

Федеральное государственное учреждение «Федеральный научный центр
Научно-исследовательский институт системных исследований Российской
академии наук»

На правах рукописи

Петрунин Максим Максимович

**S-единицы и функциональные непрерывные дроби в
гиперэллиптических полях**

Специальность 01.01.06 —
«Математическая логика, алгебра и теория чисел»

ДИССЕРТАЦИЯ
на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
академик РАН, доктор физико-математических наук, профессор
Платонов Владимир Петрович

Москва — 2019

Оглавление

	Стр.
Введение	4
Глава 1. Общий случай произвольной степени многочлена, определяющего гиперэллиптическое поле	24
1.1 Нормирования и непрерывные дроби	24
1.1.1 Нормирования	24
1.1.2 Непрерывные дроби	28
1.1.3 Наилучшие приближения	30
1.2 Квазипериодические непрерывные дроби и S -единицы	31
1.2.1 Квазипериодические и периодические непрерывные дроби .	31
1.2.2 Квадратичная иррациональность	34
1.2.3 Критерии квазипериодичности и периодичности	36
1.2.4 S и S_h -единицы	40
1.3 Периодичность квадратного корня	49
Глава 2. Случай нечетной степени многочлена, определяющего гиперэллиптическое поле	57
2.1 Симметрии разложения $\sqrt{f}$ и непрерывная дробь для $\sqrt{f}/h^s$	57
2.2 Квазипериодические, но не периодические элементы	60
2.3 Теорема Платонова и Беньаш-Кривеца о построении фундаментальной S -единицы	65
2.4 Разложение в непрерывную дробь элемента $\sqrt{f}/h^{g+1}$	68
Глава 3. Построение S-единиц больших степеней	77
3.1 Случай линейного нормирования	77
3.1.1 Базовый алгоритм метода непрерывных дробей	77
3.1.2 Алгоритм с вычислением коэффициентов подходящих дробей	79
3.1.3 Алгоритм без вычисления коэффициентов подходящих дробей	80

3.1.4	S -единицы больших степеней над $\mathbb{Q}$ в качестве поля констант	81
3.2	Случай нелинейного нормирования	88
3.2.1	Метод матричной линеаризации Платонова и Беняш-Кривеца	89
3.2.2	Алгоритм метода матричной линеаризации	91
3.2.3	S -единицы больших степеней	91
Заключение		93

Введение

Диссертация посвящена исследованию проблемы существования и построения S -единиц в гиперэллиптических полях над полем рациональных чисел, которая тесно связана с проблемой кручения в якобианах (якобиевых многообразиях) гиперэллиптических кривых. Также в диссертации исследуется связь указанных проблем с проблемой периодичности и квазипериодичности функциональных непрерывных дробей.

Вопросами, связанными с S -единицами, т.е. с элементами поля с нулевым значением нормирования, для нормирований не лежащих в конечном множестве S , в функциональном случае занимались многие математики, в числе которых Э. Артин [1] и В. П. Платонов. Проблема существования и построения S -единиц в функциональных полях представляет самостоятельный интерес, но в то же время её исследование мотивировано естественной связью S -единиц с точками кручения в якобианах гиперэллиптических кривых. Эта связь легла в основу предложенного в 2010 году В. П. Платоновым подхода к проблеме кручения, т.е. к проблеме описания подгрупп конечного порядка в якобианах гиперэллиптических кривых над числовыми полями.

В эллиптическом случае проблема кручения была полностью решена в 1977-1978 годах Б. Мазуром [2] для поля рациональных чисел: было доказано, что кручение ограничено, а также было дано описание всех возможных групп кручения.

Следующим естественным шагом является попытка получить решение проблемы кручения для гиперэллиптических кривых большего рода над полем рациональных чисел. Полное решение проблемы требует ответа на два вопроса: ограничено ли кручение и, если ограничено, то какие существуют порядки кручения? К настоящему моменту ответ на первый вопрос неизвестен даже для кривых рода 2. Последние 30 лет специалистам в этой области в основном удавалось получать результаты, связанные со вторым вопросом, и заключающиеся в нахождении кривых, якобианы которых обладают $\mathbb{Q}$ -точками кручения определенного порядка. Усилиями ряда исследователей (Е. Флин [3], Ф. Лепровост [4][5][6], Х. Огава [7], Н. Д. Элкис [8], Э. В. Хау [9][10] и других [11]) было доказано существование $\mathbb{Q}$ -точек кручения больших порядков в якобианах гиперэллиптических

кривых рода 2, определённых над $\mathbb{Q}$. Эти доказательства были получены с использованием различных методов, индивидуальных для отдельных порядков.

Пусть множество S состоит из двух нормирований гиперэллиптического поля, причём одно из них — единственное продолжение бесконечного нормирования поля рациональных функций, или оба нормирования сопряжены. Тогда нетривиальная группа S -единиц является прямым произведением мультипликативной группы поля констант и бесконечной циклической группы. Образующая циклической группы называется фундаментальной S -единицей. Предложенный В. П. Платоновым [12] новый подход к проблеме кручения в якобиевых многообразиях гиперэллиптических кривых над полем рациональных чисел был основан на построении фундаментальных S -единиц в соответствующих гиперэллиптических полях. Ранее в работе 2009 года [13] В. П. Платоновым и В. В. Беньш-Кривцем был развит математический аппарат и построены алгоритмы для нахождения фундаментальных S -единиц в гиперэллиптических полях, заданных многочленами f нечётной степени. С помощью указанного подхода в работах В. П. Платонова и М. М. Петрунина [14][15] было завершено доказательство гипотезы существования $\mathbb{Q}$ -точек любого порядка ≤ 30 , были единообразно построены все $\mathbb{Q}$ -точки простых порядков $p \leq 29$, а также было доказано существование $\mathbb{Q}$ -точек неизвестных ранее порядков в якобианах кривых рода 2.

Опираясь на полученные результаты, В. П. Платонов высказал предположение, что если рассмотреть S , состоящее из конечного и бесконечного нормирования, то порядки $\mathbb{Q}$ -точек кручения, как правило, будут определяться степенями фундаментальных S -единиц, эта числовая характеристика S -единицы была впервые введена в работе В. П. Платонова и М. М. Петрунина [16]. Одним из основных результатов диссертации является построение фундаментальных S -единиц больших степеней методами, основанными на подходе В. П. Платонова, с применением высокопроизводительных вычислений. Многие результаты настоящей диссертации в существенной степени получены с использованием симбиоза глубокой теории, эффективных алгоритмов и супервычислений.

Теория S -единиц в функциональных полях имеет глубокие связи с теорией функциональных непрерывных дробей и с проблемой периодичности функциональных непрерывных дробей. История изучения разложения квадратичных иррациональностей в функциональную непрерывную дробь восходит к Абелю [17] и Чебышеву [18]. Пусть множество S_∞ состоит из двух продолжений бесконечного нормирования поля $k(x)$ на гиперэллиптическое поле $L = k(x)(\sqrt{f})$, где k

— поле констант гиперэллиптического поля, $\text{char } k \neq 2$, а $f \in k[x]$. Существует связь кручения в якобиане гиперэллиптического поля L , S_∞ -единиц в L и разложения квадратного корня многочлена f , задающего L , в непрерывную дробь в поле формальных степенных рядов $k((1/x))$. Впервые указанная связь в современной трактовке была упомянута в работе 1980 года В. В. Адамса и М. Дж. Разара [19]. Различные аспекты функциональных непрерывных дробей в указанном случае исследовались также в работах А. Шинцеля, Дж. Ю, В. М. Шмидта, У. Цаньера, А. Дж. ван дер Пуртена, Т. Г. Бэрри и других авторов.

В. П. Платоновым и В. В. Беньш-Кривцем [13] было показано, что эффективная связь между нетривиальными S -единицами для S , состоящего из конечного и бесконечного нормирования, и функциональными непрерывными дробями возможна только в случае линейного нормирования, и была разработана теория функциональных непрерывных дробей для поля формальных степенных рядов $k((h))$, где h — линейный многочлен. Высокую эффективность метода построения S -единиц с помощью непрерывных дробей демонстрирует следующий факт: существование большей части известных к настоящему моменту порядков кручения в якобианах кривых рода 2 над $\mathbb{Q}$ может быть доказано путём построения S -единицы для множества S , содержащего линейное нормирование и бесконечное нормирование.

Кроме того, в вышеупомянутой работе было доказано, что для гиперэллиптических полей с конечным полем констант в случае линейного нормирования всякая квадратичная иррациональность, содержащаяся в соответствующем поле формальных степенных рядов, периодична, т.е. обладает периодическим разложением в непрерывную дробь. Таким образом, для конечного поля констант был сформулирован полный функциональный аналог теоремы Лагранжа: квадратичные иррациональности и только они представимы в виде бесконечных периодических непрерывных дробей. В случае функциональных непрерывных дробей с произвольным полем констант этот факт вообще говоря неверен. Более того, группа обратимых элементов кольца, элементами которого являются полные частные разложения в непрерывную дробь, может быть бесконечна. Это позволяет ввести понятие более слабое чем периодичность, а именно понятие квазипериодичности: непрерывная дробь является квазипериодической, если в бесконечной последовательности полных частных встречаются равные с точностью до мультипликативной константы элементы. Наличие элементов с квазипериодическим, но не периодическим разложением в непрерывную дробь, а

также наличие квадратичных иррациональностей с неквазипериодическим разложением в непрерывную дробь существенно отличает функциональный случай от классического случая числовых непрерывных дробей.

Для непрерывных дробей в $k((1/x))$ существование S_∞ -единиц поля $k(x)(\sqrt{f})$, $f \in k[x]$, связано с периодичностью элемента $\sqrt{f}$. Он является ключевым с точки зрения исследования периодичности и квазипериодичности непрерывных дробей в $k((1/x))$: элемент $\sqrt{f}$ периодичен всегда, когда поле $k(x)(\sqrt{f})$ содержит какие либо квазипериодические элементы, т.е. элементы с квазипериодическим разложением в непрерывную дробь [20][21]. Однако в рассматриваемом нами случае непрерывных дробей в $k((h))$, как показано в настоящей диссертации, даже при наличии в гиперэллиптическом поле периодических элементов элемент $\sqrt{f}$ квазипериодичен не всегда, а компьютерные вычисления демонстрируют, что квазипериодичность $\sqrt{f}$ сравнительно редкое явление. В 2017 году В. П. Платонову и Г. В. Фёдорову [22] удалось показать, что за исключением семейства $ch^3 + 1$, $c \in \mathbb{Q} \setminus \{0\}$, количество кубических многочленов f над $\mathbb{Q}$ с квазипериодическим разложением $\sqrt{f}$ в непрерывную дробь в $\mathbb{Q}((h))$ ограничено с точностью до естественной эквивалентности тремя примерами. Различные аспекты, связанные с квазипериодическим $\sqrt{f}$, исследовались также в работах В. П. Платонова, Г. В. Фёдорова, В. С. Жгуна [23][24] и других. В настоящей диссертации даны ответы на многие вопросы, связанные с квазипериодичностью и периодичностью непрерывных дробей элементов общего вида, а также исследованы свойства периодичности элементов, связанных с $\sqrt{f}$, в т.ч. элемента $\sqrt{f}$. Отметим, что доказательство периодичности квазипериодического $\sqrt{f}$ не может быть получено путём перенесения рассуждений о периодичности и симметриях разложения с числового случая, и требует иного подхода. В настоящей диссертации приведено доказательство этого факта, а также выведены другие свойства периодического элемента $\sqrt{f}$.

В. П. Платоновым и Г. В. Фёдоровым [25] были введены S_h -единицы, где S_h состоит из двух сопряженных конечных нормирований, связанных с неприводимым многочленом h . В случае $\deg f = 2g + 1$ бесконечное нормирование поля $k(x)$ обладает единственным продолжением на $k(x)(\sqrt{f})$, что позволяет сосредоточиться на рассмотрении S -единиц, которые при таком условии, как показано в настоящей диссертации, дают больше информации о кручении, чем более универсальные S_h -единицы.

С точки зрения исследования периодичности и квазипериодичности непрерывных дробей в $k((h))$ ключевым является элемент $\sqrt{f}/h^{g+1}$. В настоящей диссертации описаны свойства его разложения в непрерывную дробь, связь периода этого разложения и степени соответствующей S -единицы, а также получены утверждения о свойствах специальных многочленов, связанных с разложением квадратичной иррациональности в непрерывную дробь, и определяющих полное частное на шаге $n + 1$. Отметим, что свойства этих многочленов существенно используются в эффективных алгоритмах построения S -единиц, а сами многочлены тесно связаны с непрерывными дробями и многочленами Мамфорда, задающими дивизоры на гиперэллиптической кривой [26].

Каждая непрерывная дробь сходится к некоторому элементу из поля формальных степенных рядов. Если непрерывная дробь квазипериодическая, то этот элемент является квадратичной иррациональностью и лежит в соответствующем гиперэллиптическом поле. Отдельный интерес представляет описание свойств квазипериодических, но не периодических элементов, лежащих в гиперэллиптическом поле, задаваемом многочленом нечётной степени, и методы построения примеров таких элементов в явном виде. Указанные вопросы рассмотрены в настоящей диссертации.

Целью данной работы является:

- Получение критерия квазипериодичности элементов $\sqrt{f}$, $\sqrt{f}/h^{g+1}$ и более широкого класса элементов гиперэллиптического поля $k(x)(\sqrt{f})$ и поля формальных степенных рядов $k((h))$, где k — поле, $\text{char } k \neq 2$, $h, f \in k[x]$, $\deg h = 1$, $g = \lfloor \frac{\deg f - 1}{2} \rfloor$;
- Доказательство свойства периодичности квазипериодического разложения вышеуказанных элементов в непрерывную дробь;
- Описание свойств гиперэллиптического поля, определяемого многочленом нечётной степени, связанных с разложением элементов в непрерывную дробь. Установление связи между степенью фундаментальной S -единицы и квазипериодом разложения в непрерывную дробь элемента $\sqrt{f}/h^{g+1}$;
- Построение фундаментальных S -единиц новых степеней ≥ 20 для гиперэллиптических полей рода 2 над полем рациональных чисел.

Основные положения, выносимые на защиту.

- Критерий квазипериодичности разложения в непрерывную дробь в поле формальных степенных рядов $k((h))$ элементов вида $\frac{\sqrt{f}}{dh^s}$, где k — поле,

$\text{char } k \neq 2$, $h \in k[x]$, $\deg h = 1$, d — делитель бесквадратного многочлена $f \in k[x]$, а s — целое число.

- Теорема о периодичности квазипериодических разложений в непрерывную дробь в $k((h))$ элементов вида $\frac{\sqrt{f}}{dh^s}$, в частности, о периодичности квазипериодического разложения элемента $\sqrt{f}$. Существование нетривиальных примеров многочленов f , определяющих гиперэллиптическое поле, как с периодическим разложением $\sqrt{f}$ в непрерывную дробь, так и с неквазипериодическим разложением $\sqrt{f}$ в непрерывную дробь в $k((h))$.
- Необходимое условие квазипериодичности, но не периодичности разложения в непрерывную дробь в $k((h))$ элемента гиперэллиптического поля, определяемого многочленом нечётной степени.
- Оценки, связывающие степень фундаментальной S -единицы (и, таким образом, порядок некоторой точки кручения якобиана соответствующей гиперэллиптической кривой), квазипериод разложения в непрерывную дробь элемента $\sqrt{f}/h^{g+1}$, где $\deg f = 2g + 1$ и $g \in \mathbb{N}$, в $k((h))$ и номер шага n , на котором специальный вид принимают многочлены, связанные с разложением квадратичной иррациональности в непрерывную дробь. Существование элементов, на которых найденные оценки являются достижимыми.
- Эффективная программная реализация алгоритмов, являющихся развитием алгоритмов В. П. Платонова и В. В. Беняш-Кривеца поиска и построения фундаментальных S -единиц в гиперэллиптических полях для S , состоящего из конечного и бесконечного нормирования. Построение с помощью высокопроизводительных вычислений фундаментальных S -единиц больших степеней для гиперэллиптических полей рода 2 над полем рациональных чисел. Новое доказательство существования $\mathbb{Q}$ -точек кручения порядков 20, 21, ..., 30 и 32, 34, 36, 39, 40, 48 в якобианах кривых рода 2.

Основные результаты диссертации являются новыми и получены автором самостоятельно.

Теоретическая и практическая значимость.

Диссертация носит теоретический характер. Ее результаты могут быть полезны при исследовании функциональных непрерывных дробей, S -единиц и проблемы кручения. Кроме того, полученные результаты могут быть использованы в учебном процессе в рамках специальных курсов и семинаров.

Методология и методы исследования. В диссертации используются методы алгебры и алгебраической теории чисел, методы вычисления S -единиц, предложенные В. П. Платоновым и В. В. Беняш-Кривцем, методы алгебраической геометрии и методы теории функциональных непрерывных дробей, а также методы компьютерной алгебры, связанные с высокопроизводительными вычислениями.

Апробация работы. Результаты диссертации докладывались на следующих семинарах и международных научных конференциях:

1. XIV Международная конференция «Алгебра и теория чисел: современные проблемы и приложения», сентябрь 2016 года, Саратов;
2. XV Международная конференция «Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения» май 2018 года, Тула;
3. Научный-исследовательский семинар «По проблемам теоретической и прикладной алгебры и теории чисел» (рук. В. П. Платонов), ФГУ ФНЦ НИИСИ РАН, февраль 2019, Москва;
4. Научный семинар «Аналитическая теория чисел и приложения» (рук. В. Н. Чубариков), МГУ имени М.В. Ломоносова, Механико-математический факультет, март 2019, Москва;
5. Научно-исследовательский семинар кафедры высшей алгебры (рук. В. А. Артамонов), МГУ имени М.В. Ломоносова, Механико-математический факультет, апрель 2019, Москва.

Публикации. Основные результаты по теме диссертации изложены в 5 печатных изданиях, 4 из которых изданы в журналах, рекомендованных для защиты в диссертационном совете МГУ по специальности, 3 — в периодических научных журналах, индексируемых Web of Science и Scopus.

Объем и структура работы. Диссертация состоит из введения, трёх глав, и заключения. Полный объём диссертации составляет 97 страниц. Список литературы содержит 36 наименований.

Содержание работы

Во введении описывается структура диссертации и история рассматриваемых вопросов; обосновывается актуальность темы, описывается степень ее

разработанности; ставятся цели диссертации, указываются основные методы исследования и обосновывается научная новизна полученных результатов; описываются основные результаты и положения, выносимые на защиту.

Пусть k — поле характеристики отличной от 2 и $h \in k[x]$ — неприводимый над k многочлен. И пусть $f \in k[x]$ — свободный от квадратов многочлен, и $g = \lfloor \frac{\deg f - 1}{2} \rfloor$.

В первой главе приведены необходимые факты из теории нормирований, теории непрерывных дробей и теории S -единиц, введены основные определения и построена теория, описывающая поведение квазипериодических и периодических элементов в $k((h))$ в случае $\deg h = 1$. В качестве основного результата главы показана периодичность квазипериодического элементов вида $\frac{\sqrt{f}}{dh^s}$.

В параграфе §1.1 предлагается краткое изложение основных фактов из теории нормирований и функциональных непрерывных дробей в $k((h))$, которые потребуются нам для доказательства основных результатов диссертации.

Через v_h будем обозначать дискретное нормирование поля $k(x)$, задаваемое равенством $v_h(h^m \frac{a}{b}) = m$, где $a, b \in k[x]$, $h \nmid a$, $h \nmid b$, $m \in \mathbb{Z}$. Через v_∞ будем обозначать дискретное нормирование $v_\infty(a/b) = \deg b - \deg a$, $a, b \in k[x]$.

Пусть h — многочлен первой степени и пусть $\alpha = \sum_{j=e}^{\infty} b_j h^j$, где $b_j \in k$, элемент поля формальных степенных рядов $k((h))$. Обозначим через $[\alpha] = \sum_{j=e}^0 b_j h^j$ — сумму членов с неположительными, показателями степени h разложения α в ряд Лорана. Положим $A_0 = [\alpha]$ и $\alpha_i = \frac{1}{\alpha_{i-1} - A_{i-1}} \in k((h))$, $A_i = [\alpha_i]$.

В результате мы получим *непрерывную дробь*

$$A_0 + \frac{1}{A_1 + \frac{1}{A_2 + \frac{1}{A_3 + \dots}}}$$

Квазипериодическим будем называть такой элемент α поля $k((h))$, чье разложение в непрерывную дробь периодично с точностью до мультипликативной константы, т.е. если существуют такие $i, j \in \mathbb{Z}$, $c \in k \setminus \{0\}$, что $\alpha_i = c\alpha_j$. Мы будем использовать обозначение $\alpha = [A_0, \dots, A_{n-1}, \overline{B_1, \dots, B_t}^b]$ для элементов, которые разлагается в непрерывную дробь вида

$$\alpha = [A_0, \dots, A_{n-1}, B_1, B_2, \dots, B_t, bB_1, b^{-1}B_2, \dots, b^{-1}B_t, b^2B_1, b^{-2}B_2, \dots, b^{-2}B_t, b^3B_1, \dots],$$

а если $b = 1$, то будем писать, что $\alpha = [A_0, \dots, A_{n-1}, \overline{B_1, \dots, B_t}]$.

Отметим, что в случае бесконечного поля констант бесконечность множества обратимых элементов кольца $k[h^{-1}] = \{\sum_0^n a_i h^{-i} \mid a_i \in k, n \geq 0, n \in \mathbb{Z}\}$, т.е. кольца многочленов от h^{-1} , является одной из причин существования квазипериодических, но не периодических элементов. Последнее существенно отличает функциональные непрерывные дроби от числовых. В параграфе §1.2 даны основные определения и базовые факты, связанные с понятием квазипериодичности, а также показано, что квазипериодическим (и периодическим) может быть только элемент, являющийся квадратичной иррациональностью. В параграфе §1.2.2 приведены основные понятия и соотношения, связанные с разложением в непрерывную дробь квадратичной иррациональности. В частности, введены многочлены L_n и M_n , которые связаны с полным частным с номером $n + 1$ соотношением $\alpha_{n+1} = \frac{M_n + \lambda_2 \alpha}{L_n}$, где λ_2 — коэффициент минимального многочлена элемента α : $\lambda_2 \alpha^2 + \lambda_1 \alpha + \lambda_0 = 0$, $\lambda_0, \lambda_1, \lambda_2 \in k[x]$.

