S-единицы в гиперэллиптических полях

В. В. Беняш-Кривец, В. П. Платонов

В настоящей заметке мы представляем некоторые результаты о вычислении групп S-единиц в гиперэллиптических полях.

Пусть $k = \mathbb{F}_q(x)$ – поле рациональных функций от одной переменной над конечным полем $\mathbb{F}_q$ характеристики $p > 2$ и $d(x) = a_0x^{2n+1} + a_1x^{2n} + \cdots + a_{2n+1} \in \mathbb{F}_q[x]$ – свободный от квадратов многочлен, $a_0 \neq 0$. Пусть $K = k(\sqrt{d})$. Для неприводимого многочлена $v \in \mathbb{F}_q[x]$ через $|\cdot|_v$ будем обозначать соответствующее нормирование на k. Пусть (α, β) – точка на кривой $y^2 = d(x)$, $\beta \neq 0$. Тогда нормирование $|\cdot|_{x-\alpha}$ имеет два продолжения на K. Эти продолжения будем обозначать $|\cdot|_1$ и $|\cdot|_2$. Неархимедово нормирование $|\cdot|_\infty$ имеет единственное продолжение на K, которое по прежнему будем обозначать через $|\cdot|_\infty$. Следующие два случая являются базисными для исследования S-единиц: 1) $S = \{|\cdot|_\infty, |\cdot|_1\}$; 2) $S = \{|\cdot|_\infty, |\cdot|_1, |\cdot|_2\}$. Пусть $\mathscr{O}_S$ – кольцо S-целых элементов в K, т. е. таких элементов $y \in K$, что $|y|_v \geqslant 0$ для всех нормирований $|\cdot|_v$ поля K, не принадлежащих S. Множество обратимых элементов U_S кольца $\mathscr{O}_S$ называется группой S-единиц поля K. В силу обобщенной теоремы Дирихле о единицах (см. [1; 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.

В классическом случае квадратичного расширения $L = \mathbb{Q}(\sqrt{d})$ поля $\mathbb{Q}$ фундаментальную единицу поля L можно найти, используя разложение $\sqrt{d}$ в цепную дробь [2]. Однако для функциональных полей метод цепных дробей не всегда позволяет найти фундаментальную единицу. Цель настоящей заметки – найти алгоритм для вычисления фундаментальных S-единиц гиперэллиптического поля K в указанных двух случаях.

Первое предложение носит технический характер.

Предложение 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* $|\cdot|_{v'}$ *на* K, *то* $|y|_{v'} = 0$.
3. *Если* $v \mid d$ *и* $v \nmid f$, *то* $|\cdot|_v$ *имеет единственное продолжение* $|\cdot|_{v'}$ *на* K *и* $|y|_{v'}=0$.
4. *Если* $v \mid d$ *и* $v \mid f$, *то* $|\cdot|_v$ *имеет единственное продолжение* $|\cdot|_{v'}$ *на* K *и* $|y|_{v'} = 1/2$.

Следующее предложение характеризует S-целые элементы в K.

Предложение 2. *Любой элемент* $y \in \mathscr{O}_S$ *имеет вид*

$$y = (f + g\sqrt{d})(x - \alpha)^{-m},$$

где $f, g \in \mathbb{F}_q[x]$, $m \geqslant 0$. *Если при этом* $m > 0$ *и* $x - \alpha$ *не делит одновременно* f *и* g, *то* $x - \alpha \nmid f$, $x - \alpha \nmid g$.

Для доказательства предложения 2 достаточно заметить, что если знаменатель y делится на неприводимый многочлен $v \neq x - \alpha$, то для некоторого продолжения $|\cdot|_{v'}$ нормирования $|\cdot|_v$ в силу предложения 1 $|y|_{v'} < 0$.

Отметим, что не любой элемент вида $(f + g\sqrt{d})(x - \alpha)^m$ является S-целым. Для дальнейшего нам важно знать, какие значения может принимать норменное отображение на S-единицах.

Предложение 3. *Если* $\varepsilon = (f + g\sqrt{d})/(x - \alpha)^{m_1} \in U_S$, *где* $f, g \in \mathbb{F}_q[x]$, *и если* $\varepsilon \notin \mathbb{F}_q^*$, *то* $f \neq 0$, $g \neq 0$, $(f, g) = 1$ *и* $N_{K/k}(\varepsilon) = a(x - \alpha)^m$, *где* $a \in \mathbb{F}_q^*$ *и* $0 \neq m \in \mathbb{Z}$.

