УДК 511.6

В. В. Беняш-Кривец, В. П. Платонов

Группы S-единиц в гиперэллиптических полях и непрерывные дроби

Найдены новые методы вычисления фундаментальных S-единиц в гиперэллиптических полях. Исследованы непрерывные дроби в функциональных полях. В качестве применения доказано, что если нормирование задается линейным многочленом, то фундаментальная S-единица в гиперэллиптическом поле может быть найдена при помощи разложения некоторых элементов в непрерывные дроби.

Библиография: 11 названий.

Ключевые слова: S-единицы, нормирования, гиперэллиптические поля, непрерывные дроби, наилучшие приближения.

§ 1. Введение

В работах [1]–[4] представлен ряд результатов, связанных с решением проблемы вычисления групп S-единиц в гиперэллиптических полях, развитием теории непрерывных дробей в функциональных полях и их связей с вычислением фундаментальных S-единиц.

Настоящая статья содержит расширенное изложение результатов, анонсированных в [1]–[4].

Предлагаются два новых метода вычисления фундаментальных S-единиц в гиперэллиптических полях.

Первый метод базируется на новой эффективной процедуре линеаризации поиска решений естественного норменного уравнения. В важном для применений эллиптическом случае, когда нормирования из S индуцируются точками на эллиптической кривой, обнаружена новая интересная связь с ганкелевыми матрицами.

Второй метод имеет иную природу. Вначале мы получаем некоторые результаты о непрерывных дробях в функциональных полях, которые представляют определенный независимый интерес, а затем применяем их для решения норменного уравнения. В том случае, когда нормирования из S задаются линейными многочленами, метод непрерывных дробей дает самые быстрые алгоритмы вычисления фундаментальных S-единиц. Однако в отличие от первого метода метод непрерывных дробей утрачивает свою эффективность в случае, когда S содержит нормирования более общего характера.

Пусть $k = \mathbb{F}_q(x)$ – поле рациональных функций от одной переменной над конечным полем $\mathbb{F}_q$ характеристики $p > 2$. Для неприводимого многочлена

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (гранты № 09-01-00287 и № 09-01-12169).

$v \in \mathbb{F}_q[x]$ через $|\cdot|_v$ будем обозначать нормирование поля k, задаваемое равенством

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

где $a, b \in \mathbb{F}_q[x]$, $v \nmid a$, $v \nmid b$. Через $|\cdot|_\infty$ будем обозначать нормирование $|a/b|_\infty = \deg b - \deg a$.

Обозначим через $\mathscr{O}_v = \bigl\{z \in k \bigm| |z|_v \geqslant 0\bigr\}$ кольцо нормирования $|\cdot|_v$, а через $\mathfrak{p}_v = \bigl\{z \in k \bigm| |z|_v > 0\bigr\}$ – идеал нормирования $|\cdot|_v$. Тогда поле вычетов $k_v = \mathscr{O}_v/\mathfrak{p}_v$ совпадает с $\mathbb{F}_p[x]/(v)$ и является конечным расширением $\mathbb{F}_p$. Пусть $\overline{k}$ – пополнение поля k относительно нормирования $|\cdot|_v$. Продолжение нормирования $|\cdot|_v$ на $\overline{k}$ по-прежнему будем обозначать через $|\cdot|_v$. Выберем в $\mathbb{F}_q[x]$ фиксированную систему Σ представителей смежных классов по идеалу (v), состоящую из всех многочленов степени, меньшей чем $\deg v$. Тогда каждый элемент $z \in \overline{k}$ единственным образом можно представить в виде формального степенного ряда:

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

где $a_i \in \Sigma$. Если $\deg v = 1$, то поле $\overline{k}$ можно отождествить с полем формальных степенных рядов $\mathbb{F}_q((v))$.

Пусть

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

– свободный от квадратов многочлен с $a_0 \neq 0$, $K = k(\sqrt{d})$, и пусть $\overline{x}$ – образ x в поле вычетов k_v. Если $d(\overline{x}) = \beta^2$ для некоторого $0 \neq \beta \in k_v$ (а это означает, что точка $(\overline{x}, \beta)$ является k_v-точкой гиперэллиптической кривой $y^2 = d(x)$), то нормирование $|\cdot|_v$ имеет два неэквивалентных продолжения на поле K. Эти нормирования будем обозначать $|\cdot|_{v'}$ и $|\cdot|_{v''}$. Отметим, что в этом случае $v \nmid d$, $\sqrt{d} \in \overline{k}$ и $|f + g\sqrt{d}|_{v'} = |f - g\sqrt{d}|_{v''}$ для элемента $f + g\sqrt{d} \in K$. Если же $d(\overline{x}) = 0$ либо $d(\overline{x}) \neq 0$ и $d(\overline{x})$ не является квадратом в k_v, то нормирование $|\cdot|_v$ имеет единственное продолжение на поле K. Это продолжение, чтобы не усложнять обозначения, мы по-прежнему будем обозначать $|\cdot|_v$. В этом случае мы имеем $|f + g\sqrt{d}|_v = (1/2)|f^2 - g^2 d|_v$ для элемента $f + g\sqrt{d} \in K$. Так как многочлен $d(x)$ имеет нечетную степень, то нормирование $|\cdot|_\infty$ имеет единственное продолжение на K, и мы также будем обозначать его через $|\cdot|_\infty$.

Пусть S – произвольное конечное множество неэквивалентных нормирований поля K, содержащее $|\cdot|_\infty$, а $S_1 = \{|\cdot|_\infty, |\cdot|_{v_1}, \dots, |\cdot|_{v_t}\}$ – множество ограничений нормирований из S на поле k. Обозначим через $\mathscr{O}_S$ кольцо S-целых элементов в K, т.е. таких элементов $z \in K$, что $|z|_v \geqslant 0$ для всех нормирований $|\cdot|_v$ поля K, не принадлежащих множеству S. Множество обратимых элементов U_S кольца $\mathscr{O}_S$ называется *группой S-единиц поля K*. В силу обобщенной теоремы Дирихле о единицах (см. [5; гл. IV, теорема 9]) группа U_S является прямым произведением группы $\mathbb{F}_q^*$ и свободной абелевой группы G ранга $|S| - 1$. Независимые образующие группы G называются *фундаментальными S-единицами*.

§ 2. Некоторые свойства S-единиц

Пусть S – произвольное конечное множество неэквивалентных нормирований поля K, содержащее $|\cdot|_\infty$, $s=|S|-1$ и $S_1=\{|\cdot|_\infty, |\cdot|_{v_1},\dots,|\cdot|_{v_t}\}$ – множество ограничений нормирований из S на поле k.

Предложение 2.1. *Пусть $y=f+g\sqrt{d}$, где $f,g\in\mathbb{F}_q[x]$, $f\neq 0$, $g\neq 0$, $(f,g)=1$, и пусть $v\in\mathbb{F}_q[x]$ – неприводимый многочлен. Тогда справедливы следующие утверждения.*

1. *Если $|\cdot|_v$ имеет два продолжения $|\cdot|_{v'}$ и $|\cdot|_{v''}$ на K, то либо $|y|_{v'}=0$, либо $|y|_{v''}=0$.*

2. *Если $v\nmid d$ и $|\cdot|_v$ имеет единственное продолжение на K, то $|y|_v=0$.*

3. *Если $v\mid d$, то $|\cdot|_v$ имеет единственное продолжение на K. В этом случае если $v\nmid f$, то $|y|_v=0$. Если $v\mid f$, то $|y|_v=1/2$.*

Доказательство. 1. Так как $|\cdot|_v$ имеет два продолжения на K, то $v\nmid d$ и $\sqrt{d}\in\overline{k}$. Пусть в пополнении $\overline{k}$ элементы f, g и $\sqrt{d}$ представлены в виде формальных степенных рядов:

$$f=\sum_{i=0}^{r}f_iv^i,\qquad g=\sum_{i=0}^{s}g_iv^i,\qquad \sqrt{d}=\sum_{i=0}^{\infty}d_iv^i,\tag{2.1}$$

где $f_i,g_i,d_i\in\Sigma$. Допустим, что $|y|_{v'}>0$ и $|y|_{v''}>0$. Так как $|f+g\sqrt{d}|_{v''}=|f-g\sqrt{d}|_{v'}$, то мы получаем

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

Заметим, что

$$f+g\sqrt{d}=\sum_{i=0}^{\infty}h_iv^i,\qquad f-g\sqrt{d}=\sum_{i=0}^{\infty}t_iv^i,$$

где $h_i,t_i\in\Sigma$ и h_0, t_0 – остатки от деления $f_0+g_0d_0$ и $f_0-g_0d_0$ на v. Из неравенств (2.2) следует, что $h_0=t_0=0$. Поэтому v делит f_0. Так как $\deg f_0<\deg v$, то $f_0=0$. Теперь получаем, что v делит g_0d_0. Так как $v\nmid d$, то $d_0\neq 0$ и v не делит d_0. Значит, v делит g_0, откуда $g_0=0$. Таким образом, $v\mid f$ и $v\mid g$, что противоречит взаимной простоте f и g.

2. Пусть $d=\sum_{i=0}^{m}h_iv^i$, где $h_i\in\Sigma$ и $h_0\neq 0$ по условию. Так как $|\cdot|_v$ имеет одно продолжение на K, то образ h_0 в поле вычетов k_v не является квадратом. Тогда

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

Пусть в пополнении $\overline{k}$ элементы f, g, $\sqrt{d}$ представлены в виде формальных степенных рядов (2.1). Запишем

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

где $q_i\in\Sigma$ и q_0 – остаток от деления $f_0^2-g_0^2h_0$ на v. Заметим, что $q_0\neq 0$, поскольку в противном случае h_0 было бы квадратом в поле вычетов k_v. Таким образом, v не делит f^2-g^2d и $|y|_v=0$.

3. Поскольку $v \mid d$ и d – свободный от квадратов многочлен, то $|\cdot|_v$ имеет единственное продолжение на K. Тогда

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

Если v не делит f, то v не делит $f^2 - g^2 d$ и, следовательно, $|y|_v = 0$.

Предположим теперь, что $f = vf_1$, $d = vd_1$. Тогда v не делит d_1 и по условию v не делит g. Тогда мы имеем

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

поскольку v не делит $f_1^2 v - g^2 d_1$.

Предложение 2.1 доказано.

Следующее предложение характеризует S-целые элементы в K.