В параграфе §1.2.3 представлен критерий квазипериодичности произвольной квадратичной иррациональности: необходимо и достаточно проверить наличие решения в $k[h^{-1}]$, специального уравнения, зависящего от квадратичной иррациональности. А именно, функциональный аналог теоремы Лагранжа для поля $k((h))$ можно сформулировать следующим образом (для случая непрерывных дробей в $k((\frac{1}{x}))$ он был доказан Шмидтом).

Теорема 1 (Шмидт [20]). Пусть $\alpha \in k((h)) \setminus k(x)$, $\text{char } k \neq 2$.

Если α квазипериодичен, то α является квадратичной иррациональностью. Обратно, пусть α удовлетворяет уравнению

$$\Lambda_2 \alpha^2 + \Lambda_1 \alpha + \Lambda_0 = 0, \Lambda_2, \Lambda_1, \Lambda_0 \in k[h^{-1}], \text{НОД}(\Lambda_2, \Lambda_1, \Lambda_0) \in k. \quad (1)$$

Обозначим $D = \Lambda_1^2 - 4\Lambda_2\Lambda_0$. Тогда α разлагается в квазипериодическую непрерывную дробь в том и только том случае, когда соотношение:

$$Y^2 - DZ^2 = b \in k \setminus \{0\} \quad (2)$$

обладает нетривиальным решением относительно неизвестных $Y, Z \in k[h^{-1}]$ и некоторой неизвестной константы b , т.е. решением с $Z \neq 0$.

Указанный критерий позволяет выделить ключевой с точки зрения периодичности элемент гиперэллиптического поля.

Пусть $L = k(x)(\sqrt{f})$ — гиперэллиптическое поле. Предположим конечное нормирование ν_h поля рациональных функций от одного переменного $k(x)$, связанное с линейным многочленом h , обладает двумя продолжениями на L : ν_h^+ и ν_h^- , или, что то же самое, поле L имеет два вложения в $k((h))$. Зафиксируем одно из них. Тогда элементы поля L разлагаются в формальный степенной ряд по h .

Следствие 1. Пусть f — бесквадратный многочлен, и пусть разложение в непрерывную дробь некоторой квадратичной иррациональности $\alpha = \frac{v+w\sqrt{f}}{u} \in L$ квазипериодично, где $v, w, u \in k[x]$ и $\text{НОД}(v, w, u) \in k$. Тогда квазипериодична любая квадратичная иррациональность с дискриминантом $D = \frac{f}{h^{2g+2}} \in k[h^{-1}]$. В частности, квазипериодичен элемент $\frac{\sqrt{f}}{h^{g+1}}$.

Обратно, предположим, что элемент $\frac{\sqrt{f}}{h^{g+1}}$ квазипериодический. Тогда квадратичная иррациональность $\alpha = \frac{v+w\sqrt{f}}{u}$ обладает квазипериодическим разложением если и только, если уравнение (2) для $D = \frac{f}{h^{2g+2}} \in k[h^{-1}]$ имеет решение $Y, Z \in k[h^{-1}]$ такое, что $Z = Z'H$, где $H = h^{g+1-l}wu/r$, $Z' \in k[h^{-1}]$, $r = \text{НОД}(u, v^2 - w^2f)$ и $l = \max\{2 \deg u, \deg u + \deg v, \deg(v^2 - w^2f)\} - \deg r$.

Следствие 1 показывает, что квазипериодичность элемента поля L , не принадлежащего $k(x)$, возможна только при условии периодичности $\sqrt{f}/h^{g+1}$. Это позволяет считать элемент $\sqrt{f}/h^{g+1}$ ключевым с точки зрения изучения квазипериодических элементов поля L .

Следствие 2. Пусть $f = dd'$, где $d, d' \in k[x]$, $\deg d = t$, $\deg f = w$, $s \in \mathbb{Z}$. Квазипериодичность разложения следующих элементов равносильна: $\frac{\sqrt{f}}{h^{t+s}}, \frac{\sqrt{f}}{h^{w-(t+s)}}$, $\frac{\sqrt{f}}{dh^s}$, $\frac{h^s\sqrt{f}}{d'}$, $\frac{\sqrt{f}}{d'h^{2t+s-w}}$.

Следствие 2 показывает, что элемент $\frac{\sqrt{f}}{h^s}$ квазипериодический тогда и только тогда, когда квазипериодичен $\frac{\sqrt{f}}{h^{w-s}}$. В частности, при $\deg f = 2g + 1$ имеет место равносильность квазипериодичности элементов $\frac{\sqrt{f}}{h^g}, \frac{\sqrt{f}}{h^{g+1}}$.

Для квадратичной иррациональности $\alpha = \frac{v+w\sqrt{f}}{u}$ через $\alpha' = \frac{v-w\sqrt{f}}{u}$ будем обозначать элемент сопряженный к ней. В параграфе §1.2.3 для некоторых квазипериодических элементов показана их периодичность (аналогичный критерий для случая непрерывных дробей в $k((\frac{1}{x}))$ был доказан Шмидтом).

Теорема 2 (Шмидт [20]). Следующие условия на квазипериодический элемент $\alpha \in k((h))$ эквивалентны.

1. $\nu_h(\alpha) < 0$, $\nu_h(\alpha') \leq 0$, $\nu_h(\alpha - \alpha') < 0$ и $\alpha + \alpha' \in k[h^{-1}]$.

2. α разлагается в периодическую непрерывную дробь вида $[C_0, \overline{C_1, \dots, C_w}]$ с $C_i \in k[h^{-1}]$, $C_0 \neq C_w$, $v_h(C_0) < 0$ и $C_i = C_{w-i}$, для $i = 1, \dots, w-1$.

При выполнении условий выше имеют место симметрии $\alpha + \alpha' = 2C_0 - C_w$.

Откуда легко получить следствие.

Следствие 3. Элемент вида $\alpha_{d,s} = \frac{\sqrt{f}}{dh^s}$ для делителя d многочлена f и $s \neq 0 \in \mathbb{Z}$ квазипериодичен тогда и только тогда, когда он периодичен. Если его разложение периодично, то оно имеет вид $[\frac{1}{2}C_w, \overline{C_1, \dots, C_w}]$ при $s > 0$ и $[0, \frac{1}{2}C_w, \overline{C_1, \dots, C_w}]$ при $s < 0$. Причем $C_i = C_{w-i}$, для $i = 1, \dots, w-1$.

Пусть бесконечное нормирование поля $k(x)$ обладает одним продолжением на поле L (например, если $\deg f = 2g + 1$), тогда положим S — множество, состоящее из одного из двух продолжений конечного нормирования и бесконечного нормирования. А в более общем случае без ограничений на количество продолжений бесконечного нормирования положим S_h — множество, состоящее только из двух продолжений конечного нормирования. Обратимые элементы кольца S -целых (соответственно S_h -целых), образуют мультипликативную группу и называются S -единицами (S_h -единицами). Указанная группа, если она нетривиальна, изоморфна произведению $k \setminus \{0\}$ и бесконечной циклической группы. Образующая бесконечной циклической группы называется фундаментальной S -единицей (соответственно, S_h -единицей).

В параграфе §1.2.4 описаны основные факты и понятия, касающиеся S -единиц и S_h -единиц, введено понятие степени S и S_h -единицы, а также установлена связь между периодичностью ключевого элемента, наличием нетривиальных S и S_h -единиц и нетривиальностью группы кручения якобиана гиперэллиптического поля $k(x)(\sqrt{f})$.

Определение 1. Степенью S -единицы $u = \mu_1 + \mu_2\sqrt{f}$, $\mu_1, \mu_2 \in k(x)$, называется число $\deg u = m$, где m — показатель степени многочлена h в норменном уравнении $N(u) = \mu_1^2 - \mu_2^2 f = bh^m$, $b \in k \setminus \{0\}$.

Определение 2. Степенью S_h -единицы $u = \frac{\mu_1 + \mu_2\sqrt{f}}{h^m}$, $\mu_1, \mu_2 \in k[x]$, $\text{НОД}(\mu_1, \mu_2) \in k$, называется число $\deg u = m$, где m — показатель степени многочлена h в знаменателе u .

В параграфе §1.2.4 показана корректность вышеприведенных определений.

Предложение 1. Пусть $\deg h = 1$. Следующие три утверждения эквивалентны:

1. Выполнено соотношение $\mu_1^2 - \mu_2^2 f = bh^m$ для некоторого целого m и подходящих $\mu_1, \mu_2 \neq 0 \in k[x]$, $b \in k \setminus \{0\}$, $v_h(\mu_2) = 0$, а $\max\{2 \deg \mu_1, 2 \deg \mu_2 + \deg f\} = m \in \mathbb{Z}$. Если m — чётное, то обозначим $m' = m/2$, и $m = m'$ в противном случае.
2. Существуют $Z, Y \in k[h^{-1}]$, $Z \neq 0$ и $b \in k \setminus \{0\}$, $m' = -v_h(Y)$ такие, что

$$Y^2 - Z^2 \frac{f}{h^{2g+2}} = b. \quad (3)$$

3. Существует нетривиальная S_h -единица степени m' .

Если дополнительно известно, что бесконечное нормирование имеет одно продолжение на поле L , то условия выше равносильны следующему

4. Существует нетривиальная S -единица степени m' .

Рассмотрим аффинную кривую, заданную уравнением $y^2 = f(x)$. Ей соответствует гладкая проективная гиперэллиптическая кривая C с полем рациональных функций $L = k(x)(\sqrt{f})$. Пусть $\Delta^\circ(C)$ — группа классов дивизоров степени ноль гиперэллиптической кривой C . В записи дивизора для упрощения обозначений будем плейс, соответствующий нормированию, обозначать тем же символом, что и нормирование. Имеет место следующая связь S и S_h -единиц гиперэллиптического поля L и проблемы кручения в якобиане соответствующей кривой C .

Предложение 2. Пусть h — неприводимый многочлен произвольной степени такой, что v_h имеет два продолжения на поле L : v_h^+ и v_h^- . Поле L обладает фундаментальной S_h -единицей степени n тогда и только тогда, когда класс дивизора $v_h^+ - v_h^-$ имеет конечный порядок n в $\Delta^\circ(C)$.

В случае, когда бесконечное нормирование имеет одно продолжение на гиперэллиптическое поле, аналогичное утверждение верно и для S -единиц.

Предложение 3. Пусть h — неприводимый многочлен произвольной степени такой, что v_h имеет два продолжения на поле L : v_h^+ и v_h^- . Тогда поле L обладает фундаментальной S -единицей степени n тогда и только тогда, когда класс дивизора $v_h^+ - \deg h v_\infty$ имеет конечный порядок n в $\Delta^\circ(C)$. Более того, имеет место соотношение $v_h^+ - v_h^- \sim 2(v_h^+ - \deg h v_\infty)$.

В случае функциональных непрерывных дробей в $k((1/x))$ ключевым с точки зрения исследования периодичности и квазипериодичности является элемент

$\sqrt{f}$. Этот элемент периодичен в случае, когда поле $L = k(x)(\sqrt{f})$ содержит периодические элементы, однако в случае непрерывных дробей в $k((h))$ даже наличие в поле L периодических элементов не гарантирует периодичность разложения $\sqrt{f}$. Более того, компьютерные вычисления показывают, что даже при наличии периодических элементов в поле L периодичность разложения $\sqrt{f}$ — сравнительно редкое явление. Параграф §1.3 посвящен вопросу изучения периодичности $\sqrt{f}$ и, более общо, изучению периодичности элементов вида $\frac{\sqrt{f}}{dh^s}$, где d — делитель многочлена f (в том числе при $d = 1$), а s — целое число. Его итогом является следующая теорема.

Теорема 3. Пусть $s \in \mathbb{Z}$, $f \in k[x]$ — свободный от квадратов многочлен произвольной степени, $d \in k[x]$ — делитель многочлена f , и $h \in k[x]$ — линейный многочлен. Квазипериодичность разложения в функциональную непрерывную дробь элементов вида $\frac{\sqrt{f}}{dh^s}$ в $k((h))$, в т.ч. элемента $\sqrt{f}$, равносильна их периодичности.

Следующий критерий позволяет эффективно проверять на квазипериодичность разложения в непрерывную дробь элементов вида $\sqrt{f}/h^s$.

Теорема 4. Пусть f — беквадратный многочлен. Элемент $\alpha = \frac{\sqrt{f}}{h^s}$, $s \in \mathbb{Z}$ квазипериодичен тогда и только тогда, когда существует такая пара Y, Z , являющаяся решением уравнения (3), где $Z = Z'h^{-l}$ и $Y, Z' \in k[h^{-1}]$, $l = \max\{s - \lceil \frac{\deg f}{2} \rceil, \lfloor \frac{\deg f}{2} \rfloor - s\}$.

Более того, если $\deg f = 2g + 1$, то достаточно рассматривать только решение уравнения (3) с максимальным значением $v_h(Y) < 0$. Такое решение соответствует фундаментальной S -единице чётной степени или квадрату фундаментальной S -единицы нечётной степени.

В частности, теорема 4 даёт критерий квазипериодичности $\sqrt{f}$. Он квазипериодичен тогда и только тогда, когда найдётся решение с $-l \geq g + 1$ в случае, если $\deg f = 2g + 2$, или решение с $-l \geq g$ в случае, если $\deg f = 2g + 1$.

Над полем $\mathbb{Q}$ для $\deg f = 3$ из ограниченности числа нетривиальных периодических элементов $\sqrt{f}$ и теоремы 4 следует, что квазипериодических элементов с $\sqrt{f}/h^s$ с $s < 0$ или $s > \deg f$ не существует. Кроме того, даже с использованием компьютерных вычислений автору не удалось построить примеры таких элементов для $\deg f > 3$. Автору неизвестны такие примеры и автор полагает, что, вероятно, их не удастся найти. Теорема 4 показывает, что если элемент $\sqrt{f}/h^s$

квазипериодичен для некоторого $s = s_0 \leq \frac{\deg f}{2}$, то он периодичен для всех s из диапазона $s_0 \leq s \leq \frac{\deg f}{2}$. Вышесказанное дополнительно мотивирует к изучению элементов с “пограничным” значением $s = 0$.

Если для конечного поля констант в функциональном случае, как и в числовом случае, всякая квадратичная иррациональность периодична, то поиск примеров многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь для числового поля констант в функциональном случае — трудная задача. Теорема позволяет построить примеры многочленов f с периодичным разложением $\sqrt{f}$ в непрерывную дробь в $k((h))$. В настоящей диссертации построено два таких примера для $k = \mathbb{Q}$ и $h = x$: “тривиальная” серия для $f = ax^w + 1$, где $w \in \mathbb{N}$, и нетривиальный пример для $g = 2$, полученный с использованием высокопроизводительных компьютерных вычислений, связанных с применением эффективных алгоритмов построения фундаментальной S -единицы и результатов диссертации: $f = 4x^5 - 8x^4 + 12x^3 - 16x^2 + 20x + 25$.

Доказательство теоремы 3 требует нескольких вспомогательных утверждений. Выше мы видели, что методами параграфа §1.2.3 удастся доказать, что для делителя d многочлена f всякий квазипериодический элемент вида $\frac{\sqrt{f}}{dh^s}$ для $s \neq 0$ является периодическим. Однако эти методы неприменимы к элементу $\sqrt{f}$, и доказательство периодичности квазипериодического $\sqrt{f}$ в общем случае требует иного подхода, изложенного в §1.3. Ключевую роль в доказательстве этого факта играет следующее свойство многочлена $L_n = h^{2s}P_n^2 - Q_n^2f$, $b \in k \setminus \{0\}$, где P_n/Q_n — n -ая подходящая дробь к $\sqrt{f}/h^s$, для случая $s = 0$.

Лемма 1. Пусть многочлен $f \in k[x]$ свободен от квадратов, а нормирование v_h поля $k(x)$ имеет два продолжения на L , и пусть $\sqrt{f} \in k((h))$ квазипериодичен. Тогда существует делитель d многочлена f такой, что для некоторого n выполнено $L_n = bdh^w$, причём $w + \deg d = \deg f$, $b \in k \setminus \{0\}$, а $0 \leq \deg d < \deg f$.

Обозначим через $\{\alpha\} = \sum_1^\infty b_j h^j$ — сумму членов с положительными, показателями степени h разложения α в ряд Лорана. С помощью леммы удаётся доказать теорему:

Теорема 5. Пусть многочлен f свободен от квадратов, нормирование v_h поля $k(x)$ имеет два продолжения на $k(x)(\sqrt{f})$, а $\alpha = \sqrt{f}$ квазипериодичен. Тогда существует делитель d многочлена f , такой что $\{\alpha_{n+1}\} = b\{\frac{\sqrt{f}}{dh^w}\}$, где $\deg d = t$, $0 \leq \deg d < \deg f$, $w = \deg f - t$, а $b \in k \setminus \{0\}$.

Из теоремы 5 вытекает следствие о периодичности $\sqrt{f}$, которое завершает доказательство теоремы 3 в общем случае:

Следствие 4. В условиях теоремы 5 пусть $\sqrt{f}$ квазипериодичен. Тогда $\sqrt{f}$ — не-
периодичен.

Теорема 5 позволяет также сделать вывод о симметриях в разложении $\sqrt{f}$ в непрерывную дробь:

Следствие 5. В условиях теоремы 5 выполнено $\sqrt{f} = [A_0, \dots, A_{n+1}, \overline{B_1, \dots, B_N}]$, где $B_i = B_{N-i}$, для $i = 1, \dots, N - 1$.

Вторая глава посвящена случаю $\deg f = 2g + 1$ и $\deg h = 1$. Пусть многочлен f свободен от квадратов, а нормирование v_h поля $k(x)$ имеет два продолжения: v_h^+ , v_h^- на $L = k(x)(\sqrt{f})$. Положим множество S состоит из v_h^+ и бесконечного нормирования. Основным результатом главы является установление связи между степенью фундаментальной S -единицы и периодом разложения в непрерывную дробь ключевого элемента $\sqrt{f}/h^{g+1}$. Помимо этого доказаны и другие полезные для понимания этого случая факты. В частности, утверждения из параграфа §1.3, для многочлена f нечётной степени могут быть обобщены на более широкий класс элементов, что и сделано в параграфе §2.1. А именно, доказаны следующие два утверждения.

Лемма 2. Пусть $s > 0$, $\deg f = 2g + 1$ или $\deg f = 2g + 2$ и элемент $\alpha = \sqrt{f}/h^s$ — квазипериодичен. Тогда найдется такой номер n , для которого выполнено $L_n = bh^{2s}$, $b \in k \setminus \{0\}$.

Пусть теперь $\deg f = 2g + 1$, $s \geq 0$, элемент $\alpha = \sqrt{f}/h^s$ квазипериодичен и дополнительно известно, что поле L обладает нетривиальной S -единицей нечётной степени. Тогда найдется такой номер n , для которого выполнено $L_n = bh^{2g+1}$, $b \in k \setminus \{0\}$.

Лемма позволяет в случае поля L , обладающего S -единицей нечётной степени, обобщить результат теоремы 5 на более широкий класс элементов.

Теорема 6. Пусть $0 \leq s \leq g$, $\deg f = 2g + 1$ и $\alpha = \sqrt{f}/h^s$ — квазипериодичен, и пусть поле L обладает S -единицей нечётной степени. Тогда существует n такое, что $b\{\alpha_{n+1}\} = \{\sqrt{f}/h^{2g+1-s}\}$, где $b \in k \setminus \{0\}$.

Теорема 6 позволила построить пример, демонстрирующий существенное различие между случаями существования в поле L фундаментальной S -единицы чётной и нечётной степени. Отметим, что для f нечётной степени $2g+1$ при наличии нетривиальной S -единицы элементы $\sqrt{f}/h^g$ и $\sqrt{f}/h^{g+1}$ периодичны всегда. Построенный в настоящей диссертации пример показывает, что для полей, содержащих S -единицы только четных степеней утверждение теоремы 6 вообще говоря не верно.

В параграфе §2.1 также получено обобщение утверждения о симметриях разложения $\sqrt{f}$ в непрерывную дробь в $k((h))$ и построены примеры иллюстрирующие следующее следствие.

Следствие 6. В условиях теоремы 6 для $\alpha = \sqrt{f} = [A_0, A_1, \dots]$ выполняется $A_{n+1} = 2/b[\sqrt{f}/h^{2g+1}]$. Более того, $\sqrt{f} = [A_0, \dots, A_n, \overline{B_1, \dots, B_N}]$, где $B_i = B_{N+2-i}$, для $i = 2, \dots, N$.

Как отмечалось выше, квазипериодические, но не периодические элементы существенно отличают случай функциональных непрерывных дробей над произвольным полем констант от случая числовых непрерывных дробей. Параграф §2.2 посвящен таким элементам. Несмотря на то, что каждая непрерывная дробь сходится к некоторому элементу из $k((h))$, автору неизвестны примеры в литературе явного вида элементов, обладающих квазипериодическим, но не периодическим разложением в функциональную непрерывную дробь.

Обозначим для $B = b_0 + b_{-1}h^{-1} + \dots + b_{-n}h^{-n} \in k[h^{-1}]$ значение свободного коэффициента за $\text{fc}(B) = b_0$. В параграфе §2.2 найдены необходимые условия на то, что чистоквазипериодический, но не периодический элемент лежит в поле L , определённом многочленом нечётной степени, а также построены элементы, разлагающиеся в чистоквазипериодические, но не периодические функциональные непрерывные дроби малых квазипериодов.

