variables $z_1, \dots, z_m$ and

$$m = h(s+1) - \operatorname{rank} C \geqslant h(s-l+2) \geqslant 2h.$$

Let V be the space of solutions of (5.15). By what was said above, $\dim V = m \geqslant 2h$.

We associate with each nonzero tuple $(z_1^0, \dots, z_m^0) \in L^m$ the element $\overline{q}_1 = (y_1^0, \dots, y_{h(s+1)}^0)^t \in V$, where $y_i^0 = H_i(z_1^0, \dots, z_m^0)$. In turn, for an arbitrary nonzero element $\overline{q}_1 \in V$ we can construct a fraction p_1/q_1 that has the following properties: $|q_1|_v \geqslant |q|_v$ and

$$|q_1\beta - p_1|_v \geqslant |q\beta - p|_v. \tag{5.17}$$

For that we construct the polynomials $b_{-i}^0 = y_{hi+1}^0 + y_{hi+2}^0 x + \dots + y_{hi+h}^0 x^{h-1}$, $i = 0, \dots, s$. Next, we set

$$\widehat{a}_j^0 = \sum_{i+e=j} C_i \widehat{b}_e^0, \qquad j = -r, \dots, 0,$$

and consider the elements

$$q_1 = \sum_{i=0}^{s-1} b_{-i}^0 v^{-i}, \qquad p_1 = \sum_{i=0}^{-r} a_{-i}^0 v^{-i}.$$

The fraction p_1/q_1 will be the required one.

We distinguish in V two subspaces U and W, which we shall now describe. Since (5.15) has a solution $\overline{q}$ in which $b_{-s} \neq 0$, not all of the forms $H_{sh+1}, \dots, H_{sh+h}$ are zero. Let $T \subset L^m$ be the space of solutions of the homogeneous system of linear equations

$$H_{sh+1}(z_1, \dots, z_m) = \cdots = H_{sh+h}(z_1, \dots, z_m) = 0.$$

Then $\dim T \leqslant m - 1$. Let U be the set of those solutions of the system (5.15) that correspond to elements of T. Clearly, U is a proper subspace of V.

We now describe the set of those fractions p_1/q_1 for which $|q_1|_v \geqslant |q|_v$ and $p/q = p_1/q_1$ in the field $L(x)$. Since the fraction p/q is irreducible, the fraction p_1/q_1 is obtained from p/q as follows: we multiply p and q by some polynomial $\alpha \in L[x]$, and then reduce the resulting fraction $\alpha p/(\alpha q)$ to the form (5.11).

The polynomials a_0, b_0 in (5.12) are not simultaneously equal to zero. For definiteness suppose that $a_0 \neq 0$ and $\deg a_0 \geqslant \deg b_0$. Then $\alpha p = \sum_{i=-r}^{0} \alpha a_i v^i$. We claim that $\deg \alpha a_0 < \deg v$. Suppose the opposite. Then αa_0 can be represented in the form $\alpha a_0 = c_0 + c_1 v + \cdots + c_l v^l$, where $c_i \in \Sigma$, $l > 0$. Consequently, in order to represent the fraction $\alpha p/(\alpha q)$ in the form (5.11) we must divide the numerator and denominator by v^l. But then we obtain $|q_1|_v < |q|_v$; a contradiction. Thus, we have

$$\deg \alpha < \deg v - \max\{\deg a_0, \deg b_0\} = d \leqslant h.$$

Let R be the space of polynomials in $L[x]$ of degree less than d. If $\alpha \in U$, then we consider the fraction $\alpha p/(\alpha q)$ and represent it in the form (5.11). As a result we obtain a fraction p_1/q_1. Consider the column vector $\widehat{q}_1$. Since

$$\left|\beta - \frac{p_1}{q_1}\right|_v = \left|\beta - \frac{p}{q}\right|_v,$$

it follows that $\widehat{q}_1$ is a solution of (5.15) and therefore, $\widehat{q}_1 \in V$. We denote by W the set of all column vectors $\widehat{q}_1$ that can be obtained in this way, together with the zero column. Clearly, W is a subspace of V and $\dim W = d \leqslant h$. Consequently, W is a proper subspace of V.