Предложение 2.2. *Любой элемент $y \in \mathscr{O}_S$ имеет вид*

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

где $f, g \in \mathbb{F}_q[x]$, $v_j \in S_1$ и $m_j \geqslant 0$. При этом если $m_j > 0$ и нормирование $|\cdot|_{v_j}$ имеет два продолжения на K, из которых одно не принадлежит S, то v_j не делит f и v_j не делит g.

Доказательство. Пусть $y = (f + g\sqrt{d})/h$, где $f, g, h \in \mathbb{F}_q[x]$. Допустим, что $h = v^r h_1$, где v – неприводимый многочлен, не принадлежащий S_1, и $r > 0$. Без ограничения общности мы можем считать, что v не делит одновременно f и g. В силу предложения 2.1

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

для некоторого продолжения $|\cdot|_{v'}$ нормирования $|\cdot|_v$. Следовательно, $h \notin \mathscr{O}_S$.

Пусть теперь $m_j > 0$ и нормирование $|\cdot|_{v_j}$ имеет два продолжения $|\cdot|_{v_j'}$ и $|\cdot|_{v_j''}$ на K, из которых $|\cdot|_{v_j'}$ не принадлежит S. Тогда $v_j \nmid d$. Без ограничения общности мы можем считать, что v_j не делит одновременно f и g (в противном случае числитель и знаменатель можно сократить на v_j). Допустим, что $v_j \mid f$ и $v_j \nmid g$. Тогда v_j не делит $f^2 - g^2 d$. Следовательно,

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

откуда $|f + g\sqrt{d}|_{v_j'} = 0$. Таким образом, $|y|_{v_j'} = -m_j < 0$ – противоречие с тем, что $y \in \mathscr{O}_S$.

Предложение 2.2 доказано.

Отметим, что не любой элемент вида $y = (f + g\sqrt{d})/(v_1^{m_1} \cdots v_t^{m_t})$ является S-целым. Например, если нормирование $|\cdot|_{v_j} \in S_1$ имеет два продолжения на K и $|\cdot|_{v_j'}$ не принадлежит S, то элемент $1/v_j$ не является S-целым.

Обозначим через $N_{K/k}$ норменное отображение из K в k. Для дальнейшего нам важно знать, какие значения может принимать норменное отображение на S-единицах.

Предложение 2.3. *Если* $\varepsilon \in U_S$, *то* $N_{K/k}(\varepsilon) = av_1^{r_1}\cdots v_t^{r_t}$, *где* $a \in \mathbb{F}_q^*$ *и* $r_i \in \mathbb{Z}$.

Доказательство. В силу предложения 2.2

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

Тогда $N_{K/k}(\varepsilon) = (f^2 - g^2 d)v_1^{-2m_1}\cdots v_t^{-2m_t}$. Предположим, что $f^2 - g^2 d = u^s h$, где $u, h \in \mathbb{F}_q[x]$, $u \notin S_1$ – неприводимый многочлен, $s > 0$ и u не делит h. Тогда

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

Так как $\varepsilon^{-1} \in \mathscr{O}_S$, то в силу предложения 2.2 u^s делит f и g. Но тогда u^{2s} делит $f^2 - g^2 d$ – противоречие.

Предложение 2.3 доказано.

Как и в случае S-целых элементов, если элемент $\varepsilon \in K$ обладает свойством $N_{K/k}(\varepsilon) = av_1^{m_1}\cdots v_t^{m_t}$, то из этого не следует, что ε является S-единицей. Например, если нормирование $|\cdot|_{v_j}$ имеет два продолжения на K и $|\cdot|_{v_j'}$ не принадлежит S, то $N_{K/k}(v_j) = v_j^2$, однако v_j не является S-единицей.

Если $\varepsilon = (f + g\sqrt{d})/(v_1^{r_1}\cdots v_t^{r_t}) \in U_S$, то из предложения 2.3 следует, что

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

где $a \in \mathbb{F}_q^*$ и $m_1, \dots, m_t$ – неотрицательные целые числа. Следующее предложение показывает, что если норменное уравнение (2.3) при фиксированных $m_1, \dots, m_t$ имеет решение в многочленах $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, то мы легко можем построить некоторую S-единицу.

Предложение 2.4. *Пусть* $z = f + g\sqrt{d} \in K$, *где* $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, *и пусть*

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

где $a \in \mathbb{F}_q^*$, $m_i \geqslant 0$. *Обозначим через* $S_2 = \{|\cdot|_{v_1}, \dots, |\cdot|_{v_r}\}$ *множество таких нормирований из* S_1, *для которых выполнены следующие условия*:

1) $|\cdot|_{v_i}$ *имеет два продолжения* $|\cdot|_{v_i'}$ *и* $|\cdot|_{v_i''}$ *на* K;
2) $|\cdot|_{v_i''} \notin S$;
3) $|z|_{v_i''} > 0$.

Тогда $\varepsilon = z/(v_1^{m_1}\cdots v_r^{m_r}) \in U_S$. *Если* S_2 – *пустое множество, то* z *является* S-*единицей.*

Доказательство. Докажем, что $\varepsilon \in \mathscr{O}_S$. Для произвольного нормирования $|\cdot|_{v_i}$, $1 \leqslant i \leqslant r$, мы имеем

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

по построению множества S_2. Так как $|f + g\sqrt{d}|_{v_i''} > 0$, то по предложению 2.1 $|f - g\sqrt{d}|_{v_i''} = 0$, и тогда $|f + g\sqrt{d}|_{v_i''} = m_i$. Следовательно, $|\varepsilon|_{v_i''} = m_i - m_i = 0$, $i = 1, \dots, r$. Значит, $\varepsilon \in \mathscr{O}_S$.

Далее,

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

Предположим, что нормирование $|\cdot|_{v_i}$, $r+1 \leqslant i \leqslant t$, имеет два продолжения на K и $|\cdot|_{v_i''} \notin S$. Тогда по условию $|z|_{v_i''} = 0$ и из (2.4) получаем $|f - g\sqrt{d}|_{v_i''} = m_i$. Следовательно, $|\varepsilon^{-1}|_{v_i''} = m_i - m_i = 0$ и $\varepsilon^{-1} \in \mathscr{O}_S$.

Предложение 2.4 доказано.

Рассмотрим теперь следующий естественный вопрос: как расширится система независимых фундаментальных S-единиц, если мы к множеству S добавим новое нормирование $|\cdot|_v$? Ответ на него дает следующая теорема.

Теорема 2.5. *Пусть $\varepsilon_1, \dots, \varepsilon_s$ – независимые фундаментальные S-единицы поля K и $v \in \mathbb{F}_q[x]$ – такой неприводимый многочлен, что хотя бы одно из продолжений нормирования $|\cdot|_v$ на K не принадлежит S. Тогда справедливы следующие утверждения.*

1. *Предположим, что нормирование $|\cdot|_v$ имеет два продолжения $|\cdot|_{v'}$ и $|\cdot|_{v''}$ на K. Пусть при этом $|\cdot|_{v'} \in S$, $|\cdot|_{v''} \notin S$. Положим $S' = S \cup \{|\cdot|_{v''}\}$. Тогда $\varepsilon_1, \dots, \varepsilon_s, v$ – система независимых фундаментальных S'-единиц.*

2. *Предположим, что нормирование $|\cdot|_v$ имеет два продолжения $|\cdot|_{v'}$ и $|\cdot|_{v''}$ на K, которые не принадлежат S. Положим $S' = S \cup \{|\cdot|_{v'}\}$. Предположим, что ε – такая S'-единица, что*

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

с наименьшим возможным натуральным показателем m_{t+1}. Тогда $\varepsilon_1, \dots, \varepsilon_s$, ε – система независимых фундаментальных S'-единиц.

3. *Предположим, что нормирование $|\cdot|_v$ имеет единственное продолжение на K. Пусть $S' = S \cup \{|\cdot|_v\}$. Если $d/v \notin \mathbb{F}_q$, то $\varepsilon_1, \dots, \varepsilon_s, v$ – система независимых фундаментальных S'-единиц. Если же $d/v \in \mathbb{F}_q$, то $\varepsilon_1, \dots, \varepsilon_s, \sqrt{d}$ – система независимых фундаментальных S'-единиц.*

Доказательство. 1. Предположим, что единицы $\varepsilon_1, \dots, \varepsilon_s, v$ зависимы. Тогда $\varepsilon_1^{m_1} \cdots \varepsilon_s^{m_s} v^m = 1$, где $m_i \in \mathbb{Z}$ и $m \neq 0$. Следовательно, $v^m \in U_S$, однако $|v^m|_{v''} = m \neq 0$ – противоречие.

Пусть $\varepsilon_1, \dots, \varepsilon_s, \varepsilon_{s+1}$ – система независимых фундаментальных S'-единиц. Тогда

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

где $a \in \mathbb{F}_q^*$, $r_i \in \mathbb{Z}$ и $r_{s+1} \neq 0$, поскольку $v \notin U_S$. Так как $\varepsilon_i \in U_S$ для $i = 1, \dots, s$, то $|\varepsilon_i|_{v''} = 0$. Из (2.5) получаем $1 = |v|_{v''} = r_{s+1}|\varepsilon_{s+1}|_{v''}$, откуда $r_{s+1} = \pm 1$. Таким образом, учитывая (2.5), фундаментальную S'-единицу ε_{s+1} можно заменить на v.

2. Покажем, что единицы $\varepsilon_1, \dots, \varepsilon_s, \varepsilon$ независимы. Если $\varepsilon_1^{r_1} \cdots \varepsilon_s^{r_s} v^r = 1$, где $r_i \in \mathbb{Z}$ и $r \neq 0$, то $\varepsilon^r \in U_S$. Значит, $|\varepsilon^r|_{v'} = r|\varepsilon|_{v'} = 0$, откуда $|\varepsilon|_{v'} = 0$. Аналогично, $|\varepsilon|_{v''} = 0$. Следовательно, $\varepsilon \in U_S$ – противоречие с предложением 2.3.