Теорема 7. Квазипериодический, но не периодический, элемент $\alpha = [A_0, A_1, \dots, A_{2m-1}^c]$, $c \in k \setminus \{0\}$, $A_i \in k[h^{-1}]$, лежит в $k(x)(\sqrt{f})$ для некоторого многочлена f нечётной степени только, если $\text{fc}(Q_{2m-2}) + c \text{fc}(P_{2m-1}) = \pm 2\sqrt{c}$, где P_i/Q_i — i -ая подходящая дробь к α .

Отсюда, в частности, следует, что коэффициент квазипериодичности c для элементов гиперэллиптического поля, определённого многочленом нечётной степени, может быть только полным квадратом в k .

В параграфе §2.3 приводится теорема В. П. Платонова и В.В. Беньш-Кривеца для произвольного поля k характеристики отличной от 2, сформулированная в оригинале для случая конечного поля констант.

В параграфе §2.4 рассмотрено разложение в непрерывную дробь ключевого с точки зрения периодичности в гиперэллиптическом поле элемента $\sqrt{f}/h^{g+1}$ и его связь с S -единицами, и $\deg f = 2g + 1$. В параграфе §2.4 показано, что отличие от классического случая, где фундаментальная единица может быть найдена по многочлену L_{n-1} , где n — длина квазипериода, в рассматриваемом нами случае это не всегда так. Напомним, что фундаментальной единицей называется образующий элемент группы обратимых элементов кольца S_∞ -целых, где S_∞ — множество, состоящее из двух продолжений на поле L бесконечного нормирования поля $k(x)$.

Предложение 4. Пусть $\deg f = 2g + 1$, и $n \geq 0$ такое число, при котором $L_n = bh^r$, $b \in k \setminus \{0\}$.

Тогда $r = 2g + 1$ в том и только том случае, когда степень S -единицы поля $k(x)(\sqrt{f})$ является нечетным числом m , и $r = 2g + 2$ в противном случае.

Для случая $\deg f = 2g + 2$ построен контрпример к указанному предложению.

Теорема 8. Пусть $\deg f = 2g + 1$, и $\alpha = \sqrt{f}/h^{g+1}$. Фундаментальная S -единица поля $k(x)(\sqrt{f})$ существует тогда и только тогда, когда разложение α в непрерывную дробь периодически. Пусть фундаментальная S -единица существует и ее степень равна m , и пусть $n \geq 1$ — минимальное такое число, при котором $\deg L_{n-1} = \nu_h(L_{n-1})$. Возможны два случая:

1. m является четным числом, тогда $\deg L_{n-1} = 2g + 2$. При этом длина квазипериода равна n , а длина периода в этом случае равна либо n либо $2n$,
2. m является нечетным числом, тогда $\deg L_{n-1} = 2g + 1$. При этом длина периода совпадает с длиной квазипериода и равна $2n$.

В диссертации показано, что разложение $\sqrt{f}/h^{g+1}$ в непрерывную дробь обладает симметриями, а также уточнены оценки [27], связывающие степень фундаментальной S -единицы (как следствие, и порядок некоторой точки кручения якобиана соответствующей гиперэллиптической кривой) и длину периода ключевого элемента.

Следствие 7. Пусть $\deg f = 2g + 1$, и пусть $k(x)(\sqrt{f})$ обладает фундаментальной S -единицей степени m . И пусть N — длина квазипериода разложения α в непрерывную дробь, а $\delta = -v_h(A_1)$. Тогда

$$N + 2g - 1 \leq m \leq (g + 2 + \delta)N.$$

Более того, если m — нечётное число, то выполнено соотношение

$$N + 2g - 1 \leq m \leq (g + 2 + \delta)N/2,$$

иначе выполнено

$$2(N + g) \leq m \leq (g + 2 + \delta)N.$$

Завершают параграф §2.4 примеры, показывающие, что границы приведённых в следствии оценок достижимы.

Третья глава посвящена построению S -единиц больших степеней в гиперэллиптических полях рода 2 над полем рациональных чисел, и основным её результатом является построение фундаментальных S -единиц степеней 20, 21 . . . , 30 и 32, 34, 36, 39, 40, 48, откуда по предложению 3 следует существование $\mathbb{Q}$ -точек кручения соответствующих порядков в якобианах кривых рода 2.

Для случая линейного нормирования в настоящий момент наилучшими с точки зрения вычислительной сложности являются алгоритмы поиска и построения S -единиц, основанные на подходе с использованием непрерывных дробей. В параграфе §3.1 приводятся такие алгоритмы, а также способы их оптимизации. В частности, приводится алгоритм с фиксированным количеством операций на каждом шаге. С помощью программной реализации упомянутых алгоритмов, оптимизированной для исполнения на гетерогенном программно-аппаратном вычислительном комплексе, были построены S -единицы больших степеней для гиперэллиптических полей рода 2 с полем рациональных чисел в качестве поля констант.

Пусть

$$\begin{aligned} f_{20} &= (4x^4 - 2x + 1)(2x + 1), & h_{20} &= x - 1; \\ f_{21} &= 8x^5 - 7x^4 + 6x^3 - x^2 + 2x + 1, & h_{21} &= x - 1; \\ f_{22} &= (16x^4 - 16x^3 + x + 1)(x + 1), & h_{22} &= x - 1; \\ f_{23} &= -24x^5 + 153x^4 - 36x^3 - 8x^2 - 8x + 4, & h_{23} &= x - 1; \\ f_{24} &= (8x^4 - 5x^3 + 14x^2 - 12x + 8)(3x + 2), & h_{24} &= x - 2; \end{aligned}$$

$$\begin{aligned}
f_{25} &= 972x^5 + 900x^4 - 900x^3 + 165x^2 + 30x + 1, & h_{25} &= x - \frac{1}{3}; \\
f_{26} &= -(4x^4 - 21x^3 + 24x^2 + 9x - 18)(3x + 2), & h_{26} &= x - 2; \\
f_{27} &= 16x^5 + 57x^4 + 70x^3 + 39x^2 + 10x + 1, & h_{27} &= x; \\
f_{28} &= (9x^3 - 8x^2 + 20x + 16)(4x^2 + x + 4), & h_{28} &= x - \frac{4}{3}; \\
f_{29} &= 32x^5 - 47x^4 + 20x^3 + 2x^2 - 4x + 1, & h_{29} &= x - 1; \\
f_{30} &= -(32x^4 - 33x^3 - 123x^2 - 63x - 9)(x + 1), & h_{30} &= x + \frac{3}{4}; \\
f_{32} &= -(16x^4 - 99x^3 - 228x^2 - 135x - 18)(3x + 2), & h_{32} &= x; \\
f_{34} &= -(32x^3 - 59x^2 + 28x - 4)(27x^2 - 20x + 4), & h_{34} &= x; \\
f_{36} &= (3x^4 + 28x^3 - 8x^2 - 8x + 12)(4x + 3), & h_{36} &= x + 2; \\
f_{39} &= 192x^5 + 337x^4 - 1056x^3 + 852x^2 - 288x + 36, & h_{39} &= x - \frac{3}{4};
\end{aligned}$$

тогда выполнена следующая теорема.

Теорема 9. Пусть $S_j = \{\mathbf{v}_{h_j}^+, \mathbf{v}_\infty\}$, тогда для $j = 20, \dots, 30, 32, 34, 36, 39$ поле $L_j = \mathbb{Q}(x)(\sqrt{f_j})$ обладает фундаментальной S_j -единицей, степень которой равна j и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана J_{f_j} .

Метод непрерывных дробей является эффективным методом вычисления S -единиц для S , указанного выше вида. Однако, как отмечалось В. П. Платоновым и В. В. Беняш-Кривцем, он эффективно работает только в случае $\deg h = 1$. Следовательно, для некоторых гиперэллиптических полей непосредственное его применение не позволяет построить фундаментальную S -единицу. Для более общего случая в параграфе §3.2.1 использован метод матричной линейаризации. Точно также как и в случае метода непрерывных дробей авторами метода в оригинальной работы были доказаны результаты для случая конечного поля констант. В параграфе §3.2.1 приведены основные результаты, относящиеся к данному методу для случая поля $\mathbb{Q}$ в качестве поля констант и сформулирован алгоритм. Программная реализация и оптимизация алгоритма позволили построить фунда-

ментальные S -единицы степеней 40 и 48. Пусть

$$\begin{aligned} f_{40} &= -(64x^4 - 125x^3 - 250x^2 - 160x - 32)(5x + 2), & h_{40} &= x^2 - \frac{14}{5}x - \frac{8}{5}; \\ f_{48} &= (64x^4 + 225x^3 + 264x^2 + 117x + 18)(x + 2), & h_{48} &= x^2 + \frac{1}{4}x - \frac{3}{2}; \end{aligned}$$

тогда выполнена следующая теорема

Теорема 10. Пусть $S_j = \{\mathfrak{v}_{h_j}^+, \mathfrak{v}_\infty\}$, тогда для $j = 40, 48$ поле $L_j = \mathbb{Q}(x)(\sqrt{f_j})$ обладает фундаментальной S_j -единицей, степень которой равна j и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана J_{f_j} .

Таким образом, в качестве следствия из существования S -единиц больших степеней получено новое доказательство существования $\mathbb{Q}$ -точек кручения порядков 20, 21 . . . , 30 и 32, 34, 36, 39, 40, 48 в якобианах кривых рода 2.

В заключении приведены основные результаты работы.

Глава 1. Общий случай произвольной степени многочлена, определяющего гиперэллиптическое поле

1.1 Нормирования и непрерывные дроби

1.1.1 Нормирования

Напомним основные факты и определения из теории нормирований, необходимые нам для изложения.

Определение 3. Пусть K — поле. Нормирование v на K — это вещественнозначная функция $z \mapsto v(z)$ на K , удовлетворяющая следующим условиям:

1. $v(zu) = v(z) + v(u)$ для всех $z, u \in K$.
2. $v(z + u) \geq \min\{v(z), v(u)\}$.

Нормирование, группа значений которого является циклической, называется дискретным нормированием.

Пусть $h(x) \in k[x]$ — неприводимый над k многочлен. Через v_h будем обозначать дискретное нормирование поля $k(x)$, задаваемое равенством

$$v_h \left(h(x)^m \frac{a(x)}{b(x)} \right) = m,$$

где $a(x), b(x) \in k[x]$, $h(x) \nmid a(x)$, $h(x) \nmid b(x)$, $m \in \mathbb{Z}$.

Через v_∞ будем обозначать дискретное нормирование $v_\infty(a/b) = \deg b - \deg a$, $a, b \in k[x]$.

Предложение 5 ([28], Предложение 2, §2, гл. XII). Существует пара (K_v, i) , состоящая из поля K_v , полного относительно некоторого нормирования v и вложения $i : K \rightarrow K_v$, такого, что нормирование на K индуцируется нормированием на K_v (т. е. $v(z) = v(i(z))$ для $z \in K$). При этом iK плотно в K_v . Если (K'_v, i') — другая такая пара, то существует однозначно определенный изоморфизм $\phi : K_v \rightarrow K'_v$, сохраняющий нормирования, для которого коммутативна

следующая диаграмма:

$$\begin{array}{ccc} K_\nu & \xrightarrow{\varphi} & K'_\nu \\ & \nwarrow i \quad \nearrow i' & \\ & K & \end{array}$$

Определение 4. Пара (K_ν, i) , фигурирующая в предложении 5, называется некоторым пополнением K . Стандартная пара, полученная с помощью конструкции, использующей последовательности Коши (см. [28, доказательство предложения 2, §2, гл. XII]), называется пополнением K .

Далее по тексту мы будем писать K_ν и отождествлять K с iK . Единственное продолжение нормирования ν на K_ν по-прежнему будем обозначать через ν .

Предложение 6 ([28], Предложение 4, §2, гл. XII). Пусть K — поле, полное относительно нетривиального нормирования ν , и E — произвольное алгебраическое расширение K . Тогда ν имеет единственное продолжение на E . Если E конечно над K , то E полное.

Таким образом, можно утверждать, что нормирование ν может быть продолжено на пополнение K_ν , а затем однозначно продолжено на его алгебраическое замыкание $\overline{K_\nu}$. Если E — конечное расширение K или даже произвольное алгебраическое расширение, то мы можем продолжить ν на E , вложив E в $\overline{K_\nu}$ посредством изоморфизма над K и взяв индуцированное нормирование на E . Более того, всякое продолжение ν может быть получено этим способом.

Предложение 7 ([28], Предложение 6, §3, гл. XII). Пусть E — конечное расширение поля K , ν' — некоторое нормирование на E , продолжающее ν , $E_{\nu'}$ — соответствующее пополнение и $K_{\nu'}$ — замыкание K в $E_{\nu'}$, причем E отождествлено с подполем в $E_{\nu'}$. Тогда $E_{\nu'} = EK_{\nu'}$ (композиция).

Определение 5. Пусть даны два вложения $\sigma, \tau : E \rightarrow \overline{K_\nu}$ мы будем говорить, что они сопряжены над K_ν , если существует автоморфизм λ поля $\overline{K_\nu}$ над K_ν , для которого $\sigma = \lambda\tau$.

Предложение 8 ([28], Предложение 7, §3, гл. XII). Пусть E — алгебраическое расширение K . Два вложения $\sigma, \tau : E \rightarrow \overline{K_\nu}$ тогда и только тогда приводят к одному и тому же нормированию на E , когда они сопряжены над K_ν .

Чтобы понять, как устроена ситуация в случае $K = k(x)$ и квадратичного расширения $L = K(\sqrt{f})$ нам понадобится ещё одно утверждение из [28].

Предложение 9 ([28], Предложение 8, §2, гл. VII). Пусть k — поле и $\sigma : k \rightarrow L$ — вложение k в алгебраически замкнутое поле L . Пусть $E = k(\alpha)$, где α алгебраичен над k . И пусть p — неприводимый многочлен элемента α , и α является его корнем.

Тогда число возможных продолжений σ на E равно числу различных корней p .

Наконец, мы сможем сформулировать утверждение о продолжении нормирований в интересующем нас случае.

Предложение 10. Пусть $L = K(\alpha)$ — квадратичное расширение поля K , где α — корень многочлена $\alpha^2 - f = 0$, где $f \in k[x]$. Нормирование v имеет два продолжения на L , тогда и только тогда, когда $\sqrt{f} \in K_v$. В противном случае нормирование v имеет единственное продолжения на L .

Доказательство. По предложению 9 число вложений L в $\overline{K_v}$ совпадает числом корней неприводимого многочлена элемента α , которое равно равно 2. Вложение определяется образом элемента α . Рассмотрим два различных вложения $\sigma, \tau : L \rightarrow \overline{K_v}$, такие что $\sigma(\alpha) = \sqrt{f}$ и $\tau(\alpha) = -\sqrt{f}$ для некоторого фиксированного элемента $\sqrt{f} \in \overline{K_v}$.

Они сопряжены над K_v , если $\sqrt{f} \notin K_v$. Действительно, рассмотрим башню полей $K_v \subset K_v(\sqrt{f}) \subset \overline{K_v}$, автоморфизм λ поля $K_v(\sqrt{f})$ над K_v , переводящий $\sqrt{f}$ в $-\sqrt{f}$, продолжается до автоморфизма $\overline{K_v}$. В противном случае, расширение $K_v(\sqrt{f})$ тривиально и совпадает с K_v , и очевидно, что σ, τ не сопряжены. Остаётся применить предложение 8. $\square$

Обозначим через $\mathcal{O}_v = \{z \in K \mid v(z) \geq 0\}$ кольцо нормирования $v = v_h$ для некоторого неприводимого многочлена h , через $\mathfrak{p}_v = \{z \in K \mid v(z) > 0\}$ — идеал нормирования v . Тогда поле вычетов $\mathcal{O}_v/\mathfrak{p}_v$ совпадает с $k[x]/(h)$ и оно изоморфно конечному расширению k .

Выберем в $k[x]$ фиксированную систему Σ представителей смежных классов по идеалу (h) , состоящую из всех многочленов степени меньшей, чем $\deg h$. Тогда каждый элемент $z \in K_v$ единственным образом можно представить в виде

формального степенного ряда (см. например, [28, гл. XII, §6]))

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

где $a_i \in \Sigma$. В случае $\deg h = 1$ пополнение поля $K = k(x)$ по нормированию ν_h можно отождествить с полем формальных степенных рядов $K_\nu = k((h))$.

Предложение 11. Пусть f — свободный от квадратов многочлен в $k[x]$, и пусть $\bar{x}$ — образ x в поле вычетов $\mathcal{O}_\nu/\mathfrak{p}_\nu$. Нормирование ν_h имеет два продолжения на $L = K(\alpha)$, где α — корень многочлена $\alpha^2 - f = 0$, тогда и только тогда, когда $f(\bar{x}) = \beta^2$ для некоторого $0 \neq \beta \in \mathcal{O}_\nu/\mathfrak{p}_\nu$.

Замечание 1. Если $\deg h = 1$, то условие выше можно переписать как $h \nmid f$ и $f \bmod h = c^2$ для некоторой константы $c \in k$.

Аналогичным образом можно показать, что верно следующее предложение для бесконечного нормирования.

Предложение 12. Бесконечное нормирование ν_∞ имеет два продолжения на L тогда и только тогда, когда степень многочлена f — чётное число, и старший коэффициент многочлена f — полный квадрат в k . Если бесконечное нормирование обладает единственным продолжением на поле L , мы будем также обозначать его ν_∞ .

В работе [13] был доказан ряд результатов, связанных с продолжениями конечных нормирований на квадратичное расширения $L = k(x)(\sqrt{f})$. Несмотря на то, что результаты были сформулированы для случая конечного поля $k = \mathbb{F}_q$ и многочлена f нечетной степени $\deg f = 2g + 1$, их доказательство и сами результаты остаются верными и в более общем случае. Приведем формулировку нужного нам результата в необходимой нам общности.

Предложение 13. Пусть $\alpha = p + q\sqrt{f}$, где $p, q \in k[x]$, $p \neq 0$, $q \neq 0$, $\text{НОД}(p, q) = 1$, и пусть $h \in k[x]$ — неприводимый многочлен. Тогда если ν_h имеет два продолжения: ν_h^+ и ν_h^- на поле L , то либо $\nu_h^+(\alpha) = 0$, либо $\nu_h^-(\alpha) = 0$.

1.1.2 Непрерывные дроби

Случай непрерывных дробей функциональных полей для нормирования ν_∞ рассматривался в [21; 29]. Мы рассматриваем случай произвольного нормирования ν_h поля $k(x)$, где $h \in k[x]$ — многочлен первой степени. Пусть $\alpha \in k((h))$. Представим α в виде формального степенного ряда

$$\alpha = \sum_{j=e}^{\infty} b_j h^j, \quad \alpha \in k((h)), b_j \in k.$$

Обозначим через $[\alpha]$ — сумму членов с неположительными, а через $\{\alpha\}$ — с положительными показателями степени h разложения α в ряд Лорана:

$$[\alpha] = \begin{cases} \sum_{i=e}^0 b_i h^i & \text{если } e \leq 0, \\ 0 & \text{иначе;} \end{cases}$$

$$\{\alpha\} = \alpha - [\alpha] = \sum_{i=1}^{\infty} b_i h^i.$$

Положим $A_0 = [\alpha]$. Если $\alpha - A_0 \neq 0$, то положим

$$\alpha_1 = \frac{1}{\alpha - A_0} \in k((h)), \quad A_1 = [\alpha_1].$$

Далее по индукции определяем элементы A_i, α_i : если $\alpha_{i-1} - A_{i-1} \neq 0$, то

$$\alpha_i = \frac{1}{\alpha_{i-1} - A_{i-1}} \in k((h)), \quad A_i = [\alpha_i].$$

В результате мы получим *непрерывную дробь*

$$A_0 + \frac{1}{A_1 + \frac{1}{A_2 + \frac{1}{A_3 + \dots}}}. \quad (1.1)$$

Будем использовать стандартную сокращенную запись $[A_0, A_1, A_2, \dots]$ для непрерывной дроби (1.1). По построению, $\alpha_n = [A_n, A_{n+1}, \dots]$.

Конечные ряды без положительных степеней h вида $d_n h^{-n} + d_{n-1} h^{-(n-1)} + \dots + d_0 \in k(x)$ удобно рассматривать как многочлены от h^{-1} . Кольцо таких многочленов будем обозначать $k[h^{-1}]$. Этот объект в теории функциональных непрерывных дробей для $k((h))$ играет роль кольца $\mathbb{Z}$ из классического случая числовых непрерывных дробей. Соответственно, роль $\mathbb{Q}$ играет его поле частных $k(x)$.

Определим по индукции элементы $P_n, Q_n \in k[h^{-1}]$. Положим

$$P_{-2} = 0, P_{-1} = 1, Q_{-2} = 1, Q_{-1} = 0$$

и если $n \geq 0$, то

$$P_n = A_n P_{n-1} + P_{n-2}, \quad Q_n = A_n Q_{n-1} + Q_{n-2}. \quad (1.2)$$

Тогда $P_n/Q_n = [A_0, A_1, A_2, \dots, A_n]$ при $n \geq 0$. Стандартным образом можно показать, что для $n \geq -1$ справедливы соотношения

$$Q_n P_{n-1} - P_n Q_{n-1} = (-1)^n, \quad (1.3)$$

$$Q_n \alpha - P_n = \frac{(-1)^n}{Q_n \alpha_{n+1} + Q_{n-1}}, \quad (1.4)$$

$$\alpha = \frac{P_n \alpha_{n+1} + P_{n-1}}{Q_n \alpha_{n+1} + Q_{n-1}}. \quad (1.5)$$

Дробь P_n/Q_n назовем n -й *подходящей дробью* к α . По построению, $v_h(A_n) = v_h(\alpha_n) < 0$ для $n \geq 1$.