Since U and W are proper subspaces of V, we have $V \setminus (U \cup W) \neq \varnothing$. Let $\widehat{q}_1 \in V \setminus (U \cup W)$. Consider the fraction p_1/q_1 corresponding to $\widehat{q}_1$. By construction we have $|q_1|_v = |q|_v$ and $p/q \neq p_1/q_1$ in the field $L(x)$. Then it follows from inequality (5.17) that

$$\left|\beta - \frac{p_1}{q_1}\right|_v \geqslant \left|\beta - \frac{p}{q}\right|_v.$$

This contradicts the fact that p/q is a best approximation to β.

Theorem 5.4 is proved.

Proposition 5.5. *If fractions a/b and c/d are best approximations to β such that $|b|_v = |d|_v$, then there exists a constant $h \in L^*$ such that $a = hc$ and $b = hd$.*

Proof. If $a/b \neq c/d$ in $L(x)$, then by the definition of a best approximation we have the inequalities

$$\left|\beta - \frac{a}{b}\right|_v > \left|\beta - \frac{c}{d}\right|_v, \qquad \left|\beta - \frac{a}{b}\right|_v < \left|\beta - \frac{c}{d}\right|_v;$$

a contradiction. Therefore, $a/b = c/d$ in $L(x)$. By taking into account the irreducibility of these fractions we obtain the required assertion.

Proposition 5.5 is proved.

Theorem 5.6. *Suppose that* $\deg v = 1$. *The following assertions hold*:

1) *the nth convergent* p_n/q_n *to* β *is a best approximation to* β;

2) *if a fraction* a/b *is a best approximation to* β, *then there exist a convergent* p_n/q_n *to* β *and a constant* $c \in L^*$ *such that* $a = cp_n$ *and* $b = cq_n$.

Proof. 1) Since

$$p_n = c_{-s}v^{-s} + \dots + c_0, \qquad q_n = d_{-r}v^{-r} + \dots + d_0,$$

where $c_i, d_i \in L$, it follows that p_n/q_n has the form (5.11). Inequality (5.7) and Theorem 5.4 now immediately imply that p_n/q_n is a best approximation to β.

2) First we prove that $|b|_v = |q_n|_v$ for some convergent p_n/q_n. Suppose the opposite. Since $|q_0|_v = |1|_v = 0$ and $|q_n|_v < |q_{n-1}|_v$ by (5.6), and $|b|_v \leqslant 0$, it follows that there exists n such that

$$|q_{n+1}|_v < |b|_v < |q_n|_v.$$

Since a/b is a best approximation to β and $|q_n|_v > |b|_v$, we have

$$\left|\beta - \frac{a}{b}\right|_v > \left|\beta - \frac{p_n}{q_n}\right|_v.$$

Then

$$\begin{aligned}\left|\frac{1}{bq_n}\right|_v \geqslant \left|\frac{p_n}{q_n} - \frac{a}{b}\right|_v = \left|\frac{p_n}{q_n} - \beta + \beta - \frac{a}{b}\right|_v = \left|\beta - \frac{p_n}{q_n}\right|_v \\ = |q_n\beta - p_n|_v - |q_n|_v = -|q_{n+1}|_v - |q_n|_v. \qquad (5.18)\end{aligned}$$

Hence, $-|b|_v \geqslant -|q_{n+1}|_v$, which contradicts the inequality $|q_{n+1}|_v < |b|_v$. Thus, $|q_n|_v = |b|_v$ for some n. By applying Proposition 5.5 we complete the proof of Theorem 5.6.

Theorem 5.6 is proved.

In the case $\deg v > 1$ the convergent p_n/q_n is not necessarily a best approximation to β.

Example 5.7. Let k, v, and d be the same as in Example 3.7. By expanding $\sqrt{d}$ into a continued fraction we obtain

$$a_0 = x, \quad a_1 = (x+1)v^{-1} + 1, \quad a_2 = v^{-1} + x + 1, \quad a_3 = (2x+1)v^{-1}, \quad \dots .$$

Then the convergents to $\sqrt{d}$ have the form

$$\frac{p_1}{q_1} = \frac{(x+2)v^{-1} + x + 2}{(x+1)v^{-1} + 1}, \qquad \frac{p_2}{q_2} = \frac{(x+2)v^{-2} + xv^{-1} + x + 2 + v}{(x+1)v^{-2} + (2x+1)v^{-1} + x}.$$