Пусть $\varepsilon_1, \dots, \varepsilon_s, \varepsilon_{s+1}$ – система независимых фундаментальных S'-единиц. Покажем, что ε_{s+1} можно заменить на ε. Пусть

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

где $a \in \mathbb{F}_q^*$, $m_i \in \mathbb{Z}$ и $m_{s+1} \neq 0$. Пусть $N_{K/k}(\varepsilon_{s+1}) = bv_1^{k_1} \cdots v_t^{k_t} v^{k_{t+1}}$, где $b \in \mathbb{F}_q$. Заметим, что по предложению 2.3 $N_{K/k}(\varepsilon_i) = cv_1^{i_1} \cdots v_t^{i_t}$ при $i = 1, \ldots, s$. Вычислим нормы левой и правой частей в (2.6) и сравним показатели, с которыми v входит в левую и правую части. Получим

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

Так как по условию $|k_{t+1}| \geqslant m_{t+1}$, то $r_{s+1} = \pm 1$, и мы можем, используя (2.6), заменить ε_{s+1} на ε.

3. Если $d/v \notin \mathbb{F}_q$, то доказательство полностью аналогично п. 1. Пусть $d/v \in \mathbb{F}_q$. Как и в п. 1, легко показать, что $\varepsilon_1, \ldots, \varepsilon_s, \sqrt{d}$ – независимые S'-единицы. Пусть $\varepsilon_1, \ldots, \varepsilon_s, \varepsilon_{s+1}$ – система независимых фундаментальных S'-единиц. Как и в п. 2, доказываем, что ε_{s+1} можно заменить на $\sqrt{d}$.

Теорема 2.5 доказана.

Из теоремы 2.5 следует, что ключевым случаем для нахождения системы независимых фундаментальных S-единиц является следующий. Пусть $v_1, \ldots, v_t \in \mathbb{F}_q[x]$ – такие неприводимые многочлены, что каждое из нормирований $|\cdot|_{v_i}$ имеет два продолжения $|\cdot|_{v_i'}$ и $|\cdot|_{v_i''}$ на K. В качестве множества S возьмем следующее множество нормирований: $S = \{|\cdot|_\infty, |\cdot|_{v_1'}, \ldots, |\cdot|_{v_t'}\}$, т.е. из двух продолжений нормирования $|\cdot|_{v_i}$ на K в S мы включаем ровно одно. Далее мы по отдельности рассмотрим случаи, когда S содержит два элемента и когда S содержит более двух элементов.

§ 3. Случай $|S| = 2$

3.1. Общий случай. Пусть $S = \{|\cdot|_\infty, |\cdot|_{v'}\}$ и $\varepsilon \in U_S$. Тогда по предложению 2.2 $\varepsilon = (f + g\sqrt{d})/v^k$ и по предложению 2.3 $N_{K/k}(\varepsilon) = av^s$, где $a \in \mathbb{F}_q^*$. Следовательно, $N_{K/k}(f + g\sqrt{d}) = f^2 - g^2 d = av^m$ для некоторого натурального m.

Предложение 3.1. *Предположим, что m – такое минимальное натуральное число, что норменное уравнение*

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

где $a \in \mathbb{F}_q^*$, имеет решение в многочленах $f, g \in \mathbb{F}_q[x]$, $g \neq 0$. Тогда либо $f + g\sqrt{d}$, либо $f - g\sqrt{d}$ является фундаментальной S-единицей.

Доказательство. В силу предложения 2.1 либо $|f + g\sqrt{d}|_{v''} = 0$, либо $|f - g\sqrt{d}|_{v''} = 0$. Это означает, что либо $f + g\sqrt{d}$, либо $f - g\sqrt{d}$ является S-единицей. Пусть, например, $f + g\sqrt{d} \in U_S$, и пусть ε – фундаментальная S-единица. Тогда в силу предложения 2.3 $N_{K/k}(\varepsilon) = bv^k$, где $b \in \mathbb{F}_q^*$. При этом мы можем считать, что $k > 0$, заменяя при необходимости ε на ε^{-1}. Тогда $k \geqslant m$ по условию предложения. Имеем

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

где $c \in \mathbb{F}_q^*$. Рассматривая нормы обеих частей, получаем равенство $v^m = v^{rk}$, откуда $m = rk$. Следовательно, $r = 1$ и $f + g\sqrt{d} = c\varepsilon$.

Предложение 3.1 доказано.

Далее мы предлагаем метод решения норменного уравнения (3.1). Каждый элемент из пополнения $\overline{k}$ можно представить в виде формального степенного ряда с коэффициентами из Σ. Однако в случае $\deg v > 1$ произведению двух элементов из пополнения $\overline{k}$ не соответствует обычное произведение соответствующих формальных степенных рядов. Дело в том, что при умножении формальных степенных рядов коэффициенты произведения могут быть многочленами степени $\geqslant \deg v$. Поэтому полученный формальный степенной ряд нам нужно переписать в таком виде, чтобы все коэффициенты принадлежали Σ (т.е. проделать операцию "переноса цифр"). Введем следующее обозначение. Если $f(x) = f_0 + f_1x + \cdots + f_rx^r \in \mathbb{F}_q[x]$, то через $\widehat{f} = (f_0, \ldots, f_r)^t$ будем обозначать вектор-столбец коэффициентов f. Справедливо следующее предложение.

Предложение 3.2. *Пусть $v(x) = v_0 + v_1x + \cdots + v_hx^h$, $v_h \neq 0$, – фиксированный неприводимый многочлен, и пусть $a(x) = a_0 + a_1x + \cdots + a_{h-1}x^{h-1}$, $b(x) = b_0 + b_1x + \cdots + b_{h-1}x^{h-1}$ – многочлены из $\mathbb{F}_q[x]$. Разделим ab на v с остатком: $ab = gv + r$, где $g = g_0 + g_1x + \cdots + g_{h-2}x^{h-2}$, $r = r_0 + r_1x + \cdots + r_{h-1}x^{h-1}$. Тогда существуют $(h \times h)$-матрицы $A_v(a)$ и $B_v(a)$, коэффициенты которых являются линейными функциями от $a_0, \ldots, a_{h-1}$ с коэффициентами из $\mathbb{F}_q$, такие, что*

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

Замечание. В равенстве (3.2) мы добавляем 0 к столбцу $\widehat{g}$ для того, чтобы матрицы $A_v(a)$ и $B_v(a)$ имели одинаковые размеры, что удобно для дальнейших вычислений.

Доказательство предложения 3.2. Пусть $\overline{a}$, $\overline{b}$, $\overline{r}$, $\overline{x}$ – образы a, b, r, x в поле вычетов k_v. Тогда $\overline{a}\overline{b} = \overline{r}$. Пусть φ – линейный оператор на k_v, заданный посредством $z \mapsto az$, и пусть $A_v(a)$ – матрица оператора φ в базисе $1, \overline{x}, \ldots, \overline{x}^{h-1}$. Тогда мы имеем $\widehat{r} = A_v(a)\widehat{b}$.

Для нахождения матрицы $B_v(a)$ рассмотрим равенство $ab = gv + r$. Сравнивая коэффициенты при $x^h, \ldots, x^{2h-2}$ в левой и правой частях данного равенства, получаем

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

Эту систему из $h-1$ равенств можно записать в матричном виде

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

где

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

Следовательно, $\widehat{g} = T_1^{-1}T_2\widehat{b}$. Полагая $B_v(a) = \left(\begin{smallmatrix} 0 & T_1^{-1}T_2 \\ 0 & 0 \end{smallmatrix}\right)$, получаем второе из равенств (3.2).

Предложение 3.2 доказано.

Матрица $B_v(a)$ из предложения 3.2 отвечает за "переносы цифр" при умножении формальных степенных рядов. Из предложения 3.2 легко получить следующее предложение.

Предложение 3.3. *Пусть* $u_1 = \sum_{i=s_1}^{\infty} a_i v^i$, $u_2 = \sum_{i=s_2}^{\infty} b_i v^i$ *– два элемента из пополнения* $\overline{k}$. *Положим* $C_v(a_{s_1}) = A_v(a_{s_1})$ *и* $C_v(a_i) = A_v(a_i) + B_v(a_{i-1})$ *при* $i > s_1$. *Тогда* $u_1 u_2 = \sum_{j=s_1+s_2}^{\infty} L_j v^j$, *где*

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

Доказательство. Запишем произведение $u_1 u_2$ в виде

$$u_1 u_2 = \sum_{j=s_1+s_2}^{\infty} M_j v^j,$$

где $M_j = \sum_{i+s=j} a_i b_s$. Разделим $a_i b_s$ на v с остатком: $a_i b_s = g_{is} v + r_{is}$. Тогда

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

где $M_j' = \sum_{i+s=j} g_{is}$, $M_j'' = \sum_{i+s=j} r_{is}$. Следовательно,

$$u_1 u_2 = M_{s_1+s_2}'' v^{s_1+s_2} + \sum_{j=s_1+s_2+1}^{\infty} (M_{j-1}' + M_j'') v^j,$$

где $M_{s_1+s_2}'', M_{j-1}' + M_j'' \in \Sigma$. Значит,

$$L_j = \begin{cases} M_{s_1+s_2}'', & \text{если } j = s_1 + s_2, \\ M_{j-1}' + M_j'', & \text{если } j > s_1 + s_2. \end{cases}$$

Из предложения 3.2 следует, что

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

При $j = s_1 + s_2$ получаем

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

поскольку по условию $A_v(a_{s_1}) = C_v(a_{s_1})$. Если $j > s_1 + s_2$, то

$$L_j = M_{j-1}' + M_j'' = \sum_{i+s=j-1} g_{is} + \sum_{i+s=j} r_{is}.$$

Следовательно,

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

Предложение 3.3 доказано.

Предположим, что для заданного m норменное уравнение (3.1) имеет решение в многочленах $f, g \in \mathbb{F}_q[x]$, $g \neq 0$. Поскольку нормирование $|\cdot|_v$ имеет два продолжения на K, то $\sqrt{d} \in \overline{k}$. Представим f, g, $\sqrt{d}$ в виде формальных степенных рядов:

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

где $f_i, g_i, d_i \in \Sigma$. Сравнение степеней левой и правой частей в (3.1) показывает, что

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

где $[z]$ обозначает целую часть числа z. Кроме того, степени многочленов f_r и g_e должны удовлетворять следующим соотношениям:

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

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

где R – остаток от деления $m \deg v - \deg d$ на $2 \deg v$. Положим $C_v(d_i) = C_i$ и рассмотрим матрицу

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

Пусть D_m – матрица, которая получается из $\overline{D}_m$ вычеркиванием первых $r_1 + 1$ строк и столбцов с номерами $e_1 + 2, \dots, \deg v$ (если $e_1 + 2 > \deg v$, то столбцы не вычеркиваются). Следующая теорема дает алгоритм для нахождения фундаментальной S-единицы.