По индукции нетрудно показать, что выполнено:

$$\begin{aligned} v_h(P_n) &= v_h(A_n) + v_h(P_{n-1}) = \\ &= \sum_{j=0}^n v_h(A_j), \\ v_h(Q_n) &= v_h(A_n) + v_h(Q_{n-1}) = \\ &= \sum_{j=1}^n v_h(A_j). \end{aligned} \quad (1.6)$$

и, следовательно, верно:

$$v_h(Q_n \alpha - P_n) > -v_h(Q_n), \quad (1.7)$$

Откуда с помощью (1.4) можно получить $\lim_{n \rightarrow \infty} P_n/Q_n = \alpha$. Таким образом, подходящие дроби сходятся к α (подробности см. [13, §5.1]).

По аналогии с числовым случаем справедливо утверждение, что непрерывная дробь вида (1.1) произвольного элемента $\alpha \in k((h))$ конечна тогда и только тогда, когда $\alpha \in k(x)$ (см. [13, Предложение 5.1]). Элемент $k(x)$ единственным образом представляется в виде непрерывной дроби

$$\alpha = [A_0, \dots, A_n] = P_n/Q_n,$$

где $\nu_h(A_i) < 0$ и $A_i \in k[h^{-1}]$.

1.1.3 Наилучшие приближения

Элемент $k(x)$ удобно рассматривать как несократимую дробь P/Q , $P, Q \in k[h^{-1}]$, т.е. как дробь от многочленов от h^{-1} . Если $a/b \in k(x)$, где $a, b \in k[x]$ — взаимно простые многочлены, то разложим a и b по степеням h :

$$a = a_0 + a_1h + \dots + a_eh^e, \quad b = b_0 + b_1h + \dots + b_th^t,$$

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

$$\frac{a}{b} = \frac{p_{-k}h^{-k} + \dots + p_0}{q_{-l}h^{-l} + \dots + q_0} = \frac{P}{Q}, \quad (1.8)$$

где $p_i, q_i \in \Sigma$, $p_{-k} \neq 0$, $q_{-l} \neq 0$, $r \geq \max\{k, l\}$, p_0 и q_0 одновременно не равны нулю. Будем в дальнейшем предполагать, что все элементы из $k(x)$ записаны в виде (1.8).

Определение 6. Несократимая дробь $P/Q \in k(x)$ является наилучшим приближением к элементу $\psi \in k(x)_{\nu_h}$ из пополнения поля $k(x)$, если для любой другой несократимой дроби $A/B \neq P/Q$, такой, что $\nu_h(B) \geq \nu_h(Q)$, справедливо неравенство

$$\nu_h(\psi - \frac{P}{Q}) > \nu_h(\psi - \frac{A}{B}).$$

Приведем здесь без доказательства некоторые важные для изложения результаты из [13], относящиеся к понятию наилучшего приближения.

Теорема 11 ([13]). Дробь P/Q является наилучшим приближением к ψ тогда и только тогда, когда $\nu_h(\psi - P/Q) > -2\nu_h(Q)$.

Предложение 14 ([13]). Если дроби A/B и C/D — такие наилучшие приближения к ψ , что $v_h(B) = v_h(D)$, то найдется константа $\gamma \in k^*$ такая, что $A = \gamma C$, $B = \gamma D$.

Теорема 12 ([13]). Справедливы следующие утверждения:

1. n -я подходящая дробь P_n/Q_n к ψ является наилучшим приближением к ψ ;
2. Если дробь A/B является наилучшим приближением к ψ , то найдется такая подходящая дробь P_n/Q_n к ψ и такая константа $c \in k^*$, что $A = cP_n$, $B = cQ_n$.

Естественным следствием из утверждений выше является следующее предложение.

Предложение 15. Пусть $\deg h = 1$. Дробь P/Q , где $P, Q \in k[h^{-1}]$, $\text{НОД}(P, Q) = 1$, равна некоторой подходящей дроби P_n/Q_n к элементу $\alpha \in k((h))$ тогда и только тогда, когда $v_h(Q\alpha - P) > -v_h(Q)$. При этом $P = cP_n$, $Q = cQ_n$ для некоторой константы $c \in k \setminus \{0\}$.

1.2 Квазипериодические непрерывные дроби и S -единицы

1.2.1 Квазипериодические и периодические непрерывные дроби

Важным классом непрерывных дробей являются квазипериодические непрерывные дроби. В параграфе §1.2.4 мы увидим, что они являются определяющими с точки зрения существования S и S_h -единиц.

Определение 7. Разложение в непрерывную дробь элемента α называется квазипериодическим, если существуют такие $i, j \in \mathbb{Z}$, $i > j \geq 0$ и $c \in k \setminus \{0\}$, что $\alpha_i = c\alpha_j$, где α_k — полное частное с номером k к $\alpha = \alpha_0$. Наименьшее такое $i - j$ называется длиной квазипериода. В дальнейшем мы будем называть элемент (квази)периодическим, если его разложение (квази)периодично. Коэффициент c для наименьшего j среди пар i, j с наименьшим значением $i - j$ называется коэффициентом квазипериодичности элемента α .

Мы будем использовать обозначение $\alpha = [A_0, \dots, A_{n-1}, \overline{B_1, \dots, B_t}^b]$ для элементов, которые разлагается в непрерывную дробь вида

$$\alpha = [A_0, \dots, A_{n-1}, B_1, B_2, \dots, B_t, bB_1, b^{-1}B_2, \dots, b^{-1}B_t, b^2B_1, b^{-2}B_2, \dots, b^{-2}B_t, b^3B_1, \dots],$$

а если $b = 1$, то будем писать, что $\alpha = [A_0, \dots, A_{n-1}, \overline{B_1, \dots, B_t}]$.

Предложение 16. Элемент α является квазипериодическим тогда и только тогда, когда

$$\alpha = [A_0, \dots, A_{n-1}, \overline{B_1, \dots, B_{2t}}^b], \quad (1.9)$$

где $b \in k \setminus \{0\}$, а n и t — некоторые натуральные числа.

Доказательство. Пусть выполнено (1.9). Тогда из соотношения

$$b[B_1, B_2, \dots] = [bB_1, b^{-1}B_2, \dots]$$

следует, что $b\alpha_n = \alpha_{n+2t}$.

Обратно, пусть элемент α квазипериодический, т.е. найдутся такие $i, j \in \mathbb{N}$, $i > j$ и $c \in k \setminus \{0\}$, что $c\alpha_i = \alpha_j$. Без ограничения общности можно считать, что $j = 0$. Тогда

$$\alpha_j = \alpha = [A_0, \dots, A_{i-1}, \alpha_i] = c\alpha_i,$$

или

$$[A_0, \dots, A_{i-1}, A_i, \dots] = c[A_i, A_{i+1}, \dots] = [cA_i, c^{-1}A_{i+1}, cA_{i+1}, \dots].$$

Откуда $A_0 = cA_i$, $A_1 = c^{-1}A_{i+1}$, $\dots$, $A_i = c^{(-1)^i}A_{2i}$, что влечет $A_0 = cA_i = cc^{(-1)^i}A_{2i}$, $A_1 = \dots$. В зависимости от четности i два случая.

Пусть $i = 2l + 1$, тогда $A_r = A_{2i+r}$, разложение α оказывается периодическим и имеет вид (1.9) с $t = i$, $b = 1$.

Пусть теперь $i = 2l$, тогда $A_r = c^{(-1)^i}A_{r+i} = c^{(-1)^{i2}}A_{2i+r} = \dots = c^{(-1)^{in}}A_{ni+r}$, для $r = 0, \dots, i$, $n \geq 0$. В этом случае разложение α имеет вид (1.9) с $t = l$ и $b = c^{-1}$.

□

Впоследствии мы неявно будем пользоваться следующим утверждением, касающимся квазипериодичности произвольного элемента.

Предложение 17. Пусть разложение элемента $\alpha \in k((h))$ в непрерывную дробь квазипериодично. И пусть $i \geq 0$ такое минимальное целое число, что $\alpha_{N+i} = c\alpha_i$, где N — длина квазипериода, а $c \in k \setminus \{0\}$. Тогда для любых неотрицательных M, j и $c_1 \in k \setminus \{0\}$ таких, что $\alpha_{j+M} = c_1\alpha_j$, выполнено $j \geq i$, $c_1 = c^m$, $M = nN$, где $m, n \in \mathbb{Z}$. Более того, для любого натурального n существует $c_1 \in k \setminus \{0\}$ такое, что $\alpha_{i+nN} = c_1\alpha_i$.

Доказательство. Пусть $j = i$. Тогда без ограничения общности можно считать, что $i = 0$. Перепишем условие предложения:

$$\alpha_M = c_1\alpha, \alpha_N = c\alpha.$$

Получаем $\alpha_M = \frac{c_1}{c}\alpha_N$. С помощью алгоритма Евклида можно получить соотношение $\alpha_{N_1} = c_2\alpha_{N_2}$, где $N_1 - N_2 = \text{НОД}(M, N)$. Если N не делит M , то получаем противоречие с тем, что N — квазипериод. Таким образом $M = nN$. Откуда

$$c_1\alpha = \alpha_M = c^m\alpha,$$

$$\text{где } m = 1 + (-1)^N + (-1)^{2N} + \dots + (-1)^{(n-1)N}.$$

Пусть теперь $j > i$. Тогда мы в качестве α без ограничения общности можем взять α_j , т.к. для этого элемента выполнено соотношение $\alpha_{j+N} = c^{(-1)^{j-i}}\alpha_j$, и применить предыдущее рассуждение. Аналогично в случае $j < i$. В качестве α достаточно рассмотреть α_i , для которого выполнено $c^{(-1)^{i-j}}\alpha_i = \alpha_{i+M}$.

Докажем теперь, что, если для некоторого M и минимального j выполнено $c_1\alpha_j = \alpha_{j+M}$, то $i = j$. Очевидно, что $j \leq i$. Пусть строго меньше. Тогда без ограничения общности положив $j = 0$ имеем

$$c_1\alpha = \alpha_M,$$

$$c_1^{(-1)^N}\alpha_N = \alpha_{N+M}.$$

Несложно показать, что условие $i \geq M$ противоречит минимальности i , поэтому будем считать, что $i < M$. В этом случае $\alpha_{N+M} = c_3\alpha_M$. Откуда $c_4\alpha = \alpha_N$, что снова противоречит минимальности i . $\square$

1.2.2 Квадратичная иррациональность

В параграфе §1.2.3 будет показано, что всякая квазипериодическая непрерывная дробь является квадратичной иррациональностью, т.е. корнем некоторого квадратного уравнения с коэффициентами из $k[x]$. За более подробным изложением фактов, связанных с квадратичной иррациональностью, мы отсылаем читателя к [13], здесь же приведём лишь необходимые нам понятия и соотношения.

Пусть $\alpha \in k((h))$ является корнем квадратного многочлена, т.е. удовлетворяет соотношению

$$\lambda_2 \alpha^2 + \lambda_1 \alpha + \lambda_0 = 0, \quad \text{где } \lambda_0, \lambda_1, \lambda_2 \in k[x]. \quad (1.10)$$

Тогда элемент α называется *квадратичной иррациональностью*. Положим

$$H(X, Y) = \lambda_2 X^2 + \lambda_1 XY + \lambda_0 Y^2.$$

Тогда из (1.5) можно получить

$$\alpha_{n+1} = \frac{M_n + \lambda_2 \alpha}{L_n}, \quad (1.11)$$

где $M_n, L_n \in k[x]$, и выполнено:

$$L_n = (-1)^{n+1} H(P_n, Q_n) = (-1)^{n+1} (\lambda_2 P_n^2 + \lambda_1 P_n Q_n + \lambda_0 Q_n^2), \quad (1.12)$$

$$M_n = (-1)^n (\lambda_2 P_{n-1} P_n + \lambda_1 P_{n-1} Q_n + \lambda_2 Q_{n-1} Q_n). \quad (1.13)$$

Справедливо также следующее соотношение:

$$\nu_h(L_n) = \frac{1}{2} \nu_h(\lambda_1^2 - 4\lambda_0 \lambda_2) - \nu_h(A_{n+1}). \quad (1.14)$$

Из (1.11) находим $M_n = L_n \alpha_{n+1} - \lambda_2 \alpha$. Из равенства $\alpha(\lambda_2 \alpha + \lambda_1) = -\lambda_0$ следует, что $\nu_h(\lambda_2 \alpha) \geq 0$. Учитывая (1.14) и то, что $\nu_h(\alpha_{n+1}) = \nu_h(A_{n+1})$, находим

$$\nu_h(L_n \alpha_{n+1}) = \nu_h(L_n A_{n+1}) = \frac{1}{2} \nu_h(\lambda_1^2 - 4\lambda_0 \lambda_2) \geq 0.$$

Значит,

$$\nu_h(M_n) \geq \min\{\nu_h(L_n \alpha_{n+1}), \nu_h(\lambda_2 \alpha)\} \geq 0.$$

Таким образом, L_n, M_n являются многочленами из $k[x]$ и, с учётом определения L_n и M_n можно утверждать, что их степени ограничены степенями λ_i :

$$\begin{aligned}\deg M_n &\leq \max\{\deg \lambda_1, \deg \lambda_2, \deg \lambda_3\}, \\ \deg L_n &\leq \max\{\deg \lambda_1, \deg \lambda_2, \deg \lambda_3\}.\end{aligned}\tag{1.15}$$

Многочлены M_n и L_n связывает ряд рекуррентных соотношений, которые доказываются стандартным образом.

Предложение 18.

$$M_n + M_{n-1} - \lambda_1 = A_n L_{n-1}, \tag{1.16}$$

$$(\lambda_1/2)^2 - \lambda_0 \lambda_2 - (M_n - \lambda_1/2)^2 = L_n L_{n-1}, \tag{1.17}$$

$$L_{n-2} + A_n(M_{n-1} - M_n) = L_n. \tag{1.18}$$

Доказательство. В стандартное соотношение определяющее процесс построения непрерывной дроби $\alpha_{n+1} = \frac{1}{\alpha_n - A_n}$ подставим выражение (1.11) для n и $n+1$. Получим:

$$\frac{M_n + \lambda_2 \alpha}{L_n} = 1 / \left(\frac{M_{n-1} + \lambda_2 \alpha}{L_{n-1}} - A_{n-1} \right).$$

Или

$$L_n L_{n-1} = (M_{n-1} + \lambda_2 \alpha - A_{n-1} L_{n-1})(M_n + \lambda_2 \alpha).$$

После раскрытия скобок получаем:

$$M_{n-1} M_n - A_{n-1} L_{n-1} M_n - L_n L_{n-1} + \lambda_2 \alpha (M_n - A_{n-1} L_{n-1} + M_{n-1}) + \lambda_2^2 \alpha^2 = 0.$$

Но $\lambda_2 \alpha^2 = -(\lambda_1 \alpha + \lambda_0)$. Получаем:

$$M_{n-1} M_n - A_{n-1} L_{n-1} M_n - L_n L_{n-1} - \lambda_0 \lambda_2 + \lambda_2 \alpha (M_n - A_{n-1} L_{n-1} + M_{n-1} - \lambda_1) = 0.$$

В силу того, что коэффициент при α должен быть равен 0, получаем (1.16). Откуда

$$(M_{n-1} - A_{n-1} L_{n-1}) M_n - L_n L_{n-1} - \lambda_0 \lambda_2 = 0.$$

Подставим (1.16) и получим:

$$(\lambda_1 - M_n)M_n - L_n L_{n-1} - \lambda_0 \lambda_2 = 0.$$

Откуда получается равенство (1.17).

Наконец, запишем равенство (1.17) для номеров n и $n-1$, после чего вычтем их друг из друга:

$$(M_{n-1} - M_n)(M_n + M_{n-1} - \lambda_1)/L_{n-1} = L_n - L_{n-2}.$$

Воспользуемся (1.16) и, заменив последнее отношение на A_n , получаем (1.18). $\square$

1.2.3 Критерии квазипериодичности и периодичности

Выше мы отмечали важность квазипериодических и периодических элементов $k((h))$. По аналогии со случаем числовых непрерывных дробей, такие элементы обязательно являются квадратичными иррациональностями, однако обратное верно не всегда. Критерием является аналог теоремы Лагранжа для $k((h))$, его доказательство схоже с доказательством аналога теоремы Лагранжа для $k((1/x))$ из работы [20].

Теорема 13 ([20]). Пусть $\alpha \in k((h)) \setminus k(x)$, $\text{char } k \neq 2$.

Если α квазипериодичен, то α является квадратичной иррациональностью. Обратно, пусть α удовлетворяет уравнению

$$\Lambda_1 \alpha^2 + \Lambda_1 \alpha + \Lambda_0 = 0, \Lambda_2, \Lambda_1, \Lambda_0 \in k[h^{-1}], \text{НОД}(\Lambda_2, \Lambda_1, \Lambda_0) \in k. \quad (1.19)$$

Обозначим $D = \Lambda_1^2 - 4\Lambda_2\Lambda_0$. Тогда α разлагается в квазипериодическую непрерывную дробь в том и только том случае, когда соотношение:

$$Y^2 - DZ^2 = b \in k \setminus \{0\} \quad (1.20)$$

обладает нетривиальным решением относительно неизвестных $Y, Z \in k[h^{-1}]$ и некоторой неизвестной константы b , т.е. решением с $Z \neq 0$.

Замечание 2. Уравнение (1.20) имеет решение тогда и только тогда, когда имеет решение уравнение $Y^2 - DZ^2 = 1$. Действительно, рассмотрим $Y' = (Y^2 + DZ^2)/b$ и $Z' = 2YZ/b$, тогда $Y'^2 - DZ'^2 = 1$.

Следует отметить аналогию с уравнением Пелля для классического числового случая и его связь с непрерывными дробями.

Следствие 8. Если элемент α — квазипериодичен, то элемент $1/\alpha$ квазипериодичен.

Доказательство. Легко видеть, что из (1.19) следует, что квадратичная иррациональность $1/\alpha$ задаётся уравнением $A + B(1/\alpha) + C(1/\alpha)^2 = 0$. Очевидно, дискриминант этого уравнения совпадает с дискриминантом уравнения (1.19). $\square$

Теорема 13 показывает, что всякая квазипериодическая непрерывная дробь является квадратичной иррациональностью, а, следовательно, она лежит в некотором квадратичном расширении $L = k(x)(\sqrt{f})$ поля $k(x)$ для бесквадратного многочлена f . Теорема 13 позволяет выделить ключевой с точки зрения периодичности элемент.

Следствие 9. Пусть f — бесквадратный многочлен, $g = \lfloor \frac{\deg f - 1}{2} \rfloor$, и пусть разложение в непрерывную дробь некоторой квадратичной иррациональности $\alpha = \frac{v+w\sqrt{f}}{u}$ квазипериодично, где $v, w, u \in k[x]$ и $\text{НОД}(v, w, u) \in k$. Тогда квазипериодична любая квадратичная иррациональность с дискриминантом $D = \frac{f}{h^{2g+2}} \in k[h^{-1}]$. В частности, квазипериодичен элемент $\frac{\sqrt{f}}{h^{g+1}}$.

Обратно, пусть элемент $\frac{\sqrt{f}}{h^{g+1}}$ квазипериодический. Тогда квадратичная иррациональность $\alpha = \frac{v+w\sqrt{f}}{u}$ обладает квазипериодическим разложением только, если уравнение (1.20) для $D = \frac{f}{h^{2g+2}} \in k[h^{-1}]$ имеет решение $Y, Z \in k[h^{-1}]$ такое, что $Z = Z'H$, где $H = h^{g+1-l}wu/r$, $Z' \in k[h^{-1}]$, $r = \text{НОД}(u, v^2 - w^2f)$ и $l = \max\{2 \deg u, \deg u + \deg v, \deg(v^2 - w^2f)\} - \deg r$.

Доказательство. Элемент α удовлетворяет уравнению с коэффициентами в $k[x]$:

$$(u^2/r)x^2 - 2(uv/r)x + (v^2 - w^2f)/r = 0, \quad (1.21)$$

где $r = \text{НОД}(u^2, uv, v^2 - w^2f) = \text{НОД}(u, v^2 - w^2f)$. Пусть $l = \max\{2 \deg u, \deg u + \deg v, \deg(v^2 - w^2f)\} - \deg r$. Ясно, что если поделить

уравнение (1.21) на h^l , то мы получим минимальное уравнение квадратичной иррациональности α с коэффициентами в кольце $k[h^{-1}]$ с дискриминантом $D = 4h^{-2l}w^2(u/r)^2f = 4(h^{-l+g+1}wu/r)^2\frac{f}{h^{2g+2}} \in k[h^{-1}]$.

Перепишем уравнение (1.20) для α : $Y^2 - Z^2H^2\frac{f}{h^{2g+2}} = b$. Решение уравнения (1.20) с $D = H^2\frac{f}{h^{2g+2}}$ существует только при условии существования решения уравнения (1.20) с $D = \frac{f}{h^{2g+2}}$.

Обратно, пусть элемент $\frac{\sqrt{f}}{h^{g+1}}$ квазипериодический. Из рассуждений выше заключаем, что условие следствия является необходимым и достаточным. $\square$

Следствие 9 утверждает, что ключевым элементом поля L с точки зрения наличия квазипериодических элементов является элемент $\sqrt{f}/h^{g+1}$. Изучение свойств этого элемента представляет особый интерес, и мы сосредоточимся на нем в §2.4. В дальнейшем мы также увидим, что периодичность элементов вида $\frac{\sqrt{f}}{dh^s}$, где $s \in \mathbb{Z}$, а d — делитель f , имеет тесные связи с периодичностью элемента $\sqrt{f}/h^{g+1}$.

В работе [27] утверждалось, что в случае $\deg f = 2g + 1$ периодичность элементов вида $\frac{\sqrt{f}}{h^s}$, где $s = g, g + 1$, равносильна наличию нетривиальной S -единицы поля $L = k(x)(\sqrt{f})$. Позднее мы увидим, что наличие периодических элементов в L и периодичность $\sqrt{f}/h^{g+1}$ и $\sqrt{f}/h^g$ в этом случае равносильны наличию нетривиальной S -единицы в L . Но уже сейчас в качестве следствия из теоремы 13 может быть получено утверждение о том, что квазипериодичность одного из указанных элементов равносильна квазипериодичности другого. В дальнейшем мы также покажем, что такие элементы квазипериодичны в том и только том случае, когда они периодичны.