We claim that p_2/q_2 is not a best approximation to $\sqrt{d}$. By (5.7),

$$\left|\sqrt{d} - \frac{p_2}{q_2}\right|_v = -|a_3|_v - 2|q_2|_v = 5.$$

On the other hand, in order to write the convergent p_2/q_2 in the form (5.11) we need to divide the numerator and denominator by v:

$$\frac{p_2}{q_2} = \frac{\widetilde{p}_2}{\widetilde{q}_2} = \frac{(x+2)v^{-3} + xv^{-2} + (x+2)v^{-1} + 1}{(x+1)v^{-3} + (2x+1)v^{-2} + xv^{-1}}.$$

Then we have

$$\left|\sqrt{d} - \frac{\widetilde{p}_2}{\widetilde{q}_2}\right|_v = \left|\sqrt{d} - \frac{p_2}{q_2}\right|_v = 5 < -2|\widetilde{q}_2|_v = 6.$$

By Theorem 5.4, p_2/q_2 is not a best approximation to $\sqrt{d}$.

5.3. Continued fractions and S-units. In this subsection we again assume that $L = \mathbb{F}_q$ is a finite field of characteristic $p > 2$ and $k = \mathbb{F}_q(x)$. We show how continued fractions can be used for finding fundamental S-units in hyperelliptic fields.

Let $v \in \mathbb{F}_q[x]$ be an irreducible polynomial. Suppose that the valuation $|\cdot|_v$ has two non-equivalent extensions $|\cdot|_{v'}$ and $|\cdot|_{v''}$ to the field $K = k(\sqrt{d})$. Let $S = \{|\cdot|_\infty, |\cdot|_{v'}\}$. In the classical case of a quadratic extension $L = \mathbb{Q}(\sqrt{r})$, $r > 0$, of the field $\mathbb{Q}$, a fundamental unit of the field L can be found by using the expansion of $\sqrt{d}$ or $(\sqrt{d}-1)/2$ into a continued fraction (see [11], Ch. II, § 7). Our purpose is to show that in the case of the hyperelliptic field K and the valuation $|\cdot|_v$ defined by a linear polynomial v, a fundamental S-unit can be found by using the method of continued fractions.

Theorem 5.8. *Let $v \in \mathbb{F}_q(x)$ and $\deg v = 1$. Suppose that for some minimal positive integer m equation (3.1) has a solution in polynomials $f, g \in \mathbb{F}_q[x]$, $g \neq 0$. The following assertions hold.*

1. *If $m = 2t+1$, then f/g is a best approximation to $\sqrt{d}$. Thus, $f/g = p_n/q_n$ for some convergent p_n/q_n to $\sqrt{d}$.*

2. *If $m = 2t$, then there exists a divisor h of the polynomial d such that $\deg h < (1/2)\deg d$ and the equation*

$$\frac{d}{h}g_1^2 - hf_1^2 = bv^t, \tag{5.19}$$

where $b \in \mathbb{F}_q^*$, has a solution in polynomials $f_1, g_1 \in \mathbb{F}_q[x]$. Furthermore, f_1/g_1 is a best approximation to $\sqrt{d}/h$ and, consequently, $f_1/g_1 = p_n/q_n$ for some convergent p_n/q_n to $\sqrt{d}/h$. Conversely, if $f_1, g_1 \in \mathbb{F}_q[x]$ is a solution of (5.19), then f_1/g_1 is a best approximation to $\sqrt{d}/h$, $f_1/g_1 = p_n/q_n$ for some convergent p_n/q_n to $\sqrt{d}/h$, and the polynomials f and g defined by the formulae

$$f = \frac{1}{2}\left(hf_1^2 + \frac{d}{h}g_1^2\right), \qquad g = f_1g_1 \tag{5.20}$$

are a solution of equation (3.1).

Proof. 1. We write (3.1) in the form

$$(f - g\sqrt{d})(f + g\sqrt{d}) = av^{2t+1}.$$

By Proposition 2.1 we can assume that $|f+g\sqrt{d}|_{v'}=0$ and $|f-g\sqrt{d}|_{v'}=2t+1$. We expand f and g in powers of v:

$$f=b_0+b_1v+\cdots+b_rv^r, \qquad g=c_0+c_1v+\cdots+c_sv^s,$$

where $b_i, c_i \in \mathbb{F}_q$, $b_r \neq 0$, $c_s \neq 0$. A comparison of the degrees of the polynomials on the left- and right-hand sides of equation (3.1) shows that $r \leqslant t$ and $s \leqslant t$. Let $h=\max\{r,s\}$. Consider the element $\overline{f}-\overline{g}\sqrt{d}$, where

$$\overline{f}=\frac{f}{v^h}=b_0v^{-h}+\cdots+b_rv^{r-h}, \qquad \overline{g}=\frac{g}{v^h}=c_0v^{-h}+\cdots+c_sv^{s-h}.$$