Теорема 3.4. *Для натурального $m \geqslant \deg d / \deg v$ норменное уравнение* (3.1) *имеет решение в многочленах $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, тогда и только тогда, когда ранг матрицы D_m меньше, чем $e \deg v + e_1 + 1$.*

Доказательство. Предположим, что для заданного m норменное уравнение (3.1) имеет решение в многочленах $f, g \in \mathbb{F}_q[x]$, $g \neq 0$. Тогда по предложению 2.1 либо $|f + g\sqrt{d}|_{v''} = m$, либо $|f - g\sqrt{d}|_{v''} = m$. Следовательно, один из элементов $f + g\sqrt{d}$, $f - g\sqrt{d}$ при разложении в формальный степенной ряд имеет вид $\sum_{i=m}^{\infty} L_i v^i$, где $L_i \in \Sigma$. Пусть $f + g\sqrt{d} = \sum_{i=m}^{\infty} L_i v^i$. Используя предложение 3.3 для вычисления коэффициентов L_i, получаем следующие равенства:

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

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

Рассмотрим уравнение (3.10) при $i = r$. Пусть $f_r = f_{r,0} + \dots + f_{r,r_1}x^{r_1}$, $g_e = g_{e,0} + \dots + g_{e,e_1}x^{e_1}$. Тогда

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

Обозначим

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

Пусть $\widetilde{C}_i$ – матрица, которая состоит из первых r_1+1 строк матрицы C_i. Отметим, что $F(g)$ – вектор-столбец длины $e\deg v + e_1 + 1$. Из (3.10), (3.12) получаем

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

Рассматривая последние $\deg v - r_1 - 1$ уравнений в (3.12) и уравнения (3.11), получаем

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

Таким образом, однородная система линейных уравнений (3.14) с матрицей D_m имеет ненулевое решение $F(g)$. Следовательно, ранг матрицы D_m меньше, чем $e\deg v + e_1 + 1$.

Предположим теперь, что ранг матрицы D_m меньше, чем $e\deg v + e_1 + 1$. Тогда однородная система линейных уравнений (3.14) с матрицей D_m имеет ненулевое решение $F(g)$. Зная вектор-столбец $F(g)$, находим ненулевой многочлен g. Затем по формулам (3.13) найдем коэффициенты многочлена f. По построению многочлены f и g обладают свойством, что $\deg(f^2 - g^2 d) \leqslant \deg v^m$ и v^m делит $f^2 - g^2 d$. Следовательно, $f^2 - g^2 d = av^m$, где $a \in \mathbb{F}_q^*$.

Теорема 3.4 доказана.

Итак, чтобы найти фундаментальную S-единицу поля K, вначале нужно разложить $\sqrt{d}$ в формальный степенной ряд. Затем, вычисляя последовательно ранг матрицы D_m, начиная с $m \geqslant \deg d/\deg v$, находим минимальное натуральное m такое, что ранг D_m меньше, чем $e\deg v + e_1 + 1$. После этого, решая однородную систему линейных уравнений с матрицей D_m, находим ненулевой многочлен g, а по формулам (3.13) – многочлен f. Искомая фундаментальная S-единица имеет вид $f + g\sqrt{d}$.

Следующее предложение уточняет теорему 3.4 для случая неприводимого многочлена d.

Предложение 3.5. *Предположим, что многочлен d неприводим. Тогда наименьшее натуральное m, для которого норменное уравнение* (3.1) *имеет решение в многочленах $f, g \in k[x]$, $g \neq 0$, является числом нечетным.*

Доказательство. Предположим, что $m = 2t$. Так как a в (3.1) должно быть квадратом, то, разделив обе части на a, без ограничения общности можно считать, что $a = 1$, т.е. f, g – решения норменного уравнения $f^2 - g^2 d = v^{2t}$. Запишем это уравнение в виде

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

Так как d неприводим, то он делит один из множителей в левой части уравнения (3.15). Пусть, например, $f - v^t = df_1$. Тогда $f = v^t + df_1$. Подставляя это выражение в (3.15), получаем

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

откуда следует, что f_1 делит g^2. Следовательно, многочлены g и f_1 можно представить в виде $g = f_2 h g_2$, $f_1 = f_2^2 h$ для некоторых $f_2, g_2, h \in \mathbb{F}_q[x]$. Подставляя g и f_1 в (3.16), получаем

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

Из (3.17) следует, что h делит v^t, и поэтому $h = bv^r$ для некоторого $b \in \mathbb{F}_q^*$. Разделив обе части (3.17) на h, получаем, что норменное уравнение $g_2^2 - f_2^2 d = 2b^{-1}v^{t-r}$ имеет решение в многочленах $f_2, g_2 \in \mathbb{F}_q[x]$, $g_2 \neq 0$, и $t - r < 2t = m$, что противоречит минимальности m.

Предложение 3.5 доказано.

3.2. Случай эллиптической кривой. Рассмотрим более подробно случай, когда $\deg d = 3$. Покажем, что тогда матрица D_m из теоремы 3.4 является квадратной.

Пусть $m = 2m_1$ четно. Тогда из равенств (3.6)–(3.8) следует

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

$$r_1 = 0, \qquad e_1 = \left[\deg v - \frac{3}{2}\right] = \deg v - 2.$$

Тогда

$$\overline{D}_m = \begin{pmatrix} C_1 & \dots & C_{m_1} \\ \multicolumn{3}{c}{\dotfill} \\ C_{m_1} & \dots & C_{2m_1-1} \end{pmatrix}$$

и, очевидно, матрица $\overline{D}_m$ является квадратной. Матрица D_m получается из $\overline{D}_m$ вычеркиванием первой строки и столбца с номером $\deg v$.

Пусть теперь $m = 2m_1 - 1$ нечетно. Тогда из равенств (3.6)–(3.8) следует

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

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

В случае $\deg v \leqslant 2$

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

Матрица D_m получается из $\overline{D}_m$ вычеркиванием первых $\deg v$ строк (столбцы не вычеркиваются). Следовательно, при $\deg v \leqslant 2$

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

– квадратная матрица порядка $(m_1 - 1)\deg v$.

Если же $\deg v \geqslant 3$, то

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

и матрица $\overline{D}_m$ является квадратной. Матрица D_m получается из $\overline{D}_m$ вычеркиванием первых $[\deg v/2]+1$ строк и столбцов с номерами $[(\deg v+1)/2], \dots, \deg v$. Легко убедиться, что количество вычеркиваемых строк и столбцов совпадает. Значит, D_m – квадратная матрица.

Таким образом, теорему 3.4 в случае эллиптических кривых можно сформулировать следующим образом.

Теорема 3.6. *Для натурального $m \geqslant 3/\deg v$ норменное уравнение* (3.1) *имеет решение в многочленах $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, тогда и только тогда, когда* $\det D_m = 0$.

Пример 3.7. Пусть $k = \mathbb{F}_3(x)$, $v = x^2 + 1 \in k[x]$ и

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

– неприводимый многочлен. В нашем случае для многочлена $u = u_0 + u_1 x \in \Sigma$ имеем

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

Так как 2 является квадратом в поле вычетов $\mathbb{F}_3[x]/(v)$, то $\sqrt{d} \in \overline{k}$ и элемент $\sqrt{d}$ можно представить в виде формального степенного ряда:

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

Тогда первые пять матриц C_i следующие:

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

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

Так как многочлен d неприводим, то в силу предложения 3.5 искомое m является нечетным. Имеем

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

Так как m нечетно, то матрица D_m имеет вид (3.18).

Пусть $m = 3$. Тогда $D_3 = C_2$ – невырожденная матрица.

Пусть $m = 5$. Тогда

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

Имеем $\det D_5 = 0$. Однородная система линейных уравнений $D_5 F(g) = 0$ имеет решение $F(g) = (0,0,1,0)^t$, откуда $g = x$. Теперь получаем $f = 1 - 2xv - xv^2 = 2x^5 + 2x^3 + 1$. Таким образом, фундаментальная S-единица поля K имеет вид

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

3.3. Случай $\deg v = 1$**.** Пусть $v = x - \alpha$. Пополнение $\overline{k}$ можно отождествить с полем формальных степенных рядов $\mathbb{F}_q((v))$. В этом случае $A_v(f) = (0)$ и $B_v(f) = f$ для любого $f \in \mathbb{F}_q$. Если $\sqrt{d} = \sum_{i=0}^{\infty} d_i v^i$ – разложение $\sqrt{d}$ в формальный степенной ряд в $\overline{k}$, то $C_i = d_i$. Из (3.6)–(3.8) получаем, что в случае четного $m = 2l$ имеем $r = l$, если же $m = 2l - 1$, то $r = l - 1$. В обоих случаях $r_1 = e_1 = 0$, $e = l - n - 1$. Тогда матрица D_m из теоремы 3.4 имеет вид

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

Получаем следствие из теоремы 3.4.

Следствие 3.8. *Пусть* $m \geqslant 2n + 1$. *Если* $m = 2l$ (*соответственно* $m = 2l-1$), *то норменное уравнение* (3.1) *имеет решение в многочленах* $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, *тогда и только тогда, когда ранг матрицы* D_{2l} (*соответственно* D_{2l-1}), *определенной в* (3.19), *меньше, чем* $l - n$.

Если K – поле функций эллиптической кривой, т.е. $\deg d = 3$, то матрицы D_{2l} и D_{2l-1} являются квадратными, и мы получаем следующий результат.

Следствие 3.9. *Пусть* $\deg d = 3$ *и* $m \geqslant 3$. *Если* $m = 2l$ (*соответственно* $m = 2l - 1$), *то норменное уравнение* (3.1) *имеет решение в многочленах* $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, *тогда и только тогда, когда* $\det D_{2l} = 0$ (*соответственно* $\det D_{2l-1} = 0$).

Матрицы специального вида, возникающие в следствии 3.9, носят название *ганкелевых* (при другой нумерации неизвестных коэффициентов многочлена g

мы получим тёплицевы матрицы). Эти матрицы имеют многочисленные применения в алгебре, теории функций, гармоническом анализе, теории вероятностей, теории кодирования и во многих других областях (см. монографию [6] и обзор [7]).