Следствие 10. Пусть $f = dd'$, где $d, d' \in k[x]$, $\deg d = t$, $\deg f = w$, $s \in \mathbb{Z}$. Обозначим элемент $\alpha_{d,s} = \frac{\sqrt{f}}{dh^s}$. Следующие утверждения равносильны:

1. Элемент $\alpha_{1,t+s} = \frac{\sqrt{f}}{h^{t+s}}$ квазипериодический,
2. Элемент $\alpha_{1,w-(t+s)} = \frac{\sqrt{f}}{h^{w-(t+s)}}$ квазипериодический,
3. Элемент $\alpha_{d,s} = \frac{\sqrt{f}}{dh^s}$ квазипериодический,
4. Элемент $\alpha_{d',-s} = \frac{h^s\sqrt{f}}{d'}$ квазипериодический,
5. Элемент $\alpha_{d',2t+s-w} = \frac{\sqrt{f}}{d'h^{2t+s-w}}$ квазипериодический.

Доказательство. Элемент $\alpha_{d,s}$ удовлетворяет уравнению $dh^{2s}\alpha_{d,s}^2 - \frac{f}{d} = 0$. Пусть $l = \max\{t + 2s, w - t\}$, тогда $\alpha_{d,s}$ удовлетворяет следующему уравнению с коэффициентами из $k[h^{-1}]$:

$$dh^{2s-l}\alpha_{d,s}^2 - \frac{f}{d}h^{-l} = 0.$$

Дискриминант этого уравнения равен $D = 4fh^{-2(l-s)}$. Величина $l - s = \max\{t + s, w - (t + s)\}$. Дискриминант этого уравнения совпадает с дискриминантом уравнения для элемента $\frac{\sqrt{f}}{h^{t+s}}$, а также элемента $\frac{\sqrt{f}}{h^{w-(t+s)}}$. Откуда с помощью теоремы 13 сразу следует эквивалентность 1, 2 и 3.

Рассмотрим элемент $\alpha_{d',s'}$, где степень делителя d' равна $\deg d' = t' = w - t$. Соответствующий дискриминант равен $D' = 4fh^{-2(l'-s')}$, где $l' - s' = \max\{t' + s', w - t' - s'\} = \max\{w - (t - s'), t - s'\}$.

Ясно, что если $s' = -s$, то $D' = D$, откуда вытекает эквивалентность 3 и 4.

Равносильность 4 и 5 вытекает из достаточного условия $t + s = t' + s'$ на $D = D'$, которое выполняется при $s' = 2t + s - w$. $\square$

Замечание 3. Следствие 10 показывает, что элемент $\frac{\sqrt{f}}{h^s}$ квазипериодический тогда и только тогда, когда квазипериодичен $\frac{\sqrt{f}}{h^{w-s}}$. Откуда при $\deg f = 2g + 1$ следует равносильность квазипериодичности элементов $\frac{\sqrt{f}}{h^g}, \frac{\sqrt{f}}{h^{g+1}}$.

В работе [20] приведен критерий того, что квазипериодический элемент из $k((1/x))$ обладает периодическим разложением в непрерывную дробь определенного вида. Похожий результат для случая $k((h))$ доказывается аналогично. Для квадратичной иррациональности $\alpha = \frac{v+w\sqrt{f}}{u}$ через $\alpha' = \frac{v-w\sqrt{f}}{u}$ будем обозначать элемент сопряженный с ней.

Теорема 14 ([20]). Следующие условия на квазипериодический элемент $\alpha \in k((h))$ эквивалентны.

1. $v_h(\alpha) < 0, v_h(\alpha') \leq 0, v_h(\alpha - \alpha') < 0$ и $\alpha + \alpha' \in k[h^{-1}]$.
2. α разлагается в периодическую непрерывную дробь вида

$$[C_0, \overline{C_1, \dots, C_w},] \quad (1.22)$$

с $C_i \in k[h^{-1}], C_0 \neq C_w, v_h(C_0) < 0$ и $C_i = C_{w-i}$, для $i = 1, \dots, w-1$.

При выполнении условий выше $\alpha + \alpha' = 2C_0 - C_w$.

Следствие 11 ([20]). Пусть $\text{char } k \neq 2$. Следующие условия на квазипериодический элемент $\alpha \in k((h))$ эквивалентны.

- $\alpha = \sqrt{E}$, где $E \in k(x), v_h(E) < 0$ и E не является полным квадратом в $k(x)$.

– α разлагается в периодическую непрерывную дробь вида $[\frac{1}{2}C_w, \overline{C_1, \dots, C_w}]$ и $C_i = C_{w-i}$, для $i = 1, \dots, w-1$.

Следствие 12. Элемент вида $\alpha_{d,s} = \frac{\sqrt{f}}{dh^s}$ для делителя d многочлена f и $s \neq 0 \in \mathbb{Z}$ квазипериодичен тогда и только тогда, когда он периодичен. Если его разложение периодично, то оно имеет вид $[\frac{1}{2}C_w, \overline{C_1, \dots, C_w}]$ при $s > 0$ и $[0, \frac{1}{2}C_w, \overline{C_1, \dots, C_w}]$ при $s < 0$. Причем $C_i = C_{w-i}$, для $i = 1, \dots, w-1$.

Доказательство. Легко видеть, что при $s > 0$ элемент $\frac{\sqrt{f}}{dh^s}$ удовлетворяет условию следствия 11 и, таким образом, верно требуемое утверждение.

Для $s < 0$. Достаточно рассмотреть первое полное частное α_1 к $\alpha = \alpha_{d,s}$ и применить к нему следствие 11. $\square$

Следствие 12 не позволяет дать полный ответ на вопрос о периодичности квазипериодических элементов вида $\frac{\sqrt{f}}{dh^s}$, т.к. случай $s = 0$ требует отдельного подхода и будет рассмотрен далее.

1.2.4 S и S_h -единицы

Пусть $h \in k[x]$ — неприводимый над k многочлен, и конечное нормирование v_h поля $k(x)$ ассоциированное с h имеет два продолжения: v_h^+ и v_h^- на поле $L = k(x)(\sqrt{f})$.

Тогда обозначим через $S_h = \{v_h^+, v_h^-\}$ множество нормирований, состоящее из этих двух продолжений на L нормирования v_h . В случае, когда бесконечное нормирование имеет ровно одно продолжение на поле L , обозначим через $S = \{v_h^+, v_\infty\}$ множество, состоящее из бесконечного и одного из двух продолжений конечного нормирования.

Обозначим через $\mathcal{O}_S$ (соответственно, $\mathcal{O}_{S_h}$) кольцо S -целых элементов (соответственно, S_h -целых элементов) в L , т.е. таких элементов $z \in L$, что $v(z) \geq 0$ для всех нормирований v поля L , не принадлежащих множеству S (соответственно множеству S_h).

Определение 8. S -единицей называется обратимый элемент кольца $\mathcal{O}_S$ (соответственно $\mathcal{O}_{S_h}$). S -единицы (соответственно S_h -единицы) образуют группу по умножению, обозначим её через $\mathcal{U}_S$ (соответственно $\mathcal{U}_{S_h}$).

Очевидно, если $u \in \mathcal{U}_S$ (соответственно $u \in \mathcal{U}_{S_h}$), то $v(u) = 0$ для $v \notin S$ (соответственно $v \notin S_h$).

В работе [13] для $\deg f = 2g + 1$ и конечного поля констант было показано, что S -единицы являются элементами определенного вида. Аналогичными рассуждениями можно доказать следующие утверждения.

Предложение 19. Пусть $o \in \mathcal{O}_S$ или $o \in \mathcal{O}_{S_h}$. Тогда $o = \frac{\mu_1 + \mu_2 \sqrt{f}}{h^m}$ для $m \geq 0, m \in \mathbb{Z}$, где $\mu_1, \mu_2 \in k[x]$.

Обозначим через N — норменное отображение из $L = k(x)(\sqrt{f})$ в $k(x)$, т.е. $N(p + q\sqrt{f}) = p^2 - q^2 f$, где $p, q \in k(x)$.

Предложение 20. Пусть u — S -единица. Тогда $N(u) = \frac{\mu_1^2 - \mu_2^2 f}{h^{2m}} = bh^{m'} \in k \setminus \{0\}$, где $m, m' \in \mathbb{Z}$.

Пусть u — S_h -единица. Тогда $N(u) = \frac{\mu_1^2 - \mu_2^2 f}{h^{2m}} = b \in k \setminus \{0\}$, где $m \in \mathbb{Z}$.

В силу предложения 13 и предложения 20 выполнено следующее предложение.

Предложение 21. Пусть пара $\mu_1, \mu_2 \in k[x]$ — решение в многочленах уравнения

$$\mu_1^2 - \mu_2^2 f = bh^m \quad (1.23)$$

для некоторых $b \in k \setminus \{0\}$ и $m \in \mathbb{N}$.

Тогда, если $m = 2m'$, то элемент вида $\frac{\mu_1 \pm \mu_2 \sqrt{f}}{h^{m'}}$ является S_h -единицей.

Если же v_∞ имеет одно продолжение на L , то или элемент $\mu_1 + \mu_2 \sqrt{f}$ или элемент $\mu_1 - \mu_2 \sqrt{f}$ является S -единицей.

Вид нормы нетривиальной S и S_h -единицы позволяет определить понятие степени S и S_h -единицы следующим образом (см. [16], [25]):

Определение 9. Степенью S -единицы $u = \mu_1 + \mu_2 \sqrt{f}$, $\mu_1, \mu_2 \in k(x)$, называется число $\deg u = m$, где m — показатель степени многочлена h в норменном уравнении

$$N(u) = \mu_1^2 - \mu_2^2 f = bh^m, b \in k \setminus \{0\}.$$

Определение 10. Степенью S_h -единицы $u = \frac{\mu_1 + \mu_2 \sqrt{f}}{h^m}$, $\mu_1, \mu_2 \in k[x]$, $\text{НОД}(\mu_1, \mu_2) \in k$, называется число $\deg u = m$, где m — показатель степени многочлена h в знаменателе u .

Предложения 19, 20 показывают, что определения выше корректны.

Замечание 4. Если $(\mu_1 + \mu_2\sqrt{f})/h^m$ — S_h -единица и $\deg f = 2g + 1$, то из предложения 20 следует, что $\mu_1, \mu_2 \in k[x]$, а $m \deg h = \deg \mu_1 > \deg \mu_2 + g$.

Предложение 22. Пусть f — бесквадратный многочлен произвольной степени, и пусть линейное нормирование v_h поля $k(x)$ имеет два продолжения на поле $L = k(x)(\sqrt{f})$: v_h^+ и v_h^- .

В этом случае u — S_h -единица, для $S_h = \{v_h^+, v_h^-\}$, тогда и только тогда, когда $u = \frac{\mu_1 + \mu_2\sqrt{f}}{h^m}$, где $\mu_1, \mu_2 \in k[x]$, $\mu_2 \neq 0$, $v_h(\mu_2) = 0$, а $\max\{\deg \mu_1, \deg \mu_2 + \frac{1}{2} \deg f\} = m \deg h$, где $m \in \mathbb{Z}$, и $N(u) = b \in k \setminus \{0\}$.

Доказательство. Пусть существует S_h -единица u степени m . В силу предложения 20 имеем $N(u) = b \in k \setminus \{0\}$. Отсюда, $\mu_1^2 - \mu_2^2 f = bh^{2m}$.

Рассмотрим два случая.

Пусть сперва v_∞ имеет ровно одно продолжение на L , и пусть существует S_h -единица u . Тогда случай $\deg \mu_1 = \deg \mu_2 + \frac{1}{2} \deg f > m \deg h$ невозможен. Действительно, существование единственного продолжения v_∞ в силу предложения 12 гарантирует нам, что или $\deg f = 2g + 1$ или $\deg f = 2g + 2$ и старший коэффициент $lc(f)$ не является полным квадратом в k , а, следовательно, мономы многочленов μ_1^2 и $\mu_2^2 f$ степеней выше $2m$ не могут сократиться.

Пусть теперь $\deg f = 2g + 2$ и v_∞ имеет два продолжения на L : v_∞^+ и v_∞^- . Покажем, что $\max\{\deg \mu_1, \deg \mu_2 + g + 1\} = m \deg h$.

Ясно, что $\max\{2 \deg \mu_1, 2 \deg \mu_2 + \deg f\} \geq 2m$. Необходимо показать, что и в этом случае старшие мономы не могут взаимно уничтожиться.

В силу свойств неархимедова нормирования заключаем, что

$$\begin{aligned} v_\infty^+(\mu_1) &\geq \min\{v_\infty^+(\mu_1 + \mu_2\sqrt{f}), v_\infty^+(\mu_1 - \mu_2\sqrt{f})\}, \\ v_\infty^+(\mu_2\sqrt{f}) &\geq \min\{v_\infty^+(\mu_1 + \mu_2\sqrt{f}), v_\infty^+(\mu_1 - \mu_2\sqrt{f})\}. \end{aligned}$$

С другой стороны

$$\begin{aligned} v_\infty^+(\mu_1 + \mu_2\sqrt{f}) &\geq \min\{v_\infty^+(\mu_1), v_\infty^+(\mu_2\sqrt{f})\}, \\ v_\infty^+(\mu_1 - \mu_2\sqrt{f}) &\geq \min\{v_\infty^+(\mu_1), v_\infty^+(\mu_2\sqrt{f})\}. \end{aligned}$$

Таким образом,

$$\min\{v_\infty^+(\mu_1), v_\infty^+(\mu_2\sqrt{f})\} = \min\{v_\infty^+(\mu_1 + \mu_2\sqrt{f}), v_\infty^+(\mu_1 - \mu_2\sqrt{f})\}. \quad (1.24)$$

В силу того, что u — S_h -единица, заключаем, что $v_\infty^+(\mu_1 + \mu_2\sqrt{f}) = m v_\infty^+(h) = m v_\infty^-(h) = v_\infty^-(\mu_1 + \mu_2\sqrt{f}) = v_\infty^+(\mu_1 - \mu_2\sqrt{f})$. Тогда $\min\{v_\infty^+(\mu_1 + \mu_2\sqrt{f}), v_\infty^+(\mu_1 - \mu_2\sqrt{f})\} = m v_\infty^+(h) = -\deg h m$, откуда из (1.24) заключаем

$$\min\{v_\infty^+(\mu_1), v_\infty^+(\mu_2\sqrt{f})\} = -m \deg h.$$

Следовательно, $\max\{2 \deg \mu_1, 2 \deg \mu_2 + \deg f\} = 2m \deg h$.

Обратно, пусть $u = \frac{\mu_1 + \mu_2\sqrt{f}}{h^m}$, где $\mu_1, \mu_2 \in k[x]$, $\mu_2 \neq 0$, $v_h(\mu_2) = 0$, а $\max\{\deg \mu_1, \deg \mu_2 + \frac{1}{2} \deg f\} = m \deg h$, где $m \in \mathbb{Z}$ и $N(u) = b$. Ясно, что для любого конечного нормирования $v \notin S_h$ выполнено $v(N(u)) = 0$, $v(h^m) = 0$, а $v(\mu_1 \pm \mu_2\sqrt{f}) \geq 0$. Следовательно, $v(u) = 0$. Пусть теперь $v = v_\infty$ — бесконечное нормирование. Тогда имеем

$$v_\infty(\mu_1 + \mu_2\sqrt{f}) \geq \min\{v(\mu_1), v(\mu_2\sqrt{f})\} = -m \deg h,$$

$$v_\infty(\mu_1 - \mu_2\sqrt{f}) \geq \min\{v(\mu_1), v(\mu_2\sqrt{f})\} = -m \deg h.$$

Откуда $v_\infty(\mu_1 + \mu_2\sqrt{f}) = v_\infty(\mu_1 - \mu_2\sqrt{f}) = -m \deg h$. Учитывая, что $v_\infty(h^m) = -m \deg h$, заключаем, что u — S_h -единица. $\square$

Замечание 5. В силу предложения 21 в случае, если бесконечное нормирование имеет одно продолжение на поле L , можно сопоставить каждой S -единице четной степени S_h -единицу. Действительно, пусть $u = \mu_1 + \mu_2\sqrt{f}$ — S -единица положительной $2m > 0$, тогда u/h^m — S_h -единица степени m . При этом $u^{-1} = \frac{\mu_1 - \mu_2\sqrt{f}}{h^m}$ является S -единицей степени $-2m$ и кроме того является S_h -единицей степени m .

Обратное соответствие не так однозначно. Пусть $u = \frac{\mu_1 + \mu_2\sqrt{f}}{h^m}$ — S_h -единица степени m . Тогда либо uh^m , либо $u^{-1}h^m$ — S -единица степени $2m$, а соответственно либо u^{-1} , либо u — S -единица степени $-2m$. При этом в силу предложения 13 элементы uh^m и $u^{-1}h^m$ не могут быть S -единицами одновременно.

S -единицы и S_h -единицы несмотря на сходство, обладают некоторыми различиями. Так, например, S -единица может быть, как положительной, так и отрицательной степени. В то время как степень S_h -единицы обязательно положительная.

Кроме того, если $u = \frac{\mu_1 + \mu_2\sqrt{f}}{h^m}$ — S_h -единица, то и $u' = \frac{\mu_1 - \mu_2\sqrt{f}}{h^m}$ — S_h -единица. В то время как не более чем один из этих двух элементов при фиксированных $m, \mu_1, \mu_2 \neq 0$ по предложению 13 может быть S -единицей.

Опишем групповую структуру групп $\mathcal{U}_{S_h}$ и $\mathcal{U}_S$. Нижеприведённые утверждения могут быть получены из общей теории, но в целях замкнутости изложения мы выведем их здесь в частном случае более элементарными методами.

Предложение 23. *Группа S_h -единиц поля L или тривиальна, т.е. изоморфна k^* , или является произведением k^* и бесконечной циклической группы, т.е. изоморфна $k^* \times \mathbb{Z}$.*

Доказательство. По предложению 19 S_h -единица имеет вид $u = \frac{\mu_1 + \mu_2 \sqrt{f}}{h^m}$ для $m \geq 0$, где $\mu_1, \mu_2 \in k[x]$.

Нормирование ν_h^+ задаёт групповой гомоморфизм на $\nu_h^+ : \mathcal{U}_{S_h} \rightarrow \mathbb{Z}$. Покажем, что ядро этого гомоморфизма изоморфно k^* . Действительно, пусть $\nu_h^+(\frac{p+q\sqrt{f}}{h^m}) = 0$, тогда по предложению 20 выполняется $\nu_h^+(\frac{p-q\sqrt{f}}{h^m}) = 0$ в силу того, что $\nu_h^+(\frac{p+q\sqrt{f}}{h^m}) + \nu_h^+(\frac{p-q\sqrt{f}}{h^m}) = 0$. Рассмотрим $\nu_h^+(p/h^m) = \nu_h^+(\frac{p+q\sqrt{f}}{h^m} + \frac{p-q\sqrt{f}}{h^m}) \geq \min\{\nu_h^+(\frac{p+q\sqrt{f}}{h^m}), \nu_h^+(\frac{p-q\sqrt{f}}{h^m})\}$. Таким образом, получаем $\nu_h^+(p/h^m) \geq 0$, а учитывая, что предложение 22 влечёт за собой $p/h^m \in k[h^{-1}]$ и, следовательно, $\nu_h^+(p/h^m) \leq 0$, получаем $p/h^m \in k^*$. Откуда, из предложения 20 получаем $q = 0$, что влечёт за собой $p \in k^*$ и $m = 0$.

В случае, если нетривиальных S_h -единиц не существует, очевидно, что образ $\mathcal{U}_{S_h}$ тривиален. В противном случае, поскольку подгруппа циклической группы циклическая, а бесконечная циклическая группа изоморфна $\mathbb{Z}$, по теореме о гомоморфизме получаем требуемое утверждение. $\square$

Предложение 24. *Пусть ν_∞ обладает единственным продолжением на поле L . Тогда группа S -единиц поля L или тривиальна, т.е. изоморфна k^* , или является произведением k^* и бесконечной циклической группы, т.е. изоморфна $k^* \times \mathbb{Z}$.*

Доказательство. Путём возведения S -единиц в квадрат можно изоморфно отобразить группу S -единиц в собственную подгруппу S -единиц чётной степени, а в силу замечания 5 подгруппу S -единиц чётной степени можно изоморфно отобразить на группу S_h -единиц. Остаётся применить предложение 23. $\square$

Определение 11. *Образующая бесконечной циклической группы из предложения 23 (соответственно предложения 24) называется фундаментальной S_h -единицей (соответственно фундаментальной S -единицей).*

Сформулируем аналог предложения 21 для фундаментальных S и S_h -единиц.

Предложение 25. Пусть $m = 2m'$ — минимальное такое чётное натуральное число, что существует пара $\mu_1, \mu_2 \in k[x]$ — решение в многочленах уравнения (1.23) для некоторого $b \in k^*$ и такого m . Тогда элемент вида $\frac{\mu_1 \pm \mu_2 \sqrt{f}}{h^{m'}}$ является фундаментальной S_h -единицей.

Если же v_∞ имеет одно продолжение на L и m — минимальное натуральное число, что существует пара $\mu_1, \mu_2 \in k[x]$ — решение в многочленах уравнения (1.23) для некоторого $b \in k \setminus \{0\}$ и такого m , то или элемент $\mu_1 + \mu_2 \sqrt{f}$ или элемент $\mu_1 - \mu_2 \sqrt{f}$ является фундаментальной S -единицей.

Пусть $\deg h = 1$. Тогда существует взаимно-однозначное соответствие между нетривиальными S_h -единицами, нетривиальными решениями уравнения (1.23) и нетривиальными решениями в многочленах от h^{-1} уравнения (1.20), определёнными с точностью до константы. Если дополнительно известно, что бесконечное нормирование обладает единственным продолжением, то S_h -единицы также соответствуют S -единицам положительной четной степени.