Так же, как и в случае S-целых элементов, если элемент $\varepsilon \in K$ обладает свойством $N_{K/k}(\varepsilon) = a(x-\alpha)^m$, то из этого не следует, что ε является S-единицей. Однако следующее предложение показывает, что если норменное уравнение

$$f^2 - g^2 d = a(x-\alpha)^m, \tag{1}$$

где $m \neq 0$ фиксировано, имеет решение в многочленах $f, g \in \mathbb{F}_q[x]$, то либо $f + g\sqrt{d} \in U_S$, либо $f - g\sqrt{d} \in U_S$.

Предложение 4. *Пусть* $y = f + g\sqrt{d}$, *где* $f, g \in \mathbb{F}_q[x]$, *и пусть* $N_{K/k}(y) = a(x-\alpha)^m$, *где* $a \in \mathbb{F}_q^*$ *и* $m > 0$. *Тогда если* $|y|_2 = 0$, *то* $y = f + g\sqrt{d} \in U_S$, *а если* $|y|_2 > 0$, *то* $(f + g\sqrt{d})/(x-\alpha)^m \in U_S$.

Теорема 1. *Пусть* $S' = \{|\cdot|_\infty, |\cdot|_1, |\cdot|_2\}$, $S = \{|\cdot|_\infty, |\cdot|_1\}$. *Тогда если* ε – *фундаментальная* S-*единица*, *то* ε, $x - \alpha$ – *независимые фундаментальные* S'-*единицы*.

Для доказательства теоремы достаточно заметить, что если δ – произвольная S'-единица, то, как и в случае S-единиц, $N_{K/k}(\delta) = a(x-\alpha)^m$. Тогда в силу предложения 4 либо $\delta \in U_S$, либо $\delta/(x-\alpha)^m \in U_S$. В первом случае $\delta = b\varepsilon^t$, а во втором случае $\delta = b\varepsilon^t(x-\alpha)^m$, где $b \in \mathbb{F}_q^*$, $t \in \mathbb{Z}$. Это и означает, что ε, $x - \alpha$ – независимые фундаментальные S'-единицы.

Таким образом, в первую очередь нам необходимо уметь вычислить фундаментальную S-единицу. Для этого нужно найти минимальное натуральное m такое, что уравнение (1) имеет решение в многочленах $f, g \in \mathbb{F}_q[x]$. Тогда либо $f + g\sqrt{d}$, либо $f - g\sqrt{d}$ является фундаментальной S-единицей.

Обозначим $v = x - \alpha$, и пусть k_v – пополнение k относительно нормирования $|\cdot|_v$. Поле k_v можно отождествить с полем формальных степенных рядов $\mathbb{F}_q((v))$. Так как $|\cdot|_v$ имеет два продолжения на K, то $\sqrt{d} \in \mathbb{F}_q((v))$. Пусть $\sqrt{d} = \sum_{i=0}^{\infty} d_i v^i$. Следующая теорема дает алгоритм для нахождения фундаментальной S-единицы.

Теорема 2. *Пусть* $n = (\deg d - 1)/2$. *Для целого числа* $r \geqslant n$ *определим матрицы*

$$D_r = \begin{pmatrix} d_{n+1} & d_{n+2} & \dots & d_{r+1} \\ d_{n+2} & d_{n+3} & \dots & d_{r+2} \\ \dots & \dots & \dots & \dots \\ d_{n+r} & d_{n+r+1} & \dots & d_{2r} \end{pmatrix}, \qquad H_r = \begin{pmatrix} d_{n+2} & d_{n+3} & \dots & d_{r+2} \\ d_{n+3} & d_{n+4} & \dots & d_{r+3} \\ \dots & \dots & \dots & \dots \\ d_{n+r+1} & d_{n+r+2} & \dots & d_{2r+1} \end{pmatrix}.$$

Норменное уравнение (1) *с нечетным* $m = 2r + 1$ *имеет решение в ненулевых многочленах* $f, g \in \mathbb{F}_q[x]$ *тогда и только тогда*, *когда* $\operatorname{rank} D_r < r - n + 1$, *а с четным* $m = 2r$ – *тогда и только тогда*, *когда* $\operatorname{rank} H_{r-1} < r - n$.

Если K – поле эллиптической кривой, то матрицы D_r, H_r являются квадратными. В этом случае определители специального вида, возникающие в теореме 2, были впервые введены Якоби в XIX в. и носят название "персимметрический определитель" (persymmetric determinants), а матрицы такого вида называются "ганкелевыми матрицами" (Hankel matrices).

Замечание. Мы ограничились здесь нормированиями, связанными с точками на гиперэллиптической кривой над полем $\mathbb{F}_q$. В действительности аналогичные результаты справедливы для любых нормирований поля $\mathbb{F}_q(x)$.

Список литературы

[1] А. Вейль, *Основы теории чисел*, Мир, М., 1972. **[2]** З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Наука, М., 1964.

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

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

Представлено В. М. Бухштабером
Принято редколлегией
16.07.2007