Пример 3.10. Пусть $d = x^3 + x^2 + x + 1 \in \mathbb{F}_5[x]$, $v = x$. Тогда в пополнении $\overline{k}$ имеем следующее разложение $\sqrt{d}$ в формальный степенной ряд:

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

Нормирование $|\cdot|_v$ имеет два продолжения на $k(\sqrt{d})$. Пусть $S = \{|\cdot|_\infty, |\cdot|_{v'}\}$. Имеем $D_3 = (1)$, $D_4 = (0)$. В качестве решения однородной системы линейных уравнений с матрицей D_4 возьмем $g = 1$. Тогда из условий $|f + \sqrt{d}|_{v'} = 4$, $\deg f \leqslant 2$ получаем $f = -1 - 3x - x^2$. Таким образом, $\varepsilon = -x^2 - 3x - 1 + \sqrt{d}$ – фундаментальная S-единица и $N_{K/k}(\varepsilon) = x^4$.

§ 4. Случай $|S| > 2$

Пусть теперь $S = \{|\cdot|_\infty, |\cdot|_{v_1'}, \dots, |\cdot|_{v_t'}\}$, где $t > 1$. В силу п. 2 теоремы 2.5 система независимых фундаментальных S-единиц может быть построена индуктивным образом. Обозначим $S_i = \{|\cdot|_\infty, |\cdot|_{v_1'}, \dots, |\cdot|_{v_i'}\}$, $S_i' = \{|\cdot|_\infty, |\cdot|_{v_i'}\}$. Пусть δ_i – фундаментальная S_i'-единица, которая может быть найдена при помощи теоремы 3.4. Пусть $N_{K/k}(\delta_i) = b_i v_i^{m_i}$, где $b_i \in \mathbb{F}_q^*$.

Предположим теперь, что мы уже построили независимые фундаментальные S_i-единицы $\varepsilon_1, \dots, \varepsilon_i$. По теореме 2.5 нам нужно найти такую S_{i+1}-единицу ε_{i+1}, что

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

где $a_{i+1} \in \mathbb{F}_q^*$ и показатель $m_{i+1,i+1} > 0$ наименьший возможный. Тогда $\varepsilon_1, \dots, \varepsilon_i, \varepsilon_{i+1}$ – система независимых фундаментальных S_{i+1}-единиц.

Пусть $\varepsilon_1, \dots, \varepsilon_t$ – построенные таким образом независимые фундаментальные S-единицы. Рассмотрим матрицу

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

Справедливо следующее предложение.

Предложение 4.1. *Существует такая система независимых фундаментальных S-единиц $\varepsilon_1, \dots, \varepsilon_t$, что матрица $H(\varepsilon_1, \dots, \varepsilon_t)$, определенная в (4.1), обладает следующими свойствами*:

1) $0 \leqslant m_{ir} < m_{rr}$ *для* $r = 1, \dots, t-1$, $i = r+1, \dots, t$;
2) $\varepsilon_i = f_i + g_i\sqrt{d}$, *где* $f_i, g_i \in \mathbb{F}_q[x]$, $g_i \neq 0$, $i = 1, \dots, t$;
3) $\sum_{j=1}^{i} m_{ij} \deg v_j \geqslant \deg d$;
4) m_{ii} *делит* m_i *для* $i = 1, \dots, t$;
5) *если* $m_{ii} = m_i$, *то* $m_{i1} = \dots = m_{i,r-1} = 0$;
6) *строка* $(m_i/m_{ii})(m_{i1}, \dots, m_{i,i-1})$ *является целочисленной линейной комбинацией строк* $(m_{11}, 0, \dots, 0)$, $\dots$, $(m_{i-1,1}, \dots, m_{i-1,i-1})$.

Доказательство. 1) Пусть $\varepsilon_1,\dots,\varepsilon_t$ – построенная индуктивно система независимых фундаментальных S-единиц. Если $\varepsilon'_1,\dots,\varepsilon'_t$ – другая система независимых фундаментальных S-единиц, то

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

При этом $B=(b_{ij})\in GL_t(\mathbb{Z})$. Обратно, если дана произвольная матрица $B=(b_{ij})\in GL_t(\mathbb{Z})$, то формулы (4.2) определяют переход к новой системе независимых фундаментальных S-единиц. Нетрудно видеть, что при этом

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

Поэтому, умножая $H(\varepsilon_1,\dots,\varepsilon_t)$ на подходящую матрицу $B\in GL_t(\mathbb{Z})$, мы можем добиться выполнения условия 1).

2) Пусть $\varepsilon_i=(f_i+g_i\sqrt{d})/(v_1^{l_1}\cdots v_i^{l_i})$, где $f_i,g_i\in\mathbb{F}_q[x]$, $g_i\neq 0$, и пусть, например, $l_1>0$. Тогда

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

Так как $N_{K/k}(\varepsilon_i)=(f_i^2-g_i^2d)/(v_1^{2l_1}\cdots v_i^{2l_i})$, то мы имеем

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

Так как $m_{i1}\geqslant 0$ по условию, то $2l_1+m_{i1}>0$. Тогда по предложению 2.1 $|f_i+g_i\sqrt{d}|_{v''_1}=2l_1+m_{i1}$. Из (4.3) следует, что $2l_1+m_{i1}=l_1$, откуда мы получаем равенство $m_{i1}=-l_1<0$ – противоречие.

3) Так как в силу условия 2) $\varepsilon_i=f_i+g_i\sqrt{d}$, то $f_i^2-g_i^2d=v_1^{m_{i1}}\cdots v_i^{m_{ii}}$. Так как $g_i\neq 0$, то, сравнивая степени левой и правой частей, получаем требуемое утверждение.

4) Так как δ_i является S_i-единицей, то $\delta_i=c_i\varepsilon_1^{a_1}\cdots\varepsilon_i^{a_i}$, где $c_i\in\mathbb{F}_q^*$. Тогда

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

откуда получаем $m_i=a_im_{ii}$, что и доказывает условие 4). Если $m_{ii}=m_i$, то $a_i=1$, и мы можем заменить ε_i на δ_i. После этой замены будет выполнено условие 5).

6) Из (4.4) следует, что

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

Предложение 4.1 доказано.

Следствие 4.2. *Пусть $\varepsilon_1,\dots,\varepsilon_{t-1}$ – система независимых фундаментальных S_{t-1}-единиц. Пусть m_{tt} – наименьший натуральный делитель m_t со следующим свойством: существуют целые числа $0\leqslant m_{tj}<m_{jj}$, $j=1,\dots,t-1$, удовлетворяющие условиям* 3), 5), 6) *предложения* 4.1, *такие, что норменное уравнение*

$$f^2-g^2d=av_1^{m_{t1}}\cdots v_t^{m_{tt}}, \tag{4.5}$$

где $a\in\mathbb{F}_q^*$, имеет решение в многочленах $f,g\in\mathbb{F}_q[x]$, $g\neq 0$. Пусть ε_t – S-единица, полученная из этого решения при помощи предложения 2.4. *Тогда $\varepsilon_1,\dots,\varepsilon_t$ – система независимых фундаментальных S-единиц.*

Как и в случае одного нормирования, решение норменного уравнения (4.5) сводится к решению некоторой однородной системы линейных уравнений. Из (4.5) следует, что

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

Пусть $f = f_0 + f_1x + \dots + f_rx^r$, $g = g_0 + g_1x + \dots + g_lx^l$. Выберем одно из нормирований $|\cdot|_{v_j}$, $1 \leqslant j \leqslant t$, и представим $f + g\sqrt{d}$ в виде формального степенного ряда от v_j:

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

где $L_i \in \Sigma$, при этом коэффициенты многочлена L_i являются линейными формами от $f_0, \dots, f_r$, $g_0, \dots, g_l$. Потребуем, чтобы выполнялись условия

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

Тогда (4.6) дает однородную систему линейных уравнений относительно коэффициентов $f_0, \dots, f_r$, $g_0, \dots, g_l$ с некоторой матрицей M_{v_j}:

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

Проделав данное построение для всех нормирований $|\cdot|_{v_j}$, $j = 1, \dots, t$, получим, что $f_0, \dots, f_r$, $g_0, \dots, g_l$ – решение однородной системы линейных уравнений

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

где M – блочная матрица вида $M = \begin{pmatrix} M_{v_1} \\ \vdots \\ M_{v_t} \end{pmatrix}$.

Обратно, если $f_0, \dots, f_r$, $g_0, \dots, g_l$ – такое решение (4.7), что не все g_i равны нулю, то по построению ненулевой многочлен $f^2 - g^2d$ делится на произведение $v_1^{m_{t1}} \cdots v_t^{m_{tt}}$. Кроме того, $\deg f^2 - g^2d \leqslant \deg v_1^{m_{t1}} \cdots v_t^{m_{tt}}$. Следовательно, $f^2 - g^2d = av_1^{m_{t1}} \cdots v_t^{m_{tt}}$, где $a \in \mathbb{F}_q^*$.

Таким образом, нами доказана

Теорема 4.3. *Норменное уравнение (4.5) имеет решение $f, g \in \mathbb{F}_q[x]$, $g \neq 0$, тогда и только тогда, когда однородная система линейных уравнений (4.7) имеет такое решение $f_0, \dots, f_r$, $g_0, \dots, g_l$, что не все g_k равны нулю.*

Отметим также следующее свойство S-единиц, справедливое при нашем выборе S.

Предложение 4.4. *Пусть $\varepsilon \in U_S$. Если $N_{K/k}(\varepsilon) \in \mathbb{F}_q^*$, то $\varepsilon \in \mathbb{F}_q^*$.*

Доказательство. Пусть $\varepsilon = (f + g\sqrt{d})/(v_1^{m_1} \cdots v_t^{m_t})$, где $f, g \in \mathbb{F}_q[x]$. Предположим, что $m_1 > 0$. Тогда $|f + g\sqrt{d}|_{v_1'} = m_1$. По условию $N_{K/k}(\varepsilon) = a$, следовательно,

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

Отсюда получаем, что $|f+g\sqrt{d}|_{v_1'}+|f-g\sqrt{d}|_{v_1'}=2m_1$. Так как $|f+g\sqrt{d}|_{v_1'}>0$, то по предложению 2.1 $|f+g\sqrt{d}|_{v_1'}=2m_1$ – противоречие. Значит, $m_1=\dots=m_t=0$. Но тогда $N_{K/k}(\varepsilon)\notin\mathbb{F}_q^*$, что противоречит условию.

Предложение 4.4 доказано.