Предложение 26. Пусть $\deg h = 1$. Следующие три утверждения эквивалентны:

1. Выполнено соотношение (1.23) для некоторого целого m и подходящих $\mu_1, \mu_2 \neq 0 \in k[x]$, $b \in k \setminus \{0\}$, $v_h(\mu_2) = 0$, а $\max\{2 \deg \mu_1, 2 \deg \mu_2 + \deg f\} = m \in \mathbb{Z}$. Если m — чётное, то обозначим $m' = m/2$, и $m = m'$ в противном случае.
2. Существуют $Z \neq 0, Y \in k[h^{-1}]$ и $b \in k \setminus \{0\}$, $m' = -v_h(Y)$ такие, что

$$Y^2 - Z^2 \frac{f}{h^{2g+2}} = b. \quad (1.25)$$

3. Существует нетривиальная S_h -единица степени m' .

Если дополнительно известно, что бесконечное нормирование имеет одно продолжение на поле L , то условия выше равносильны следующему

4. Существует нетривиальная S -единица степени m' .

Доказательство. Эквивалентность 3 и 1 вытекает из предложения 22. Эквивалентность 4, 1 и 3 следует предложения 21 и замечания 5.

Докажем эквивалентность 1 и 2. Пусть известно, что для некоторого целого $m > 0$ и подходящих $\mu_1, \mu_2 \neq 0 \in k[x]$, $b \in k \setminus \{0\}$, $v_h(\mu_2) = 0$ таких, что $\max\{2 \deg \mu_1, 2 \deg \mu_2 + \deg f\} = m \in \mathbb{Z}$, выполнено:

$$\mu_1^2 - \mu_2^2 f = bh^m. \quad (1.26)$$

Без ограничения общности, можем считать, что m — чётно, т.к. в случае нечётного m согласно доказанному выше существует S -единица и мы будем рассматривать уравнение (1.26) соответствующее квадрату S -единицы.

Поделив обе стороны на h^m мы получим выражение (1.25), где $Y = \mu_1 h^{-m/2}$, $Z = \mu_2 h^{-m/2+(g+1)}$, $f/h^{2g+2} \in k[h^{-1}]$.

Обратно, пусть выполнено (1.25).

Тогда $2v_h(Y) = 2v_h(Z) + 2(g+1) = m$. Домножим обе части (1.25) на h^m получаем (1.26). $\square$

Замечание 6. Из доказательства предложения 22 следует, что если будет найдено решение уравнения $\mu_1^2 - \mu_2^2 f = bh^{2m}$, для которого не выполнено $\max\{\deg \mu_1, \deg \mu_2 + g + 1\} = m \deg h$, то элемент u , построенный по найденному решению не является S_h -единицей.

Действительно, пусть $\deg \mu_1 > m \deg h$, тогда $\deg \mu_2 + g + 1 = \deg \mu_1 > m \deg h$. Из (1.24) получаем:

$$\min\{v_\infty^+(\mu_1 + \mu_2 \sqrt{f}), v_\infty^+(\mu_1 - \mu_2 \sqrt{f})\} = \min\{v_\infty^+(\mu_1), v_\infty^+(\mu_2 \sqrt{f})\} < -m \deg h.$$

Т.е. хотя бы одно из двух нормирований v_∞^+ или v_∞^- будет меньше $-m \deg h$. Для определенности, пусть $v_\infty^+(\mu_1 + \mu_2 \sqrt{f}) < -m \deg h$, тогда $v_\infty^+(u) = v_\infty^+(\mu_1 + \mu_2 \sqrt{f}) - v_\infty^+(h^m) < 0$. Последнее противоречит тому, что u — S_h -единица.

Отметим, что подобная ситуация возможна только в случае, если бесконечное нормирование имеет два продолжения на поле L .

Пример 1. Рассмотрим многочлены $f = x^4 + x^3 + \frac{5}{4}x^2 + x + 1$ и $h = x$. В силу того, что старший коэффициент равен 1, бесконечное нормирование имеет два продолжения. Для $\mu_1 = x^2 + \frac{1}{2}x + 1$ и $\mu_2 = 1$ выполнено

$$\mu_1^2 - \mu_2^2 f = h^2.$$

Подгруппа кручения эллиптической кривой, задаваемой уравнением $y^2 = f(x)$, имеет порядок 2. В силу предложения 26 и нижеследующего предложения 27 можно утверждать, что в поле L не существует нетривиальных S_h -единиц, т.к. уравнение (1.25) не имеет решений (иначе была бы точка кручения порядка не меньше $2g + 2 = 4$).

Из теоремы 13, предложения 26 и следствия 12 вытекает следующее утверждение.

Следствие 13. Пусть $\deg h = 1$. Элемент $\frac{\sqrt{f}}{h^{g+1}}$ периодичен тогда и только тогда, когда существует нетривиальная S_h -единица поля $L = k(x)(\sqrt{f})$.

Пусть дополнительно известно, что $\deg f = 2g + 1$. Тогда условие выше эквивалентно периодичности $\frac{\sqrt{f}}{h^g}$, а также существованию S -единицы.

Доказательство. В обоих случаях получаем значение $D = 4\frac{f}{h^{2g+2}}$. По предложению 26 уравнение $Y^2 - DZ^2 = b$, где $Y, Z \in k[h^{-1}]$ имеет решение тогда и только тогда, когда существует нетривиальная S_h -единица. В случае $\deg f = 2g + 1$ это условие равносильно также и существованию S -единицы.

Остается применить теорему 13 и следствие 12. □

Таким образом, условие наличия квазипериодических и периодических элементов в поле L , существования S_h и в соответствующих случаях S -единиц, а также периодичности $\frac{\sqrt{f}}{h^{g+1}}$ — это эквивалентные условия.

Рассмотрим аффинную кривую, заданную уравнением $y^2 = f(x)$. Ей соответствует гладкая проективная гиперэллиптическая кривая C с полем рациональных функций $L = k(x)(\sqrt{f})$. Пусть $\Delta^\circ(C)$ — группа классов дивизоров степени ноль гиперэллиптической кривой C . Мы будем следовать подходу к изложению книги [30], где теория дивизоров дана с использованием понятия плейса (максимального идеала кольца нормирования). В записи дивизора для упрощения обозначений будем плейс, соответствующий нормированию, обозначать тем же символом, что и нормирование. Имеет место следующая связь S и S_h -единиц гиперэллиптического поля L и проблемы кручения в якобиане соответствующей кривой C .

Предложение 27. Пусть h — неприводимый многочлен произвольной степени такой, что ν_h имеет два продолжения на поле L : ν_h^+ и ν_h^- . Поле L обладает фундаментальной S_h -единицей степени n тогда и только тогда, когда класс дивизора $\nu_h^+ - \nu_h^-$ имеет конечный порядок n в $\Delta^\circ(C)$.

В случае, когда бесконечное нормирование имеет одного продолжение на гиперэллиптическое поле, аналогичное утверждение верно и для S -единиц.

Предложение 28. Пусть h — неприводимый многочлен произвольной степени такой, что ν_h имеет два продолжения на поле L : ν_h^+ и ν_h^- . Тогда поле L обладает фундаментальной S -единицей степени n тогда и только тогда, когда класс

дивизора $\mathfrak{v}_h^+ - \deg h \mathfrak{v}_\infty$ имеет конечный порядок n в $\Delta^\circ(C)$. Более того, имеет место соотношение

$$\mathfrak{v}_h^+ - \mathfrak{v}_h^- \sim 2(\mathfrak{v}_h^+ - \deg h \mathfrak{v}_\infty). \quad (1.27)$$

Ограничимся доказательством только предложения 28, доказательство предложения 27 аналогично.

Доказательство. Пусть класс дивизора $\mathfrak{v}_h^+ - \deg h \mathfrak{v}_\infty$ имеет конечный порядок m . Тогда $m(\mathfrak{v}_h^+ - \deg h \mathfrak{v}_\infty) = (u)$, где (u) — дивизор некоторой функции $u \in L$. Очевидно, что u является S -единицей. Ее степень равна m в силу предложения 13 и соотношения (1.26).

Обратно, пусть u — фундаментальная S -единица. Рассмотрим главный дивизор $(u) = m_1 \mathfrak{v}_h^+ + m_2 \mathfrak{v}_\infty$. Поскольку степень дивизора (u) равна нулю, выполняется следующее соотношение:

$$\deg(u) = m_1 \deg h + m_2 = 0.$$

Отсюда получаем $m_2 = -m_1 \deg h$. Таким образом

$$(u) = m_1(\mathfrak{v}_h^+ - \deg h \mathfrak{v}_\infty).$$

В силу предложения 13 и соотношения (1.26) степень S -единицы равна m_1 . Рассмотрим следующий главный дивизор:

$$(h) = \mathfrak{v}_h^+ + \mathfrak{v}_h^- - 2 \deg h \mathfrak{v}_\infty.$$

Откуда $2(\mathfrak{v}_h^+ - \deg h \mathfrak{v}_\infty) = \mathfrak{v}_h^+ - \mathfrak{v}_h^- + (h)$. Т.е. в группе классов дивизоров выполнено (1.27). $\square$

Отметим, что главный дивизор S_h -единицы u_h степени $|m|$ имеет вид $(u_h) = m(\mathfrak{v}_h^+ - \mathfrak{v}_h^-)$, и можно считать, что $m > 0$, т.к. в противном случае, можно рассматривать S_h -единицу u_h^{-1} . Главный дивизор S -единицы u степени $m > 0$ имеет вид $(u) = m(\mathfrak{v}_h^+ - \deg h \mathfrak{v}_\infty)$.

В примере 1 мы видели, что в случае существования двух продолжений бесконечного нормирования старшие мономы левых частей в уравнении (1.26) могут сократиться. Однако в случае, если продолжение единственно, старшие мономы не сокращаются и согласно замечанию 5 S и S_h -единицы существуют одновременно и связаны между собой. Из предложения 28 нетрудно следует, что степени фундаментальных S и S_h -единиц связаны между собой.

Следствие 14. Пусть v_∞ имеет одно продолжение на поле L и пусть $S = \{v_h^+, v_\infty\}$.

Если поле L обладает фундаментальной S_h -единицей u_h степени m , то или $u = h^m u_h$ или $h^m u_h^{-1}$ — S -единица степени $2m$. Она является либо фундаментальной S -единицей, либо квадратом фундаментальной S -единицы.

Если существует фундаментальная S -единица u степени $m > 0$, то u^2/h^m — нетривиальная S_h -единица степени m . Более того, S_h -единица u^2/h^m является фундаментальной, если m — нечетное число. В противном случае, поле L обладает фундаментальной S_h -единицей степени $m/2$.

Доказательство. Главный дивизор S_h -единицы u_h степени m имеет вид $(u_h) = m(v_h^+ - v_h^-)$, будем считать, что $m > 0$, т.к. в противном случае, можно рассматривать S_h -единицу u_h^{-1} . Главный дивизор S -единицы u степени $m > 0$ имеет вид $(u) = m(v_h^+ - \deg h v_\infty)$.

Из рассуждений выше следует, что если u_h — фундаментальная S_h -единица степени m , то $u_h h^m$ — S -единица степени $2m$, а если u — фундаментальная S -единица степени m , то u^2/h^m — S_h -единица степени m . Откуда понятно, что если S_h -единица степени m является фундаментальной, то в силу (1.27) ей соответствует фундаментальная S -единица степени или m или $2m$. Верно и обратное: фундаментальной S -единице степени $m > 0$ соответствует фундаментальная S_h -единица степени или $m/2$ или m в зависимости от четности m . $\square$

1.3 Периодичность квадратного корня

Пусть на протяжении всего параграфа §1.3 $\deg h = 1$. В теореме 13 и следствии 9 был установлен критерий квазипериодичности произвольной квадратичной иррациональности $\frac{v+w\sqrt{f}}{u}$, $v, w, u \in k[x]$. Рассмотрим теперь более точный критерий квазипериодичности элемента $\frac{\sqrt{f}}{h^s}$, $s \in \mathbb{Z}$.

Определение 12. Будем называть фундаментальным решением уравнения (1.25) в многочленах от h^{-1} решение с максимальным значением $v_h(Y) < 0$.

Пусть $\deg f = 2g + 1$ или $\deg f = 2g + 2$. Тогда $\lceil \frac{\deg f}{2} \rceil = g + 1$, а

$$\left\lfloor \frac{\deg f}{2} \right\rfloor = \begin{cases} g, & \text{если } \deg f = 2g + 1, \\ g + 1, & \text{если } \deg f = 2g + 2. \end{cases}$$

Теорема 15. Пусть f — бесквадратный многочлен. Элемент $\alpha = \frac{\sqrt{f}}{h^s}$, $s \in \mathbb{Z}$ квазипериодичен тогда и только тогда, когда существует такая пара Y, Z , являющаяся решением уравнения (1.25), где $Z = Z'h^{-l}$ и $Y, Z' \in k[h^{-1}]$, $l = \max\{s - \lceil \frac{\deg f}{2} \rceil, \lfloor \frac{\deg f}{2} \rfloor - s\}$.

Более того, если $\deg f = 2g + 1$, то достаточно рассматривать только фундаментальное решение уравнения (1.25). Такое решение соответствует фундаментальной S -единице четной степени или квадрату фундаментальной S -единицы нечетной степени.

Доказательство. В случае $l = 0$ теорема верна в силу следствия 13, поэтому будем предполагать, что $l > 0$.

Из следствия 9 вытекает, что α квазипериодичен тогда и только тогда, когда $Y, Z = Z'h^{-l}$, где $Y, Z' \in k[h^{-1}]$, $l = \max\{s - (g + 1), \lfloor \frac{\deg f}{2} \rfloor - s\}$ — некоторое нетривиальное решение уравнения (1.25).

Пусть $\deg f = 2g + 1$. Тогда $l = \max\{s - (g + 1), g - s\}$. И пусть T, U — фундаментальное решение уравнения (1.25). Обозначим $F = f/h^{2g+1} \in k[h^{-1}]$. В силу того, что нетривиальная группа S -единиц равна произведению $k \setminus \{0\}$ и бесконечной циклической группы, а также предложения 26 для всякого решения Y, Z выполнено следующее:

$$Y + Z\sqrt{h^{-1}F} = c \left(T + U\sqrt{h^{-1}F} \right)^m, \quad c \in k \setminus \{0\}.$$

Откуда

$$Z = cU \sum_{i \geq 0} \binom{m}{2i+1} T^{m-2i-1} (h^{-1}F)^i U^{2i}.$$

Следовательно, если h^{-l} делит Z в кольце $k[h^{-1}]$, т.е. $Z = h^{-l}Z'$, где $Z', h^{-l} \in k[h^{-1}]$, то либо $h^l \mid U$, либо $h^l \nmid U$ и $h^{-1} \mid T$. Однако, из (1.25) для T, U следует, что $h^{-1} \nmid T$. $\square$

Замечание 7. В частности, теорема 15 даёт критерий квазипериодичности $\sqrt{f}$. Он квазипериодичен тогда и только тогда, когда найдётся решение $s - l \geq g + 1$ в случае, если $\deg f = 2g + 2$, или решение $s - l \geq g$ в случае, если $\deg f = 2g + 1$.

Для поля констант $k = \mathbb{Q}$ и $\deg f = 3$ из ограниченности числа периодических элементов $\sqrt{f}$ (см. [22]) и теоремы 15 следует, что квазипериодических элементов с $\sqrt{f}/h^s$ с $s < 0$ или $s > \deg f$ не существует. Кроме того, даже с использованием компьютерных вычислений автору не удалось построить примеры таких элементов для $k = \mathbb{Q}$ и $\deg f > 3$. Автору неизвестны такие примеры и автор полагает, что, вероятно, их не удастся найти. Теорема 15 показывает, что если элемент $\sqrt{f}/h^s$ квазипериодичен для некоторого $s = s_0 \leq \frac{\deg f}{2}$, то он периодичен для всех s из диапазона $s_0 \leq s \leq \frac{\deg f}{2}$. Вышесказанное дополнительно мотивирует к изучению элементов с “пограничными” значениями $s = 0$ и $s = \deg f$.

В следствии 13 было доказано, что элемент $\sqrt{f}/h^{g+1}$ квазипериодичен всегда, когда в поле L есть нетривиальная S_h -единица. А в случае $\deg f = 2g + 1$ из существования нетривиальных S -единиц в поле L следует периодичность элементов $\sqrt{f}/h^{g+1}$, $\sqrt{f}/h^g$. А что можно сказать про случаи $s < \lfloor \frac{\deg f}{2} \rfloor$ и $\lceil \frac{\deg f}{2} \rceil < s$? В силу следствия 10 достаточно рассматривать только условие $s < \lfloor \frac{\deg f}{2} \rfloor$. И оказывается, что не всегда можно утверждать, что при наличии нетривиальных S_h -или S -единиц в поле L элемент $\sqrt{f}/h^s$ обязательно квазипериодичен или, наоборот, не квазипериодичен для заданного $\deg f$ и $s < \lfloor \frac{\deg f}{2} \rfloor$. В частности, элемент $\sqrt{f}$, как правило, не квазипериодичен. Однако, встречаются и редкие исключения. Теорема 15 и алгоритм построения фундаментальной S -единицы из [13] и параграфа §2.3 дают инструмент для определения квазипериодичности элементов такого типа. Рассмотрим следующий простой, но показательный пример.

Пример 2. Возьмем $g > 0$, $k = \mathbb{Q}$, $h = x$ и $f = ax^w + 1$, $a \in \mathbb{Q} \setminus \{0\}$, где $w = 2g + 1$ или $w = 2g + 2$. Решение уравнения (1.25) выглядит следующим образом:

$$Y = 1 + \frac{2}{ax^w}, Z = \frac{2}{ax^{w-g-1}}; Y^2 - Z^2 \frac{f}{x^{2g+2}} = 1.$$

Оно фундаментально в силу того, что нетривиального решения (1.25) с $0 > \nu_h(Y) > -(2g + 2)$ не существует. Из него получаем, что $Z = \frac{2}{a}h^{-(g+1-w)}$. И следовательно, по теореме 15 элементы $\sqrt{f}$, $\frac{\sqrt{f}}{h^s}$, $s = 1, \dots, w$, квазипериодичны.

По следствию 12 заключаем, что элементы $\frac{\sqrt{f}}{h^s}$, $s = 1, \dots, w$ периодичны, а чтобы доказать периодичность $\sqrt{f}$ достаточно рассмотреть его первое полное частное и применить теорему 14. В самом деле, рассмотрим $\alpha_1 = \frac{1}{\sqrt{f} - [\sqrt{f}]}$ — первое полное частное к $\sqrt{f}$. Получаем $\alpha_1 = \frac{\sqrt{f} + [\sqrt{f}]}{f - ([\sqrt{f}])^2}$. Откуда $\alpha_1 + \alpha'_1 = \frac{2[\sqrt{f}]}{f - ([\sqrt{f}])^2} =$

$\frac{2}{ax^w} \in k[h^{-1}]$. Кроме того

$$\begin{aligned} \mathbf{v}_h(\alpha_1) &= -\mathbf{v}_h(ax^w) < 0, \\ \mathbf{v}_h(\alpha'_1) &= -\mathbf{v}_h(\sqrt{f} - [\sqrt{f}]) < 0, \\ \mathbf{v}_h(\alpha_1 - \alpha'_1) &= \mathbf{v}_h\left(\frac{2\sqrt{f}}{f - ([\sqrt{f}])^2}\right) = -\mathbf{v}_h(ax^w) < 0. \end{aligned}$$

По теореме 14 элемент α_1 периодичен, а следовательно, периодичен и элемент $\alpha = \sqrt{f}$.

Для $g = 2$ найти периодичный $\sqrt{f}$ и h , для которых степень соответствующей S -единицы поля $\mathbb{Q}(x)(\sqrt{f})$ будет больше 5 сравнительно трудная задача. Укажем здесь пример таких f, h , для которых соответствующая S -единица обладает степенью 7, а $\sqrt{f}$ периодичен. Непосредственное применение теоремы 14, как это было сделано в примере 2, к элементу из нижеследующего примера 3 не позволяет доказать его периодичность. Впрочем, для конкретного элемента периодичность следует из явного вида непрерывной дроби.

Пример 3. Возьмем $g = 2, k = \mathbb{Q}, h = x$ и $f = 4x^5 - 8x^4 + 12x^3 - 16x^2 + 20x + 25$. Нетривиальная S -единица существует, и фундаментальное решение уравнения (1.25) выглядит следующим образом:

$$\begin{aligned} Y &= -1 - \frac{49}{2x^5} - \frac{35}{x^6} - \frac{25}{2x^7}, Z = -\frac{7}{2x^2} - \frac{6}{x^3} - \frac{5}{2x^4} = \frac{1}{x^2}\left(-\frac{7}{2} - \frac{6}{x} - \frac{5}{2x^2}\right); \\ Y^2 - Z^2 \frac{f}{x^6} &= 1. \end{aligned}$$

Откуда получаем, что $Z = Z'h^{-2}$. И следовательно, по теореме 15 элементы $\sqrt{f}, \frac{\sqrt{f}}{h^s}, s = 1, \dots, 5$, квазипериодичны. По следствию 12 заключаем, что элементы $\frac{\sqrt{f}}{h^s}, s = 1, \dots, 5$ периодичны.

Разложение $\sqrt{f}$ является периодическим и выглядит следующим образом

$$\sqrt{f} = [5, \frac{1}{2x} + \frac{1}{2}, \overline{-4 + \frac{4}{x} - \frac{4}{x^2} + \frac{4}{x^3} - \frac{4}{x^4} - \frac{10}{x^5}, \frac{1}{2x} + \frac{3}{5}, -\frac{50}{x} - 60, \frac{1}{25} - \frac{1}{25x} + \frac{1}{25x^2} - \frac{1}{25x^3} + \frac{1}{25x^4} + \frac{1}{10x^5}, -\frac{50}{x} - 60, \frac{1}{2x} + \frac{3}{5}}].$$

Пример 4. Возьмем $g = 2, k = \mathbb{Q}, h = x$ и $f = (8x^2 + 7x + 2)(5x^2 + 4x + 1)(3x + 2)$. Нетривиальная S -единица существует, и фундаментальное решение уравнения (1.25) выглядит следующим образом:

$$Y = -1 - \frac{48}{5x} - \frac{74}{5x^2} - \frac{8}{x^3} - \frac{8}{5x^4}, Z = -\frac{2}{5} - \frac{4}{5x}; Y^2 - Z^2 \frac{f}{x^6} = 1.$$

Откуда получаем, что $h^{-1} \nmid Z$. И следовательно, по теореме 15 элементы $\frac{\sqrt{f}}{h^s}$, $s \neq 2, 3$, не квазипериодичны. В частности, не квазипериодичен $\sqrt{f}$.