Since $\overline{f}/\overline{g}$ has the form (5.11) and

$$|\overline{f}-\overline{g}\sqrt{d}|_{v'}=2t+1-h \geqslant t+1 > -|\overline{g}|_{v'}=t,$$

by Theorem 5.4 the fraction $\overline{f}/\overline{g}=f/g$ is a best approximation to $\sqrt{d}$. Then by Theorem 5.6 we have $f/g=p_n/q_n$ for some convergent p_n/q_n to $\sqrt{d}$.

2. Since a in equation (3.1) must be a square, after dividing both sides by a we can assume without loss of generality that f, g is a solution of the norm equation $f^2-g^2d=v^{2t}$. Hence we obtain

$$(f-v^t)(f+v^t)=g^2d. \tag{5.21}$$

Let $d=d_1d_2\cdots d_r$ be the factorization of d into irreducible factors over $\mathbb{F}_q$. Then each polynomial d_i divides exactly one of the factors: $f-v^t$ or $f+v^t$. Otherwise we would have d_i dividing v^t and therefore $d_i=cv$, where $c \in \mathbb{F}_q^*$. But then v divides d, which is not the case.

Let h_1 be the product of those d_i that divide $f-v^t$, and h_2 the product of those d_i that divide $f+v^t$. Then $h_1h_2=d$ and $(h_1,h_2)=1$. For definiteness suppose that $\deg h_1 < \deg h_2$, that is, $\deg h_1 < (1/2)\deg d$. We write

$$f-v^t=h_1u_1, \qquad f+v^t=h_2u_2. \tag{5.22}$$

From (5.22) we obtain

$$f=\frac{1}{2}(h_1u_1+h_2u_2), \qquad v^t=\frac{1}{2}(h_2u_2-h_1u_1). \tag{5.23}$$

By substituting (5.22) into (5.21), we obtain $u_1u_2=g^2$. Note that $(u_1,u_2)=1$ (otherwise f and g would not be coprime). Then $u_1=f_1^2$ and $u_2=g_1^2$. Thus,

$$f=\frac{1}{2}(h_1f_1^2+h_2g_1^2), \qquad g=f_1g_1. \tag{5.24}$$

From (5.23), (5.24) we obtain

$$2v^t=\frac{d}{h_1}g_1^2-h_1f_1^2. \tag{5.25}$$

Thus, equation (3.1) has a solution in polynomials $f,g \in \mathbb{F}_q[x]$ if and only if equation (5.25) has a solution in polynomials $f_1,g_1 \in \mathbb{F}_q[x]$ for some divisor h_1 of the polynomial d such that $\deg h_1 < (1/2)\deg d$.

We now prove that the fraction f_1/g_1 is a best approximation to the fraction $\sqrt{d}/h_1$. By the minimality of $m = 2t$ we have $\deg h_1 \geqslant 1$. We consider in more detail equation (5.25). We write it in the form

$$h_1\left(\frac{\sqrt{d}}{h_1}g_1 - f_1\right)\left(\frac{\sqrt{d}}{h_1}g_1 + f_1\right) = 2v^t. \tag{5.26}$$

Since $|h_1|_{v'} = 0$ and $|\sqrt{d}|_{v'} = 0$, by Proposition 2.1 we can assume that

$$\left|\frac{\sqrt{d}}{h_1}g_1 + f_1\right|_{v'} = 0, \qquad \left|\frac{\sqrt{d}}{h_1}g_1 - f_1\right|_{v'} = t.$$

We expand f_1 and g_1 in powers of v:

$$f_1 = b_0 + b_1 v + \dots + b_r v^r, \qquad g_1 = c_0 + c_1 v + \dots + c_s v^s,$$

where $b_i, c_i \in \mathbb{F}_q$, $b_r \neq 0$, $c_s \neq 0$. By comparing the degrees on the left- and right-hand sides of equation (5.25), we obtain $r < t/2$ and $s < t/2$. Let $h = \max\{r, s\}$. Consider the element $(\sqrt{d}/h_1)\overline{g}_1 - \overline{f}_1$, where

$$\overline{f}_1 = \frac{f_1}{v^h}, \qquad \overline{g}_1 = \frac{g_1}{v^h}.$$

Since $\overline{f}_1/\overline{g}_1$ has the form (5.11) and

$$\left|\frac{\sqrt{d}}{h_1}\overline{g}_1 - \overline{f}_1\right|_{v'} = t - h > h = -|\overline{g}_1|_{v'},$$

by Theorem 5.4 the fraction $\overline{f}_1/\overline{g}_1 = f_1/g_1$ is a best approximation to $\sqrt{d}/h_1$. Then by Theorem 5.6 we have $f_1/g_1 = p_n/q_n$ for some convergent p_n/q_n to $\sqrt{d}/h$.