Замечание. Предложение 4.4 перестает быть верным в случае произвольного S. Действительно, пусть ε – фундаментальная единица из примера 3.10. Положим $S_1=S\cup\{|\cdot|_{x''}\}$. Тогда элемент ε/x^2 является нетривиальной S_1-единицей и $N_{K/k}(\varepsilon/x^2)=1$. Отметим, что ε/x^2 не является S-единицей (и даже S-целым элементом).

Пример 4.5. Предположим, что выполнены условия примера 3.10. Пусть $u=x-1$. Нормирование $|\cdot|_u$ имеет два продолжения $|\cdot|_{u'}$ и $|\cdot|_{u''}$ на $k(\sqrt{d})$. Положим $S_1=\{|\cdot|_\infty,|\cdot|_{v'},|\cdot|_{u'}\}$. Найдем систему независимых фундаментальных S_1-единиц.

Вначале положим $T=\{|\cdot|_\infty,|\cdot|_{u'}\}$ и найдем фундаментальную T-единицу. Пусть k_1 – пополнение k относительно $|\cdot|_u$. В поле k_1 имеем следующее разложение $\sqrt{d}$ в формальный степенной ряд:

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

Имеем $D_3=(2)$, $D_4=(0)$. Как и в примере 3.10, получаем $g=1$, $f=-2-4(x-1)-2(x-1)^2=3x^2$. Таким образом, $\varepsilon_1=3x^2+\sqrt{d}$ – фундаментальная T-единица и $N_{K/k}(\varepsilon_1)=-(x-1)^4$.

Если ε, ε_2 – система независимых фундаментальных S_1-единиц, то по предложению 4.1 матрица $H(\varepsilon,\varepsilon_2)$ может иметь один из следующих видов:

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

Будем рассматривать эти случаи последовательно, пока не найдем систему независимых фундаментальных S_1-единиц.

1) Имеем норменное уравнение $f^2-g^2d=ax^2(x-1)$. Тогда $\deg f=1$, $\deg g=0$. Пусть $f=f_0+f_1x$. Элемент $f+g\sqrt{d}$ в пополнении $\overline{k}$ относительно нормирования $|\cdot|_x$ имеет вид

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

Отсюда получаем уравнения $f_0+g=0$, $f_1+3g=0$.

Элемент $f+g\sqrt{d}$ в пополнении k_1 имеет вид

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

Отсюда получаем уравнение $f_0+f_1+2g=0$. Таким образом, имеем однородную систему линейных уравнений с матрицей $\left(\begin{smallmatrix}1&0&1\\0&1&3\\1&1&2\end{smallmatrix}\right)$, которая невырождена. Значит, $f_0=f_1=g=0$, и наше норменное уравнение не имеет нетривиальных решений.

2) Имеем норменное уравнение $f^2-g^2d=ax^3(x-1)$. Тогда $\deg f=2$, $\deg g=0$. Пусть $f=f_0+f_1x+f_2x_2$. В этом случае получаем однородную систему линейных уравнений с матрицей $\left(\begin{smallmatrix}1&0&0&1\\0&1&0&3\\0&0&1&1\\1&1&1&2\end{smallmatrix}\right)$, которая также невырождена. Поэтому норменное уравнение также не имеет нетривиальных решений.

3) Имеем норменное уравнение $f^2 - g^2 d = ax^2(x-1)^2$. Тогда, как и в п. 2), $\deg f = 2$, $\deg g = 0$. Получаем однородную систему линейных уравнений с матрицей $\begin{pmatrix} 1&0&0&1\\ 0&1&0&3\\ 1&1&1&2\\ 0&1&2&4 \end{pmatrix}$, определитель которой равен нулю. Решая эту систему, получаем $f = 4 + 2x + 2x^2$, $g = 1$. По следствию 4.2 $\varepsilon = -x^2 - 3x - 1 + \sqrt{d}$, $\varepsilon_2 = 2x^2 + 2x + 4 + \sqrt{d}$ – система независимых фундаментальных S_1-единиц.

§ 5. Непрерывные дроби в функциональных полях

5.1. Построение и свойства непрерывных дробей. Непрерывные дроби в функциональных полях в случае нормирования $|\cdot|_\infty$ были впервые введены Э. Артином (см. [8]). Мы рассматриваем общий случай произвольного нормирования $|\cdot|_v$ поля $k = L(x)$, где L – произвольное поле. Пусть $\beta \in \overline{k}$. Представим β в виде формального степенного ряда:

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

где $d_i \in \Sigma$, и положим

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

Пусть $a_0 = [\beta]$. Если $\beta - a_0 \neq 0$, то положим

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

Далее по индукции определяем элементы a_i, β_i: если $\beta_{i-1} - a_{i-1} \neq 0$, то

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

В результате получим непрерывную дробь

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

Предложение 5.1. *Непрерывная дробь* (5.1) *конечна тогда и только тогда, когда $\beta \in k$.*

Доказательство. Предположим, что $\beta \in k$. Пусть $\beta_i = b_i/c_i$, где $b_i, c_i \in L[x]$ и $(b_i, c_i) = 1$. Тогда по построению $|\beta_i|_v = -s < 0$. Пусть

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

где $a_i \in \Sigma$. Тогда

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

Так как $|\beta_i - [\beta_i]|_v > 0$, то $b_i - c_{i+1}(a_0 + \cdots + a_s v^s) = v^s b_{i+1}$, где $b_{i+1} \in L[x]$. Тогда

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

При этом $\deg c_{i+1} < M_i$ и $\deg b_{i+1} < M_i$, где $M_i = \max\{\deg b_i, \deg c_i\}$. Убывающая цепочка натуральных чисел M_i должна оборваться. Это означает, что непрерывная дробь (5.1) конечна. Обратное утверждение очевидно.

Предложение 5.1 доказано.

Будем использовать стандартную сокращенную запись для непрерывной дроби (5.1) $[a_0, a_1, a_2, \dots]$. По построению $\beta_n = [a_n, a_{n+1}, \dots]$.

Определим по индукции элементы $p_i, q_i \in k$. Положим

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

и если $n \geqslant 0$, то

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

Тогда $p_n/q_n = [a_0, a_1, a_2, \dots, a_n]$ при $n \geqslant 0$. Стандартным образом можно показать (см. [9]), что для $n \geqslant -1$ справедливы соотношения

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

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

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

Дробь p_n/q_n назовем *n-й подходящей дробью к β*. По построению $|a_n|_v = |\beta_n|_v < 0$ для $n \geqslant 1$. Из (5.2) по индукции легко получить соотношение

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

а из (5.4) получаем

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

или, что эквивалентно,

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

Значит, $\lim_{n\to\infty} p_n/q_n = \beta$, т.е. подходящие дроби сходятся к β.

Стандартным образом, как и в случае поля вещественных чисел, можно показать, что если непрерывная дробь $[a_0, a_1, \dots]$ для β является периодической, то $\beta \in \overline{k}$ – квадратичная иррациональность. В случае бесконечного поля L и нормирования $|\cdot|_\infty$ обратное утверждение верно не всегда (см. [10]). Справедливо

Предложение 5.2. *Пусть $L = \mathbb{F}_q$ – поле из q элементов и $\deg v = 1$. Если $\beta \in \overline{k} = L((v))$ – квадратичная иррациональность, то непрерывная дробь для β периодична.*

Доказательство. Пусть $\beta \in L((v))$ является корнем квадратного многочлена $H(X) = rX^2 + sX + t$, где $r, s, t \in L[v]$, и $\beta = [a_0, a_1, \dots]$ – разложение β в непрерывную дробь. Положим

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

Тогда из (5.5) получаем

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

где

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

Ясно, что для достаточно большого n имеем $|p_n/q_n - \beta|_v > |\beta - \overline{\beta}|_v$, где $\overline{\beta}$ – второй корень $H(X)$. Тогда

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

Так как $\beta - \overline{\beta} = 2\sqrt{D}/r$, то $|\beta - \overline{\beta}|_v = (1/2)|D|_v - |r|_v$. Отсюда получаем

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

Поскольку $H(X, Y) = r(X - \beta Y)(X - \overline{\beta} Y)$, то, учитывая (5.7), находим

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

Найдем нижнюю оценку для $|B_n|_v$. Из (5.9) находим $B_n = A_n\beta_{n+1} - r\beta$. Из равенства $\beta(r\beta + s) = -t$ следует, что $|r\beta|_v \geqslant 0$. Учитывая (5.10) и то, что $|\beta_{n+1}|_v = |a_{n+1}|_v$, находим

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

Значит,

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

Таким образом, A_n, B_n являются многочленами из $L[x]$. Их степени не превосходят $\max\{\deg r, \deg s, \deg t\}$. Поскольку поле L конечно, то таких многочленов конечное число. Это означает, что для некоторых i и j должно быть $A_i = A_{i+j}$, $B_i = B_{i+j}$. Тогда $\beta_i = \beta_{i+j}$ и непрерывная дробь для β периодична.

Предложение 5.2 доказано.

Отметим, что в случае $\deg v > 1$ приведенное выше рассуждение перестает быть справедливым. Хотя A_n, B_n по-прежнему будут многочленами из $L[x]$, мы не можем утверждать, что их степени ограничены сверху.

5.2. Наилучшие приближения. Введем понятие наилучшего приближения к элементу $\beta \in \overline{k}$. Если $a/b \in L(x)$, где $a, b \in L[x]$ – взаимно простые многочлены, то разложим a и b по степеням v:

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

где $a_i, b_i \in \Sigma$, $a_s \neq 0$, $b_t \neq 0$. Тогда, разделив a и b на v^r, где $r = \max\{s, t\}$, мы представим дробь a/b в виде

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

где $c_i, d_i \in \Sigma$, $c_{-m} \neq 0$, $d_{-r} \neq 0$, c_0 и d_0 одновременно не равны нулю. Будем в дальнейшем предполагать, что все элементы из $L(x)$ записаны в виде (5.11).

Определение 5.3. Несократимая дробь $p/q \in L(x)$ является *наилучшим приближением* к $\beta \in \overline{k}$, если для любой другой несократимой дроби $a/b \neq p/q$ такой, что $|b|_v \geqslant |q|_v$, справедливо неравенство

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

Теорема 5.4. *Дробь p/q является наилучшим приближением к β тогда и только тогда, когда выполнено одно из следующих условий.*

1. *Пусть* $\deg v = 1$. *Дробь p/q является наилучшим приближением к β тогда и только тогда, когда $|\beta - p/q|_v > -2|q|_v$.*

2. *Пусть* $\deg v > 1$. *Если $|\beta - p/q|_v > -2|q|_v + 1$, то дробь p/q является наилучшим приближением к β. Если дробь p/q является наилучшим приближением к β, то $|\beta - p/q|_v > -2|q|_v$.*

Доказательство. Предположим, что для дроби p/q выполнено следующее условие:

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

Пусть c/d – такая дробь, что $c/d \neq p/q$ и $|d|_v \geqslant |q|_v$. Поскольку

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

то

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

Из последнего неравенства получаем

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

Значит, дробь p/q является наилучшим приближением к β.