В работах [22; 23] для эллиптического случая $\deg f = 3$ и поля рациональных чисел в качестве поля констант доказана конечность в некотором смысле числа классов многочленов, корень из которых разлагается в квазипериодическую непрерывную дробь. Однако в общем случае произвольной степени f вопрос о конечности остается открытым.

Как отмечалось выше для произвольного многочлена f метод доказательства периодичности квазипериодического корня, используемый в примере 2, не применим. Доказательство этого факта требует иных подходов.

Лемма 3. Пусть многочлен $f \in k[x]$ свободен от квадратов, а $\sqrt{f} \in k((h))$ квазипериодичен. Тогда существует делитель d многочлена f такой, что для некоторого n выполнено $L_n = bdh^w$, причём $w + \deg d = \deg f$, $b \in k \setminus \{0\}$, а $0 \leq \deg d < \deg f$.

Доказательство. По теореме 15 квазипериодичность $\sqrt{f} \in k((h))$ равносильно существованию решения $Y, Z \in k[h^{-1}]$, $Z \neq 0$, уравнения

$$Y^2 - Z^2 \frac{f}{h^{2g+2}} = b \in k \setminus \{0\}, \quad (1.28)$$

и при этом $Z = Z'h^{-l}$, где $v_h(Z') \neq 0$ и $l \geq \lfloor \frac{\deg f}{2} \rfloor$.

Среди всех таких решений выберем решение с минимальным значением $-v_h(Y) = e$, тогда из (1.28) следует, что выполнено равенство

$$p'^2 - fq'^2 = b'h^{2e}, \quad (1.29)$$

где $p' = Yh^e$, $q' = Zh^{e-g-1}$. При этом, в силу того, что $Z = Z'h^{-l}$, заключаем, что $\deg p' = e$, $\deg q' = e - (g + 1 + l)$.

В силу того, что $l > 0$, мы можем утверждать, что $b' = (p'_e)^2 \in k \setminus \{0\}$, где p'_e — старший коэффициент многочлена p . Преобразуем (1.29) следующим образом

$$(p' - p'_e h^e)(p' + p'_e h^e) = q'^2 f.$$

Рассмотрим произвольный отличный от константы делитель многочлена f : если он делит одновременно две скобки выражение слева, то, очевидно, он делит и h^e , а это противоречит тому, что $h \nmid f$. Следовательно, любой делитель многочлена f делит либо одну, либо другую скобку. Обозначим произведение делителей, делящих $p' - p'_e h^e$, через d . Тогда выполнено:

$$\begin{aligned} p' - p'_e h^e &= dp^2, \\ p' + p'_e h^e &= \frac{f}{d} q^2. \end{aligned} \quad (1.30)$$

Откуда

$$\frac{f}{d} q^2 - dp^2 = bh^e, \quad (1.31)$$

где $b = 2p'_e \in k$, $p, q \in k[x]$. И выполнено $p' = \frac{1}{2}(\frac{f}{d} q^2 + dp^2)$, $q' = qp$.

Перепишем (1.31) следующим образом:

$$fq^2 - (dp)^2 = bdh^e.$$

Наша задача — выяснить, при каких условиях dp/q совпадает с подходящей дробью P_n/Q_n к $\sqrt{f}$ для некоторого n . Чтобы доказать требуемое, нам по предложению 15 необходимо и достаточно показать, что $v_h(\bar{q}\sqrt{f} - \overline{dp}) > -v_h(\bar{q})$, где $\frac{dp}{q} = \frac{\overline{dp}}{\bar{q}}$ и $\overline{dp} = dph^{-r}$, $\bar{q} = qh^{-r} \in k[h^{-1}]$, $r = \max\{\deg q, \deg d + \deg p\}$. В силу предложения 13 и того, что h не делит f , без ограничения общности можно считать, что $v_h(q\sqrt{f} - dp) = e$, откуда $v_h(\bar{q}\sqrt{f} - \overline{dp}) = e - r$. Таким образом, в силу того, что $v_h(\bar{q}) = -r$, нам необходимо показать, что $e > 2r$.

Пусть $\deg d = t$. Тогда из (1.30) и (1.31) следует, что $2\deg q + \deg f = t + e$ и $2(t + \deg p) = t + e - m_p \leq t + e$ для некоторого $m_p > 0$. Откуда $r = \frac{e+t-m'}{2}$, где $m' = \min\{m_p, \deg f\}$.

Отсюда, необходимое и достаточное условие: $e > 2r$ на то, что dp/q — наилучшее приближение к $\sqrt{f}$, становится равносильно условию $m' > t$.

С другой стороны, $\deg q' = \deg p + \deg q = e - \frac{1}{2}(m_p + \deg f)$. Следовательно, $m_p = 2l + (2g + 2 - \deg f) > 0$, т.е. $m_p = 2l$, если $\deg f = 2g + 2$, и $m_p = 2l + 1$, если $\deg f = 2g + 1$.

В силу того, что $l \geq \lfloor \frac{\deg f}{2} \rfloor$, получаем $m_p \geq \deg f$. Следовательно, выполнено $m' = \deg f$. Откуда вытекает требуемое условие, если выполнено $t < \deg f$.

Рассмотрим оставшийся случай. Пусть $t = \deg f$, тогда $q^2 - fp^2 = bh^e$, причем $2 \deg q = e$, а $\deg p = \frac{e - (m_p + \deg f)}{2} = e/2 - (g + 1 + l)$. Поделив обе части уравнения (1.31) на h^e , мы получим решение $Y_1 = qh^{-e}$, $Z_1 = ph^{-e} \in k[h^{-1}]$ уравнения (1.28), причем $Z_1 = Z'_1 h^{-l}$, а $-\nu_h(Y_1) = e/2$. Полученное противоречит минимальности e и минимальности решения Y, Z уравнения (1.28).

Таким образом, мы доказали, что для некоторого n выполнено $dp/q = P_n/Q_n$, и с точностью до константы выполнено $P_n = \overline{dp}$, $Q_n = \overline{q}$. Откуда $L_n = b''dh^{e-2r}$, а, как показано выше, $w = e - 2r = m' - t$, следовательно, $t + w = m'$. Наконец, $m' = \min\{m_p, \deg f\}$, и при условии, что $m_p \geq \deg f$, получаем $t + w = \deg f$. $\square$

С использованием леммы удастся доказать следующую теорему.

Теорема 16. Пусть многочлен f свободен от квадратов, а $\alpha = \sqrt{f}$ квазипериодичен. Тогда существует делитель d многочлена f , такой что $\{\alpha_{n+1}\} = b\{\frac{\sqrt{f}}{dh^w}\}$, где $\deg d = t$, $0 \leq \deg d < \deg f$, а $w = \deg f - t$.

Доказательство. В силу леммы 3 заключаем, что существует делитель d многочлена f , $\deg d = t$, и некоторый номер n , такие что $L_n = bdh^w$.

Тогда по формуле (1.11) для $\alpha = \sqrt{f}$ получаем следующее:

$$\alpha_{n+1} = \frac{M_n + \sqrt{f}}{L_n} = \frac{M_n}{bdh^w} + \frac{1}{b} \frac{\sqrt{f}}{dh^w}. \quad (1.32)$$

В силу соотношения (1.17) для $\sqrt{f}$ выполнено $f - M_n^2 = L_n L_{n-1}$ и бесквадратности f мы можем утверждать, что если делитель d многочлена f делит L_n , то он делит и многочлен M_n . Кроме того, по (1.15) имеем $\deg M_n \leq \deg f$. Откуда следует, что $\frac{M_n}{bdh^w} \in k[h^{-1}]$, что в свою очередь вместе с соотношением (1.32) завершает доказательство теоремы. $\square$

Рассмотрим пример из [25].

Пример 5. Пусть $f = (6x + 5)(x^4 - 2x^3 + 3x^2 - 4x + 5)$, $h = x$. Элемент $\alpha = \sqrt{f}$ периодичен. Более того,

$$\alpha = [5, x^{-1} + 1, \overline{-2(1 - x^{-1} + x^{-2} - x^{-3} + x^{-4}), 1/10(11 + 10x^{-1}), -10(11 + 10x^{-1})}^{-\frac{1}{100}}].$$

В то время как

$$\frac{\sqrt{f}}{(6x+5)x^4} = [1 - x^{-1} + x^{-2} - x^{-3} + x^{-4},$$

$$-\frac{1}{10}(11 + 10x^{-1}), 10(11 + 10x^{-1}), -\frac{1}{50}(1 - x^{-1} + x^{-2} - x^{-3} + x^{-4})]^{-100}.$$

Таким образом, $\{\alpha_2\} = -\{\frac{\sqrt{f}}{(6x+5)x^4}\}$.

Следствие 15. В условиях теоремы 16 пусть $\sqrt{f}$ квазипериодичен. Тогда $\sqrt{f}$ — периодичен.

Доказательство. В силу следствия 10 заключаем, что элемент $\frac{\sqrt{f}}{dh^w}$ квазипериодичен для любого делителя d многочлена f , где $w = \deg f - \deg d$. По следствию 12 этот элемент периодичен. Остается применить теорему 16. $\square$

Следствие 16. В условиях теоремы 16 выполнено $\sqrt{f} = [A_0, \dots, A_{n+1}, \overline{B_1, \dots, B_N}]$, где $B_i = B_{N-i}$, для $i = 1, \dots, N-1$.

Доказательство. Теорема 16 утверждает, что $\{\alpha_{n+1}\} = b\{\frac{\sqrt{f}}{dh^w}\}$.

В силу следствия 12 получаем $\frac{\sqrt{f}}{dh^w} = [\frac{1}{2}B_N, \overline{B_1, \dots, B_N}]$, где $B_i = B_{N-i}$, для $i = 1, \dots, N-1$, откуда $\alpha_{n+2} = [\overline{B_1, \dots, B_N}]$. $\square$

Итогом этого параграфа является следующая теорема.

Теорема 17. Пусть $s \in \mathbb{Z}$, $f \in k[x]$ — свободный от квадратов многочлен произвольной степени, $d \in k[x]$ — делитель многочлена f , и $h \in k[x]$ — линейный многочлен. Квазипериодичность разложения в функциональную непрерывную дробь элемента $\frac{\sqrt{f}}{dh^s}$ в $k((h))$ равносильна его периодичности. В частности, квазипериодичность $\sqrt{f}$ равносильна его периодичности.

Глава 2. Случай нечетной степени многочлена, определяющего гиперэллиптическое поле

На протяжении всей главы 2 будем, если не оговорено обратное, предполагать, что $\deg f = 2g + 1$ и $\deg h = 1$.

2.1 Симметрии разложения $\sqrt{f}$ и непрерывная дробь для $\sqrt{f}/h^s$

Утверждения, используемые в параграфе §1.3, в случае $\deg f = 2g + 1$ могут быть обобщены на более широкий класс элементов.

Лемма 4. Пусть $s > 0$, $\deg f = 2g + 1$ или $\deg f = 2g + 2$ и элемент $\alpha = \sqrt{f}/h^s$ — квазипериодичен. Тогда найдется такой номер n , для которого выполнено $L_n = h^{2s}P_n^2 - Q_n^2f = bh^{2s}$, $b \in k \setminus \{0\}$, где P_n/Q_n — n -ая подходящая дробь к α .

Пусть теперь $\deg f = 2g + 1$, $s \geq 0$, элемент $\alpha = \sqrt{f}/h^s$ квазипериодичен и дополнительно известно, что поле L обладает нетривиальной S -единицей нечетной степени. Тогда найдется такой номер n , для которого выполнено $L_n = bh^{2g+1}$, $b \in k \setminus \{0\}$.

Доказательство. По следствию 9 наличие квазипериодических элементов в $k(x)(\sqrt{f})$ равносильно существованию нетривиального решения уравнения (1.20):

$$Y^2 - Z^2F = b, \quad (2.1)$$

где $F = f/h^{2g+2}$, $Y, Z'h^{-l} = Z \in k[h^{-1}]$, $l \geq 0$, $b \in k \setminus \{0\}$.

Тогда для любого s выполнено:

$$h^{2s}Y^2 - (Z')^2h^{2(s-l-g-1)}f = bh^{2s}.$$

Пусть $\nu_h(Y) = e$, тогда из (2.1) получаем $\nu_h((h^eY)^2 - (h^{e-g-1}Z)^2f) = 2e$, причем $h^eY, h^{e-g-1}Z \in k[x]$ и по предложению 13 без ограничения общности получаем $\nu_h\left(Y - Zh^{s-g-1}\frac{\sqrt{f}}{h^s}\right) = \nu_h\left(h^eY - Zh^{e+s-g-1}\frac{\sqrt{f}}{h^s}\right) - \nu_h(h^e) = e$. В то же время $-\nu_h(Zh^{s-g-1}) = e - s$. Таким образом, по предложению 15 мы можем

утверждать, что если $s > 0$ и $s - l - g - 1 \leq 0$, то для некоторого n выполнено $L_n = h^{2s}P_n^2 - Q_n^2f = b'h^{2s}$, где с точностью до константы $P_n = Y$, $Q_n = Z'h^{s-l-g-1}$ и P_n/Q_n — подходящая дробь к $\alpha = \sqrt{f}/h^s$.

Если $0 < s \leq g + 1$, то первое утверждение леммы выполняется автоматически для любого $l \geq 0$, если же $s > g + 1$, то вышеуказанные условия на s выполнены тогда и только тогда, когда $s - (g + 1) \leq l$, что, в силу теоремы 15 равносильно квазипериодичности элемента α .

Пусть теперь $\deg f = 2g + 1$, $s \geq 0$ и степень фундаментальной S -единицы $u = p + q\sqrt{f}$ является нечетным числом m . Тогда фундаментальное решение уравнения (1.20) соответствует квадрату фундаментальной S -единицы (см. замечание 10). Кроме того, согласно предложению 15 найдется такой номер n , что $p/q = P_n/Q_n$.

В силу теоремы 15 получаем, что $\sqrt{f}/h^s$ квазипериодичен тогда и только тогда, когда существуют пара $Y, Z'h^{-l}$ — фундаментальное решение уравнения (1.20). Т.е. $Y^2 - (Z'h^{-(g+1+l)})^2f = b$, где $l = \max(s - (g + 1), g - s)$.

Пусть $\deg q = t$, тогда в силу нечетности m и тождества $p^2 - q^2f = bh^m$ получаем $m = 2t + 2g + 1$. Перепишем тождество: $h^{2s}p^2 - (qh^s)^2f = bh^{m+2s}$.

В силу вышесказанного, если для $s \geq 0$ окажется, что $\deg p \leq t + s$, мы сможем утверждать, что с точностью до константы $P_n = p/h^t$, $Q_n = q/h^{t+s}$, где P_n/Q_n — подходящая дробь к α и $L_n = bh^{2g+1}$.

Рассмотрим $u^2 = p_1 + q_1\sqrt{f}$, где $p_1 = p^2 + q^2f$, $q_1 = 2pq$. S -единица u^2 с точностью до константы соответствует фундаментальному решению Y, Z , причем с точностью до константы $Y = p_1/h^m$, $Z = q_1/h^{m-(g+1)}$. Откуда $q_1 = Z'h^{m-(g+1)-l}$ и, следовательно, $t + \deg p = \deg q_1 \leq m - (g + 1 + l)$. Таким образом, $\deg p \leq t + g - l$.

Пусть $s \geq g + 1$ и $l = s - (g + 1)$. В этом случае имеем $\deg p \leq t + 2g + 1 - s \leq t + s$. Пусть $s \leq g$ и $l = g - s$. В этом случае имеем $\deg p \leq t + s$.

В обоих случаях мы можем утверждать, что $L_n = bh^{2g+1}$. □

С использованием леммы удастся доказать следующую теорему.

Теорема 18. Пусть $0 \leq s \leq g$, $\deg f = 2g + 1$ и $\alpha = \sqrt{f}/h^s$ — квазипериодичен, и пусть поле L обладает S -единицей нечетной степени. Тогда существует n такое, что $b\{\alpha_{n+1}\} = \{\sqrt{f}/h^{2g+1-s}\}$, где $b \in k \setminus \{0\}$.

Доказательство. Выпишем формулу (1.11) для нашего случая:

$$\alpha_{n+1} = \frac{M_n + h^{2s}\alpha}{L_n}. \quad (2.2)$$

В силу леммы 4 имеем, что для некоторого n выполнено $L_n = bh^{2g+1}$. Кроме того, $\deg M_n \leq \max\{2s, 2g+1\} = 2g+1$.

Тогда в силу (2.2) получаем $b\alpha_{n+1} = M_n/h^{2g+1} + \sqrt{f}/h^{2g+1-s}$. Откуда $M_n/h^{2g+1} \in k[h^{-1}]$ и $b\{\alpha_{n+1}\} = \{\sqrt{f}/h^{2g+1-s}\}$.

□

Отметим, что для f нечетной степени $2g+1$ при наличии нетривиальной S -единицы элементы $\sqrt{f}/h^g$ и $\sqrt{f}/h^{g+1}$ периодичны всегда. И поэтому теорема 18 вместе с нижеследующим примером 6 демонстрирует существенное различие между случаями существования фундаментальной S -единицы поля L четной и нечетной степени. Пример показывает, что для полей, содержащих S -единицы только четных степеней утверждение теоремы 18 вообще говоря не верно.

Пример 6. Возьмем $g = 2$, $k = \mathbb{Q}$, $h = x$ и $f = 220x^5 + 224x^4 - 1054x^3 + 1072x^2 - 468x + 81$, $h = x$. Степень фундаментальной S -единицы равна 6.

$$\begin{aligned} \alpha^{(2)} &= \sqrt{f}/h^2 = [-26/x + 9/x^2 + 22, \overline{1/5/x, -52/x + 18/x^2 + 44}], \\ \alpha^{(3)} &= \sqrt{f}/h^3 = [22/x - 26/x^2 + 9/x^3 + 5, \\ &\quad \overline{-44/25/x + 52/25/x^2 - 18/25/x^3 - 2/5, 44/x - 52/x^2 + 18/x^3 + 10}]. \end{aligned}$$

Очевидно, ни для каких n , m и $b \in \mathbb{Q} \setminus \{0\}$ не выполнено $\alpha_n^{(2)} = b\alpha_m^{(3)}$, т.к. в разложении $\alpha^{(3)}$ есть бесконечно много элементов с нормированием -3, а для разложения $\alpha^{(2)}$ это не так.

Выпишем формулу (1.17) для $\alpha = \sqrt{f}$:

$$L_n = \frac{f - M_n^2}{L_{n-1}}. \quad (2.3)$$

Подставляя (2.3) в (2.2) получаем:

$$\sqrt{f} - M_n = \frac{L_{n-1}}{\alpha_{n+1}}.$$

Отсюда коэффициент с номером m многочлена M_n выглядит следующим образом:

$$M_{n,m} = f_m, \quad m = 0, 1, \dots, s_n + s_{n+1} - 1, \quad (2.4)$$

где $\sqrt{f} = \sum_{j=0}^{\infty} f_j h^j$, $s_n = -\mathbf{v}_h(\alpha_n) = -\mathbf{v}_h(A_n) = \mathbf{v}_h(L_{n-1})$.

Следствие 17. В условиях теоремы 18 для $\alpha = \sqrt{f} = [A_0, A_1, \dots]$ выполняется $A_{n+1} = 2/b[\sqrt{f}/h^{2g+1}]$. Более того, $\sqrt{f} = [A_0, \dots, A_n, \overline{B_1, \dots, B_N}]$, где $B_i = B_{N+2-i}$, для $i = 2, \dots, N$.

Доказательство. Как в доказательстве теоремы 18 получаем $b\alpha_{n+1} = M_n/h^{2g+1} + \sqrt{f}/h^{2g+1}$. В силу (2.4) получаем

$$M_{n,m} = f_m, \quad m = 0, 1, \dots, s_n + s_{n+1} - 1,$$

где $s_{n+1} = 2g + 1$, а $s_n \geq 1$. Откуда в силу того, что $\deg M_n \leq 2g + 1$:

$$\begin{aligned} bA_{n+1} &= 2[\sqrt{f}/h^{2g+1}], \\ b\{\alpha_{n+1}\} &= \{\sqrt{f}/h^{2g+1}\}. \end{aligned}$$

Пусть $\alpha^{(2g+1)} = \sqrt{f}/h^{2g+1} = [A_0^{(2g+1)}, \overline{A_1^{(2g+1)}, \dots, A_M^{(2g+1)}}]$.

В силу следствия 12, и теоремы 18 получаем, что

$$\alpha_{n+1} = b^{-1} [2A_0^{(2g+1)}, \dots, A_{M-1}^{(2g+1)}].$$

Откуда следуют указанные в утверждении симметрии. □

Пример 7. Возьмем $g, k, h = x$ и f как в примере 3.

В качестве иллюстрации к теореме и следствию 17 отметим, что $\alpha_3^{(0)} = -\alpha_1^{(5)}$, $\alpha_1^{(1)} = -\alpha_3^{(4)}$, $\alpha_1^{(2)} = -\alpha_3^{(3)}$, где $\alpha^{(s)} = \sqrt{f}/h^s = [A_0^{(s)}, A_1^{(s)}, \dots]$. Кроме того, $A_2^{(0)} = -2A_0^{(5)}$.