Theorem 5.8 is proved.

We point out that Theorem 5.8 becomes false in the case $\deg v > 1$. We turn to Examples 3.7 and 5.7 considered above. The element $\varepsilon = f + g\sqrt{d}$, where $f = 2x^5 + 2x^3 + 1$ and $g = x$, is a fundamental S-unit. It is easy to verify that $f/g \neq p_1/q_1$ and $f/g \neq p_2/q_2$. A fortiori, f/g does not coincide with any convergent p_n/q_n to $\sqrt{d}$ for $n > 2$, since the degree of the denominator is always greater than 1.

Theorem 5.8 gives an algorithm for calculating a fundamental S-unit in the case $\deg v = 1$. Let $d_1, \dots, d_r$ be all the divisors of the polynomial d of degree at most $(1/2)\deg d$. We calculate consecutively the convergents to $\sqrt{d}$, $\sqrt{d}/d_1, \dots, \sqrt{d}/d_r$ and, for each convergent p_n/q_n, verify whether equation (5.19) holds. As soon as we find a convergent p_n/q_n satisfying (5.19), by formulae (5.20) we find a solution f, g of the norm equation (3.1). Then either $f + g\sqrt{d}$ or $f - g\sqrt{d}$ is a fundamental S-unit.

Bibliography

[1] V. V. Benyash-Krivets and V. P. Platonov, "S-units in hyperelliptic fields", *Uspekhi Mat. Nauk* **62**:4 (2007), 149–150; English transl. in *Russian Math. Surveys* **62**:4 (2007), 784–786.

[2] V. V. Benyash-Krivets and V. P. Platonov, "Groups of S-units in hyperelliptic fields", *Dokl. Ross. Akad. Nauk* **417**:4 (2007), 446–450; English transl. in *Dokl. Math.* **76**:3 (2007), 886–890.

[3] V. V. Benyash-Krivets and V. P. Platonov, "Continued fractions and S-units in hyperelliptic fields", *Uspekhi Mat. Nauk* **63**:2 (2008), 159–160; English transl. in *Russian Math. Surveys* **63**:2 (2008), 357–359.

[4] V. V. Benyash-Krivets and V. P. Platonov, "Continued fractions and S-units in function fields", *Dokl. Ross. Akad. Nauk* **423**:2 (2008), 155–160; English transl. in *Dokl. Math.* **78**:3 (2008), 833–838.

[5] A. Weil, *Basic number theory*, Springer-Verlag, New York 1967.

[6] I. S. Iokhvidov, *Hankel and Toeplitz matrices and forms. Algebraic theory*, Nauka, Moscow 1974; English transl., Birkhäuser, Boston–Basel–Stuttgart 1982.

[7] A. Böttcher and K. Rost, "Topics in the numerical linear algebra of Toeplitz and Hankel matrices", *GAMM Mitt. Ges. Angew. Math. Mech.* **27**:2 (2004), 174–188.

[8] E. Artin, "Quadratische Körper im Gebiete der höheren Kongruenzen. I", *Math. Z.* **19**:1 (1924), 153–206.

[9] S. Lang, *Introduction to diophantine approximations*, Addison-Wesley, Reading, MA–London–Don Mills, ON 1966.

[10] W. W. Adams and M. J. Razar, "Multiples of points on elliptic curves and continued fractions", *Proc. London Math. Soc.* (3) **41**:3 (1980), 481–498.

[11] A. I. Borevich and I. R. Shafarevich, *Number theory*, Nauka, Moscow 1964; English transl., Academic Press, New York–London 1966.

V. V. Benyash-Krivets
Belarusian State University, Minsk
E-mail: benyash@bsu.by

Received 10/JUN/09
Translated by E. KHUKHRO

V. P. Platonov
Scientific Research Institute for System Studies
of Russian Academy of Sciences, Moscow
E-mail: platonov@niisi.ras.ru