Предположим теперь, что дробь p/q является наилучшим приближением к β. Пусть $h = \deg v$. Запишем элементы p, q, β в виде формальных степенных рядов от v:

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

где $a_i, b_i, u_i \in \Sigma$, $a_{-r} \neq 0$, $b_{-s} \neq 0$. Допустим, что $|\beta - p/q|_v \leqslant -2|q|_v$. Тогда $l = |q\beta - p|_v \leqslant -|q|_v = s$. Из определения наилучшего приближения легко получить, что $l > 0$. Тогда мы должны иметь $|p|_v = |q|_v + |\beta|_v$, т.е. $r = s - m$. Положим

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

где матрицы A_v, B_v определены в (3.2). Тогда $q\beta = \sum_{j=m-s}^{\infty} d_j v^j$, где $\widehat{d_j} = \sum_{i+e=j} C_i \widehat{b_e}$. Поскольку

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

то мы получаем следующие равенства:

$$\widehat{a_i} = \widehat{d_i}, \qquad i = -r, \dots, 0, \tag{5.13}$$

$$\widehat{d_1} = \widehat{d_2} = \dots = \widehat{d_{l-1}} = 0. \tag{5.14}$$

Обозначим

$$\widehat{q} = \begin{pmatrix} \widehat{b_0} \\ \dots \\ \widehat{b_{-s}} \end{pmatrix}, \qquad C = \begin{pmatrix} C_1 & \dots & C_{s+1} \\ \dots & \dots & \dots \\ C_{l-1} & \dots & C_{s+l-1} \end{pmatrix}.$$

Из (5.14) следует, что $\widehat{q}$ является решением однородной системы линейных уравнений

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

где $Y = (y_1, \dots, y_{h(s+1)})^t$ – вектор-столбец, содержащий $h(s+1)$ переменных. Матрица C с коэффициентами из поля L содержит $h(s+1)$ столбцов и $h(l-1)$ строк. Поскольку по нашему предположению $l \leqslant s$, то $\operatorname{rank} C \leqslant h(l-1)$. Следовательно, общее решение (5.15) имеет вид

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

где H_i – некоторая линейная форма от переменных $z_1, \dots, z_m$ и

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

Пусть V – пространство решений (5.15). В силу сказанного $\dim V = m \geqslant 2h$.

Каждому ненулевому набору $(z_1^0, \dots, z_m^0) \in L^m$ поставим в соответствие элемент $\overline{q}_1 = (y_1^0, \dots, y_{h(s+1)}^0)^t \in V$, где $y_i^0 = H_i(z_1^0, \dots, z_m^0)$. В свою очередь, для произвольного ненулевого элемента $\overline{q}_1 \in V$ можно построить дробь p_1/q_1, обладающую следующими свойствами: $|q_1|_v \geqslant |q|_v$ и

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

Для этого построим многочлены $b^0_{-i} = y^0_{hi+1} + y^0_{hi+2}x + \dots + y^0_{hi+h}x^{h-1}$, $i = 0, \dots, s$. Далее, положим

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

и рассмотрим элементы

$$q_1 = \sum_{i=0}^{s-1} b^0_{-i} v^{-i}, \qquad p_1 = \sum_{i=0}^{-r} a^0_{-i} v^{-i}.$$

Дробь p_1/q_1 будет искомой.

Выделим в V два подпространства U и W, которые мы сейчас опишем. Поскольку (5.15) имеет решение $\overline{q}$, в котором $b_{-s} \neq 0$, то не все из форм $H_{sh+1}, \dots, H_{sh+h}$ являются нулевыми. Пусть $T \subset L^m$ – пространство решений однородной системы линейных уравнений

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

Тогда $\dim T \leqslant m-1$. Пусть U – множество тех решений системы (5.15), которые соответствуют элементам из T. Ясно, что U – собственное подпространство в V.

Опишем теперь множество тех дробей p_1/q_1, для которых $|q_1|_v \geqslant |q|_v$ и $p/q = p_1/q_1$ в поле $L(x)$. Так как дробь p/q несократима, то p_1/q_1 получается из p/q следующим образом: мы умножаем p и q на некоторый многочлен $\alpha \in L[x]$, а затем полученную дробь $\alpha p/(\alpha q)$ приводим к виду (5.11).

Многочлены a_0, b_0 в (5.12) не равны одновременно нулю. Пусть для определенности $a_0 \neq 0$ и $\deg a_0 \geqslant \deg b_0$. Тогда $\alpha p = \sum_{i=-r}^{0} \alpha a_i v^i$. Покажем, что $\deg \alpha a_0 < \deg v$. Допустим противное. Тогда αa_0 можно представить в виде $\alpha a_0 = c_0 + c_1 v + \dots + c_l v^l$, где $c_i \in \Sigma$, $l > 0$. Следовательно, для того чтобы представить дробь $\alpha p/(\alpha q)$ в виде (5.11), нужно числитель и знаменатель разделить на v^l. Но тогда мы получим $|q_1|_v < |q|_v$ – противоречие. Итак, мы имеем

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

Пусть R – пространство многочленов из $L[x]$ степени меньше d. Если $\alpha \in U$, то рассмотрим дробь $\alpha p/(\alpha q)$ и представим ее в виде (5.11). В результате получим дробь p_1/q_1. Рассмотрим вектор-столбец $\widehat{q}_1$. Так как

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

то $\widehat{q}_1$ является решением (5.15), а значит, $\widehat{q}_1 \in V$. Обозначим через W множество всех вектор-столбцов $\widehat{q}_1$, которые получаются таким образом, вместе с нулевым столбцом. Ясно, что W – подпространство в V и $\dim W = d \leqslant h$. Следовательно, W – собственное подпространство в V.

Так как U и W – собственные подпространства в V, то $V \setminus (U \cup W) \neq \varnothing$. Пусть $\widehat{q}_1 \in V \setminus (U \cup W)$. Рассмотрим дробь p_1/q_1, соответствующую $\widehat{q}_1$. По построению имеем $|q_1|_v = |q|_v$ и $p/q \neq p_1/q_1$ в поле $L(x)$. Тогда из неравенства (5.17) следует, что

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

Это противоречит тому, что p/q – наилучшее приближение к β.

Теорема 5.4 доказана.

Предложение 5.5. *Если дроби a/b и c/d – такие наилучшие приближения к β, что $|b|_v = |d|_v$, то найдется константа $h \in L^*$ такая, что $a = hc$, $b = hd$.*

Доказательство. Если $a/b \neq c/d$ в $L(x)$, то по определению наилучшего приближения справедливы неравенства

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

– противоречие. Значит, $a/b = c/d$ в $L(x)$. Учитывая несократимость этих дробей, получаем требуемое утверждение.

Предложение 5.5 доказано.

Теорема 5.6. *Пусть $\deg v = 1$. Справедливы следующие утверждения*:

1) *n-я подходящая дробь p_n/q_n к β является наилучшим приближением к β*;

2) *если дробь a/b является наилучшим приближением к β, то найдутся такая подходящая дробь p_n/q_n к β и такая константа $c \in L^*$, что $a = cp_n$, $b = cq_n$.*

Доказательство. 1) Поскольку

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

где $c_i, d_i \in L$, то p_n/q_n имеет вид (5.11). Теперь неравенство (5.7) и теорема 5.4 немедленно влекут, что p_n/q_n является наилучшим приближением к β.

2) Вначале докажем, что $|b|_v = |q_n|_v$ для некоторой подходящей дроби p_n/q_n. Допустим противное. Поскольку $|q_0|_v = |1|_v = 0$, $|q_n|_v < |q_{n-1}|_v$ в силу (5.6) и $|b|_v \leqslant 0$, то найдется такое n, что

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

Поскольку a/b – наилучшее приближение к β и $|q_n|_v > |b|_v$, то

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

Тогда мы имеем

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

Отсюда $-|b|_v \geqslant -|q_{n+1}|_v$, что противоречит неравенству $|q_{n+1}|_v < |b|_v$. Итак, для некоторого n мы имеем $|q_n|_v = |b|_v$. Применяя предложение 5.5, завершаем доказательство теоремы 5.6.

Теорема 5.6 доказана.

В случае $\deg v > 1$ подходящая дробь p_n/q_n не обязательно является наилучшим приближением к β.

Пример 5.7. Пусть k, v и d такие же, как и в примере 3.7. Разлагая $\sqrt{d}$ в непрерывную дробь, получаем

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

Тогда подходящие дроби к $\sqrt{d}$ имеют вид

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

Покажем, что p_2/q_2 не является наилучшим приближением к $\sqrt{d}$. В силу (5.7)

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

С другой стороны, чтобы записать подходящую дробь p_2/q_2 в виде (5.11), нужно числитель и знаменатель разделить на v:

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

Тогда имеем

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

В силу теоремы 5.4 p_2/q_2 не является наилучшим приближением к $\sqrt{d}$.

5.3. Непрерывные дроби и S-единицы. В этом пункте мы снова предполагаем, что $L = \mathbb{F}_q$ – конечное поле характеристики $p > 2$, $k = \mathbb{F}_q(x)$. Мы покажем, как непрерывные дроби могут быть использованы для нахождения фундаментальных S-единиц в гиперэллиптических полях.

Пусть $v \in \mathbb{F}_q[x]$ – неприводимый многочлен. Предположим, что нормирование $|\cdot|_v$ имеет два неэквивалентных продолжения $|\cdot|_{v'}$ и $|\cdot|_{v''}$ на поле $K = k(\sqrt{d})$. Пусть $S = \{|\cdot|_\infty, |\cdot|_{v'}\}$. В классическом случае квадратичного расширения $L = \mathbb{Q}(\sqrt{r})$, $r > 0$, поля $\mathbb{Q}$ фундаментальную единицу поля L можно найти, используя разложение $\sqrt{d}$ либо $(\sqrt{d}-1)/2$ в непрерывную дробь (см. [11; гл. II, § 7]). Наша цель – показать, что и в случае гиперэллиптического поля K и нормирования $|\cdot|_v$, определяемого линейным многочленом v, фундаментальную S-единицу можно найти, используя метод непрерывных дробей.

Теорема 5.8. *Пусть $v \in \mathbb{F}_q(x)$ и $\deg v = 1$. Предположим, что для некоторого минимального натурального m уравнение* (3.1) *имеет решение в многочленах $f, g \in \mathbb{F}_q[x]$, $g \neq 0$. Справедливы следующие утверждения.*

1. *Если* $m = 2t+1$, *то* f/g *является наилучшим приближением к* $\sqrt{d}$. *Таким образом,* $f/g = p_n/q_n$ *для некоторой подходящей дроби* p_n/q_n *к* $\sqrt{d}$.

2. *Если* $m = 2t$, *то найдется делитель* h *многочлена* d, $\deg h < (1/2)\deg d$, *такой, что уравнение*

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

где $b \in \mathbb{F}_q^*$, *имеет решение в многочленах* $f_1, g_1 \in \mathbb{F}_q[x]$. *При этом* f_1/g_1 *является наилучшим приближением к* $\sqrt{d}/h$ *и, следовательно,* $f_1/g_1 = p_n/q_n$ *для некоторой подходящей дроби* p_n/q_n *к* $\sqrt{d}/h$. *Наоборот, если* $f_1, g_1 \in \mathbb{F}_q[x]$ – *решение* (5.19), *то* f_1/g_1 *является наилучшим приближением к* $\sqrt{d}/h$, $f_1/g_1 = p_n/q_n$ *для некоторой подходящей дроби* p_n/q_n *к* $\sqrt{d}/h$ *и многочлены* f *и* g, *определяемые по формулам*

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

являются решением уравнения (3.1).

Доказательство. 1. Запишем (3.1) в виде

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

В силу предложения 2.1 можно считать, что $|f+g\sqrt{d}|_{v'} = 0$, $|f-g\sqrt{d}|_{v'} = 2t+1$. Разложим f и g по степеням v:

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

где $b_i, c_i \in \mathbb{F}_q$, $b_r \neq 0$, $c_s \neq 0$. Сравнение степеней многочленов в левой и правой частях уравнения (3.1) показывает, что $r \leqslant t$, $s \leqslant t$. Пусть $h = \max\{r, s\}$. Рассмотрим элемент $\overline{f} - \overline{g}\sqrt{d}$, где

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

Так как $\overline{f}/\overline{g}$ имеет вид (5.11) и

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

то по теореме 5.4 дробь $\overline{f}/\overline{g} = f/g$ является наилучшим приближением к $\sqrt{d}$. Тогда по теореме 5.6 $f/g = p_n/q_n$ для некоторой подходящей дроби p_n/q_n к $\sqrt{d}$.

2. Так как a в уравнении (3.1) должно быть квадратом, то, разделив обе части на a, без ограничения общности можно считать, что f, g – решение норменного уравнения $f^2 - g^2d = v^{2t}$. Отсюда получаем

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

Пусть $d = d_1d_2\cdots d_r$ – разложение d на неприводимые множители над $\mathbb{F}_q$. Тогда каждый многочлен d_i делит ровно один из множителей: $f - v^t$ или $f + v^t$. В противном случае мы имели бы, что d_i делит v^t, а значит, $d_i = cv$, где $c \in \mathbb{F}_q^*$. Но тогда v делит d, а это не так.

Пусть h_1 – произведение тех d_i, которые делят $f - v^t$, а h_2 – произведение тех d_i, которые делят $f + v^t$. Тогда $h_1 h_2 = d$, $(h_1, h_2) = 1$. Пусть для определенности $\deg h_1 < \deg h_2$, т.е. $\deg h_1 < (1/2)\deg d$. Запишем

$$f - v^t = h_1 u_1, \qquad f + v^t = h_2 u_2. \tag{5.22}$$

Из (5.22) получаем

$$f = \frac{1}{2}(h_1 u_1 + h_2 u_2), \qquad v^t = \frac{1}{2}(h_2 u_2 - h_1 u_1). \tag{5.23}$$

Подставляя (5.22) в (5.21), получаем $u_1 u_2 = g^2$. Заметим, что $(u_1, u_2) = 1$ (в противном случае f и g не были бы взаимно простыми). Тогда $u_1 = f_1^2$, $u_2 = g_1^2$. Таким образом,

$$f = \frac{1}{2}(h_1 f_1^2 + h_2 g_1^2), \qquad g = f_1 g_1. \tag{5.24}$$

Из (5.23), (5.24) получаем

$$2v^t = \frac{d}{h_1} g_1^2 - h_1 f_1^2. \tag{5.25}$$

Таким образом, уравнение (3.1) имеет решение в многочленах $f, g \in \mathbb{F}_q[x]$ тогда и только тогда, когда уравнение (5.25) имеет решение в многочленах $f_1, g_1 \in \mathbb{F}_q[x]$ для некоторого делителя h_1 многочлена d такого, что $\deg h_1 < (1/2)\deg d$.

Докажем теперь, что дробь f_1/g_1 является наилучшим приближением к дроби $\sqrt{d}/h_1$. В силу минимальности $m = 2t$ мы имеем $\deg h_1 \geqslant 1$. Рассмотрим подробнее уравнение (5.25). Запишем его в виде

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

Так как $|h_1|_{v'} = 0$, $|\sqrt{d}|_{v'} = 0$, то в силу предложения 2.1 мы можем считать, что

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

Разложим f_1 и g_1 по степеням v:

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

где $b_i, c_i \in \mathbb{F}_q$, $b_r \neq 0$, $c_s \neq 0$. Сравнивая степени в левой и правой частях уравнения (5.25), получаем $r < t/2$, $s < t/2$. Пусть $h = \max\{r, s\}$. Рассмотрим элемент $(\sqrt{d}/h_1)\overline{g}_1 - \overline{f}_1$, где

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

Так как $\overline{f}_1/\overline{g}_1$ имеет вид (5.11) и

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

то по теореме 5.4 дробь $\overline{f}_1/\overline{g}_1 = f_1/g_1$ является наилучшим приближением к $\sqrt{d}/h_1$. Тогда по теореме 5.6 $f_1/g_1 = p_n/q_n$ для некоторой подходящей дроби p_n/q_n к $\sqrt{d}/h$.

Теорема 5.8 доказана.

Отметим, что теорема 5.8 становится неверной в случае $\deg v > 1$. Обратимся к рассмотренным выше примерам 3.7 и 5.7. Фундаментальной S-единицей является элемент $\varepsilon = f + g\sqrt{d}$, где $f = 2x^5 + 2x^3 + 1$, $g = x$. Легко проверить, что $f/g \neq p_1/q_1$ и $f/g \neq p_2/q_2$. Тем более, f/g не совпадает ни с одной подходящей дробью p_n/q_n к $\sqrt{d}$ для $n > 2$, поскольку степень знаменателя всегда будет больше 1.

Теорема 5.8 дает алгоритм для вычисления фундаментальной S-единицы в случае $\deg v = 1$. Пусть $d_1, \dots, d_r$ – все делители многочлена d степени, не превосходящей $(1/2)\deg d$. Будем последовательно вычислять подходящие дроби к $\sqrt{d}$, $\sqrt{d}/d_1, \dots, \sqrt{d}/d_r$ и для каждой подходящей дроби p_n/q_n проверять, выполняется ли равенство (5.19). Как только мы найдем подходящую дробь p_n/q_n, удовлетворяющую (5.19), по формулам (5.20) находим решение f, g норменного уравнения (3.1). Тогда либо $f + g\sqrt{d}$, либо $f - g\sqrt{d}$ будет фундаментальной S-единицей.

Список литературы

[1] В. В. Беняш-Кривец, В. П. Платонов, “S-единицы в гиперэллиптических полях”, *УМН*, **62**:4 (2007), 149–150; англ. пер.: V. V. Benyash-Krivets, V. P. Platonov, “S-units in hyperelliptic fields”, *Russian Math. Surveys*, **62**:4 (2007), 784–786.

[2] В. В. Беняш-Кривец, В. П. Платонов, “Группы S-единиц в гиперэллиптических полях”, *Докл. РАН*, **417**:4 (2007), 446–450; англ. пер.: V. V. Benyash-Krivets, V. P. Platonov, “Groups of S-units in hyperelliptic fields”, *Dokl. Math.*, **76**:3 (2007), 886–890.

[3] В. В. Беняш-Кривец, В. П. Платонов, “Непрерывные дроби и S-единицы в гиперэллиптических полях”, *УМН*, **63**:2 (2008), 159–160; англ. пер.: V. V. Benyash-Krivets, V. P. Platonov, “Continued fractions and S-units in hyperelliptic fields”, *Russian Math. Surveys*, **63**:2 (2008), 357–359.

[4] В. В. Беняш-Кривец, В. П. Платонов, “Непрерывные дроби и S-единицы в функциональных полях”, *Докл. РАН*, **423**:2 (2008), 155–160; англ. пер.: V. V. Benyash-Krivets, V. P. Platonov, “Continued fractions and S-units in function fields”, *Dokl. Math.*, **78**:3 (2008), 833–838.

[5] А. Вейль, *Основы теории чисел*, Мир, М., 1972; пер. с англ.: A. Weil, *Basic number theory*, Springer-Verlag, New York, 1967.

[6] И. С. Иохвидов, *Ганкелевы и тёплицевы матрицы и формы. Алгебраическая теория*, Наука, М., 1974; англ. пер.: I. S. Iohvidov, *Hankel and Toeplitz matrices and forms. Algebraic theory*, Birkhäuser, Boston–Basel–Stuttgart, 1982.

[7] A. Böttcher, 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] С. Ленг, *Введение в теорию диофантовых приближений*, Мир, М., 1970; пер. с англ.: S. Lang, *Introduction to diophantine approximations*, Addison-Wesley, Reading, MA–London–Don Mills, ON, 1966.

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

[11] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Наука, М., 1964; англ. пер.: A. I. Borevich, I. R. Shafarevich, *Number theory*, Academic Press, New York–London, 1966.

В. В. Беняш-Кривец (V. V. Benyash-Krivets)
Белорусский государственный университет, г. Минск
E-mail: benyash@bsu.by

Поступила в редакцию
10.06.2009

В. П. Платонов (V. P. Platonov)
Научно-исследовательский институт
системных исследований РАН, г. Москва
E-mail: platonov@niisi.ras.ru