2.2 Квазипериодические, но не периодические элементы

В первой главе мы рассматривали некоторые важные квазипериодические элементы, которые с необходимостью являются периодическими. Несмотря на то, что каждая непрерывная дробь сходится к некоторому элементу из $k((h))$, в литературе практически не встречается явный вид квазипериодических, но не

периодических элементов. В настоящем параграфе мы изучим свойства таких элементов в гиперэллиптических полях, порождённых многочленами нечётной степени.

Обозначим для $B = b_0 + b_{-1}h^{-1} + \dots + b_{-n}h^{-n} \in k[h^{-1}]$ значение свободного коэффициента за $\text{fc}(B) = b_0$.

Предложение 29. *Квазипериодический, но не периодический, элемент $\alpha = [\overline{A_0, A_1^c}]$, $c \in k \setminus \{0\}$, $A_i \in k[h^{-1}]$, лежит в $k(x)(\sqrt{f})$ для некоторого многочлена f нечётной степени только, если $\text{fc}(A_0)\text{fc}(A_1) = \frac{-(1+c)\pm 2\sqrt{c}}{c}$, где $t_i = \nu_h(A_i)$.*

Доказательство. Рассмотрим непрерывную дробь элемента $\alpha = [\overline{A_0, A_1^c}]$, $c \neq 1$, $c \in k \setminus \{0\}$:

$$\begin{aligned}\alpha &= A_0 + \frac{1}{A_1 + \frac{1}{c\alpha}} = A_0 + \frac{c\alpha}{c\alpha A_1 + 1} \\ &= \frac{c\alpha A_1 A_0 + c\alpha + A_0}{c\alpha A_1 + 1}.\end{aligned}$$

Откуда получаем квадратичную зависимость на α :

$$\alpha^2 c A_1 + \alpha(1 - c A_0 A_1 - c) - A_0 = 0,$$

где $A_0, A_1 \in k[h^{-1}]$. Пусть $s_i = -\nu_h(A_i)$, для $i = 0, 1$. Тогда перепишем зависимость в виде многочленов из $k[h]$.

$$\alpha^2 c a_1 h^{s_0} + \alpha(h^{s_0+s_1}(1-c) - c a_0 a_1) - a_0 h^{s_1} = 0,$$

где $a_i = A_i h^{s_i} \in k[h]$, при этом кольца $k[h]$ и $k[x]$ изоморфны. Дискриминант для этого уравнения равен

$$D = (h^{s_0+s_1}(1-c) - c a_0 a_1)^2 + 4 c a_0 a_1 h^{s_0+s_1}.$$

Ясно, что если $\deg a_i < s_i$ для некоторого i , то $\deg D$ будет чётным числом. Наша задача выбрать такие A_i , чтобы итоговый D имел нечётную степень. Раскроем дискриминант:

$$\begin{aligned}D &= h^{2(s_0+s_1)}(1-c)^2 - 2c(1-c)a_0 a_1 h^{s_0+s_1} \\ &\quad + c^2 a_0^2 a_1^2 + 4 c a_0 a_1 h^{s_0+s_1} = \\ &= (h^{s_0+s_1})^2(1-c)^2 + 2(c+1)(c a_0 a_1) h^{s_0+s_1} \\ &\quad + (c a_0 a_1)^2.\end{aligned}$$

Напомним, что многочлены записаны как многочлены от h . Мы хотим, чтобы старшие коэффициенты сократились. Положим $z = c \operatorname{lc}(a_0) \operatorname{lc}(a_1)$ и запишем желаемое:

$$(1 - c)^2 + 2(1 + c)z + z^2 = 0.$$

Это уравнение имеет решения вида

$$\begin{aligned} z &= \frac{1}{2}(-2(1 + c) \pm \sqrt{4(1 + c)^2 - 4(1 - c)^2}) \\ &= -(1 + c) \pm 2\sqrt{c}. \end{aligned}$$

Предложение доказано. □

Из доказательства предложения 29 ясен алгоритм построения квазипериодического, но не периодического элемента. Воспользуемся им для построения примера.

Пример 8. Пусть $c = 4$. Тогда $z = -5 \pm 4$. Пусть $z = -1$. Зафиксируем $\operatorname{lc}(a_0) = 1$, тогда $\operatorname{lc}(a_1) = -1/4$.

Пусть $s_0 = 2$, а $s_1 = 1$. Тогда $a_0 = d_0 + d_1x + x^2$, а $a_1 = e_0 - 1/4x$.

И для $d_0 = 1$, $d_1 = 0$, $e_0 = 1$ дискриминант будет следующего вида:

$$D = 32x^5 + 8x^4 + 24x^3 + 33x^2 - 8x + 16.$$

А квазипериодический элемент α следующего:

$$\begin{aligned} \alpha &= \frac{-3x^3 + (x^2 + 1)(x - 4) - \sqrt{D}}{2(x - 4)x^2} \\ &= \overline{[x^{-2} + 1, x^{-1} - 1/4]^4}. \end{aligned}$$

Для обобщения предложения 29 нам потребуются элементы $P_n, Q_n \in k(x)$ из §1.1.2.

Теорема 19. Квазипериодический, но не периодический, элемент $\alpha = \overline{[A_0, A_i, \dots, A_{2m-1}]^c}$, $c \in k \setminus \{0\}$, $A_i \in k[h^{-1}]$, лежит в $k(x)(\sqrt{f})$ для некоторого многочлена f нечётной степени только, если $fc(Q_{n-2}) + cfc(P_{n-1}) = \pm 2\sqrt{c}$, где $n = 2m$.

Доказательство. Имеем $c\alpha = \alpha_{2m}$. Откуда

$$\alpha = \frac{c\alpha P_{n-1} + P_{n-2}}{c\alpha Q_{n-1} + Q_{n-2}}. \quad (2.5)$$

Откуда

$$cQ_{n-1}\alpha^2 + (Q_{n-2} - cP_{n-1})\alpha - P_{n-2} = 0.$$

Воспользуемся (1.6) и рассмотрим $\mathbf{v}_h(P_n) = \mathbf{v}_h(Q_n) + \mathbf{v}_h(A_0) = \sum_{i=0}^n \mathbf{v}_h(A_i) = \sum_{i=0}^n t_i$, где $t_i = \mathbf{v}_h(A_i)$. Обозначим $s_n = \sum_{i=0}^n t_i$.

Рассмотрим значения нормирований у коэффициентов при степени α :

$$\mathbf{v}_h(cQ_{n-1}) = s_{n-1} - t_0,$$

$$\mathbf{v}_h(Q_{n-2} - cP_{n-1}) = \mathbf{v}_h(P_{n-1}) = s_{n-1},$$

$$\mathbf{v}_h(P_{n-2}) = s_{n-2}.$$

Наименьшее значение нормирования получается равно s_{n-1} . Перепишем (2.5) так, чтобы получилось выражение от α с коэффициентами из $k[h]$:

$$cQ_{n-1}h^{-s_{n-1}}\alpha^2 + (Q_{n-2} - cP_{n-1})h^{-s_{n-1}}\alpha - P_{n-2}h^{-s_{n-1}} = 0.$$

Откуда дискриминант $D = h^{2s_{n-1}}D'$, где

$$\begin{aligned} D' &= (Q_{n-2} - cP_{n-1})^2 + 4cQ_{n-1}P_{n-2} = \\ &= Q_{n-2}^2 - 2cQ_{n-2}P_{n-1} + \\ &+ c^2P_{n-1}^2 + 4cQ_{n-1}P_{n-2}. \end{aligned}$$

Воспользуемся соотношением (1.3) и тем, что $n = 2m$:

$$D' = Q_{n-2}^2 + c^2P_{n-1}^2 + 2cQ_{n-2}P_{n-1} - 4c.$$

Перепишем условие:

$$D' = (Q_{n-2} + cP_{n-1})^2 - 4c.$$

Откуда получаем условия зануления свободного коэффициента и, соответственно, утверждение теоремы. $\square$

Замечание 8. Условие $fc(Q_{n-2}) + cfc(P_{n-1})$ можно переписать следующим образом:

$$\begin{aligned} fc(Q_{n-2}) - 1 + c(fc(P_{n-1}) - 1) = \\ = (c + 1) \pm 2\sqrt{c}, \end{aligned} \tag{2.6}$$

что для $n = 2$ совпадает с условием предложения 29.

Следствие 18. Пусть квазипериодический элемент лежит в гиперэллиптическом поле, порождённом многочленом нечётной степени. Тогда коэффициент квазипериодичности этого элемента является полным квадратом в поле k .

Для случая $n = 2$ мы видели, что достаточно проверять только выражение, зависящее от произведения $fc(A_0)fc(A_1)$, однако в более общем случае, ситуация несколько усложняется.

Пример 9. Построим P_1, P_2, P_3 и Q_1, Q_2, Q_3 :

$$\begin{aligned} P_0 &= A_0, \quad Q_0 = 1, \\ P_1 &= A_1 A_0 + 1, \quad Q_1 = A_1, \\ P_2 &= A_2 A_1 A_0 + A_2 + A_0, \\ Q_2 &= A_2 A_1 + 1, \\ P_3 &= A_3 A_2 A_1 A_0 + A_3 A_2 + A_3 A_0 + A_1 A_0 + 1, \\ Q_3 &= A_3 A_2 A_1 + A_3 + A_1 \end{aligned}$$

Выражение (2.6) приобретает следующий вид:

$$\begin{aligned} &cfc(A_0 A_1 A_2 A_3 + A_0 A_1 + A_0 A_3 + A_2 A_3) + \\ &+ fc(A_1 A_2) = -(c + 1) \pm 2\sqrt{c}, \end{aligned}$$

Для того, чтобы дискриминант имел нечётную степень, мы должны требовать равенство 0 уже более сложного выражения, чем в случае $n = 2$.

Пусть $c = 4$. Тогда $z = -5 \pm 4$. Пусть $z = -1$. Зафиксируем $fc(A_0) = fc(A_1) = fc(A_3) = 1$, тогда $fc(A_2) = -1$.

Пусть $s_i = 1$, для $i = 0, \dots, 3$. Выбор коэффициентов при x^{-1} свободный, пусть это будут 1. Тогда $A_2 = -1 + x^{-1}$, а $A_i = 1 + x$, $i = 0, 1, 3$.

Тогда дискриминант имеет следующий вид:

$$\begin{aligned} D &= 64x^7 + 168x^6 + 272x^5 + 329x^4 + \\ &+ 272x^3 + 168x^2 + 64x + 16, \end{aligned}$$

а квазипериодический элемент α имеет вид:

$$\begin{aligned} \alpha &= \frac{4x^4 + 8x^3 + 11x^2 + 8x + 4 - \sqrt{D}}{8x^4 + 8x^3 + 8x^2 + 8x} \\ &= \left[\frac{1}{x} + 1, \frac{1}{x} + 1, \frac{1}{x} - 1, \frac{1}{x} + 1 \right]^4. \end{aligned}$$

2.3 Теорема Платонова и Беньш-Кривеца о построении фундаментальной S -единицы

В параграфе §1.2.4 мы видели, что наличие S -единиц в поле $L = k(x)(\sqrt{f})$ для многочлена f степени $2g + 1$ является критерием существования периодических элементов этом поле. Предложение 26 и следствие 13 показывают, что существование и вид нетривиальных S -единиц непосредственно связаны с периодичностью ключевого элемента. Более того, с учётом следствия 9 вид фундаментальной S -единицы позволяет сделать выводы о квазипериодичности произвольного элемента поля L . В связи с этим возникает естественный вопрос о вычислении фундаментальной S -единицы для заданного f и соответствующего поля L . Для конечного поля констант ответ на этот вопрос был дан в [13].

Сформулируем без доказательства аналог теоремы 5.8 из работы [13] для произвольного поля k характеристики отличной от 2, что позволяет использовать этот результат в том числе и для поля $\mathbb{Q}$ в качестве поля констант. В настоящем параграфе будем для удобства обозначений в последующих параграфах использовать α и β вместо μ_1 и μ_2 в уравнении (1.23).

Теорема 20 ([13]). Пусть $\deg h = 1$ и $\deg f = 2g + 1$. Предположим, что для некоторого минимального натурального m уравнение

$$\alpha^2 - \beta^2 f = ch^m \quad (2.7)$$

имеет решение в многочленах $\alpha, \beta \in k[x]$, $\beta \neq 0$ для некоторой константы $c \in k$. Справедливы следующие утверждения

1. Если $m = 2t + 1$, то $\frac{\alpha}{\beta}$ является наилучшим приближением к $\sqrt{f}$. Таким образом, $\frac{\alpha}{\beta} = \frac{P_n}{Q_n}$ для некоторой подходящей дроби $\frac{P_n}{Q_n}$ к $\sqrt{f}$.
2. Если $m = 2t$, то найдется делитель d многочлена f , $\deg d < \frac{1}{2} \deg f$, такой что уравнение

$$\frac{f}{d} \beta_1^2 - d \alpha_1^2 = bh^t, \quad (2.8)$$

где $b \in k$, имеем решение в многочленах $\alpha_1, \beta_1 \in k[x]$. При этом $\frac{\alpha_1}{\beta_1}$ является наилучшим приближением к $\frac{\sqrt{f}}{d}$ и, следовательно, $\frac{\alpha_1}{\beta_1} = \frac{P_n}{Q_n}$ для некоторой подходящей дроби $\frac{P_n}{Q_n}$ к $\frac{\sqrt{f}}{d}$.

Наоборот, если $\alpha_1, \beta_1 \in k[x]$ — решение (2.8), то $\frac{\alpha_1}{\beta_1}$ является наилучшим приближением к $\frac{\sqrt{f}}{d}$, $\frac{\alpha_1}{\beta_1} = \frac{P_n}{Q_n}$ для некоторой подходящей дроби $\frac{P_n}{Q_n}$ к $\frac{\sqrt{f}}{d}$.

и многочлены α и β , определяемые по формулам

$$\alpha = \frac{1}{2} \left(d\alpha_1^2 + \frac{f}{d}\beta_1^2 \right), \quad \beta = \alpha_1\beta_1, \quad (2.9)$$

являются решением уравнения (2.7) для $m = 2t$.

Доказательство. По аналогии с доказательством [13, Теорема 5.8]. □

Замечание 9. Отметим, что теорема 20 становится неверной в случае $\deg h > 1$. Контрпример приведён в [13] (примеры 3.7 и 5.7).

Пример 10. Теорема 20 также становится неверной в случае, когда $\deg h = 1$ и $\deg f = 2g + 2$.

Пусть $k = \mathbb{Q}$, $f = 8x^4 + 8x^3 + 1$, а $h = x$. Фундаментальная S_h -единица обладает степенью 4 и имеет следующим вид:

$$u = \frac{1 - 2x + 2x^2 + 4x^3 - 4x^4 + (1 - 2x + 2x^2) \sqrt{f}}{x^4}$$

При этом многочлен f неприводим над $\mathbb{Q}$ и, следовательно, второй пункт теоремы 20 не выполнен. Покажем, что и первый пункт не может быть выполнен не только для f , указанного выше, но и для более широкого класса многочленов.

Действительно, пусть $\deg f = 2g + 2$, и ν_∞ имеет одно продолжение на L . Запишем (2.7) в виде

$$(\alpha - \beta\sqrt{f})(\alpha + \beta\sqrt{f}) = ch^m.$$

В силу предложения 13 мы можем считать, что $\nu_h^+(\alpha + \beta\sqrt{f}) = 0$, $\nu_h^+(\alpha - \beta\sqrt{f}) = m$. Разложим α и β по степеням h :

$$\alpha = a_0 + a_1h + \cdots + a_rh^r, \quad \beta = b_0 + b_1h + \cdots + b_sh^s,$$

где $a_i, b_i \in k$, $a_r \neq 0$, $b_s \neq 0$.

В силу предложения 12 число m является чётным. Сравнение степеней многочленов в левой и правой части (2.7) и показывает, что $r \leq t$, $s \leq t$, где $t = m/2$. Пусть $l = \max\{r, s\}$. Будем рассматривать многочлены f , для которых решение соответствующего уравнения обладает свойством $l = t$. Многочлен f из первой части настоящего примера обладает этим свойством. Рассмотрим элемент $\bar{\alpha} - \bar{\beta}\sqrt{f}$, где

$$\bar{\alpha} = \frac{\alpha}{h^l} = a_0h^{-l} + \cdots + a_rh^{r-l}, \quad \bar{\beta} = \frac{\beta}{h^l} = b_0h^{-l} + \cdots + b_sh^{s-l}.$$

Так как $\bar{\alpha}/\bar{\beta}$ имеет вид (1.8) и

$$\mathbf{v}_h^+(\bar{\alpha} - \bar{\beta}\sqrt{f}) = 2t - l = -\mathbf{v}_h^+(\bar{\beta}) = t,$$

то по предложению 15 дробь $\bar{\alpha}/\bar{\beta} = \frac{\alpha}{\beta}$ не равна никакой подходящей дроби к $\sqrt{f}$.

Теорема 20 позволяет с использованием инструментария непрерывных дробей и предложения 25 строить фундаментальную S и S_h -единицу, а, таким образом, с помощью предложения 26, и фундаментальное решение в многочленах от h^{-1} уравнения (1.25) и фундаментальное решение (то есть минимальное, например, по степени $\deg \mu_1$) в многочленах от x уравнения (1.23). Действительно, в работе [13] после теоремы 5.8, обобщением которой является теорема 20, было отмечено, что она дает алгоритм для вычисления фундаментальной S -единицы в случае $\deg h = 1$ и $\deg f = 2g + 1$. А именно, пусть $d_1, \dots, d_r$ — все делители многочлена f степени, не превосходящей $1/2 \deg f$. Будем последовательно вычислять подходящие дроби к $\sqrt{f}$, $\sqrt{f}/d_1, \dots, \sqrt{f}/d_r$ и для каждой подходящей дроби P_n/Q_n проверять, выполняется ли равенство (2.8):

$$\frac{f}{d_i} \beta_1^2 - d_i \alpha_1^2 = bh^t, \quad \frac{P_n}{Q_n} = \frac{\alpha_1}{\beta_1}.$$

Алгоритм заканчивает работу, как только мы найдем подходящую дробь P_n/Q_n , удовлетворяющую (2.8). Тогда по формулам (2.9) находим решение α, β нормального уравнения (2.7). В этом случае либо $\alpha + \beta\sqrt{f}$, либо $\alpha - \beta\sqrt{f}$ будет фундаментальной S -единицей.

В [32] было показано, что в случае существования фундаментальной S -единицы существует единственный делитель $d \in \{1, d_1, \dots, d_r\}$, для которого в приведенном алгоритме найдется соответствующая подходящая дробь P_n/Q_n , дающая решение (2.8).

Сформулированный выше алгоритм является вычислительно ёмким, в параграфе §3.1.1 мы обсудим его более подробно, а в параграфах §3.1.2 и §3.1.3 будут предложены алгоритмы, базирующиеся на указанном выше, но более оптимальные с точки зрения вычислительной ёмкости.

2.4 Разложение в непрерывную дробь элемента $\sqrt{f}/h^{g+1}$

В параграфе §1.11 отмечалось, что элемент $\sqrt{f}/h^{g+1}$ является ключевым с точки зрения изучения квазипериодичности элементов поля $L = k(x)(\sqrt{f})$. В частности, следствие 9 позволяет сделать вывод о периодичности произвольного элемента исследуя исключительно решения уравнения (1.20) для D , связанного с $\sqrt{f}/h^{g+1}$. Кроме того, если поле L содержит квазипериодические элементы, то элемент $\sqrt{f}/h^{g+1}$ квазипериодичен. В силу сказанного, исследование периодичности ключевого элемента $\sqrt{f}/h^{g+1}$ представляет отдельный интерес.

В случае $\deg f = 2g + 2$ описание разложения в непрерывную дробь элемента $\alpha = \sqrt{f}/h^{g+1}$ может быть получено путем применения стандартного бирационального преобразования переводящего v_h^+ в v_∞^+ , а v_h^- в v_∞^- соответствующей кривой, и применения разработанной теории для случая S , состоящего из двух бесконечных нормирований.

Поэтому в рамках настоящего параграфа мы сосредоточимся на случае $\deg f = 2g + 1$ и S -единицах, отдельно отмечая утверждения, которые верны и в четном случае. Отметим также, что для этого случая в силу следствия 14 рассмотрение S -единиц даёт потенциально больше информации о кручении в якобиане соответствующей гиперэллиптической кривой, нежели рассмотрение S_h -единиц.

Как мы видели в §1.1.2 с каждым шагом разложения квадратичной иррациональности $\alpha = \frac{\sqrt{f}}{h^{g+1}}$ в непрерывную дробь связаны два многочлена $L_j, M_j \in k[x]$, степень которых не превосходит $2g + 2$. Для данного α выражение (1.12) выглядит следующим образом:

$$L_j = (-1)^{j+1}(h^{2g+2}P_j^2 - fQ_j^2).$$

Замечание 10. Пусть $\deg f = 2g + 1$, и для поля $L = k(x)(\sqrt{f})$ группа S -единиц нетривиальна. В предложении 26 было показано, что всякому решению уравнения $\mu_1^2 - \mu_2^2 f = bh^m$ для некоторого целого $m > 0$, $\mu_1, \mu_2 \neq 0 \in k[x]$, $b \in k \setminus \{0\}$, соответствует S -единица. Легко видеть, что ее степень m , и что указанному решению и S -единице соответствует единственная (в силу строгого убывания $v_h(P_n)$ с ростом n) подходящая дробь $\frac{P_n}{Q_n} = \frac{\mu_1}{\mu_2 h^{g+1}}$ к элементу $\sqrt{f}/h^{g+1}$.

Наоборот, если для какой-то подходящей дроби P_n, Q_n выполнено $L_n = bh^r$, или

$$(-1)^{n+1}(h^{2g+2}P_n^2 - fQ_n^2) = bh^r, \quad (2.10)$$

где $b \in k \setminus \{0\}$, $r \in \mathbb{N}$, то ей соответствует S -единица. Чтобы построить ее норменное уравнение достаточно в (2.10) домножить обе части на общий знаменатель, который будет степенью h .

Кроме того, в силу предложения 26 существует соответствие между уравнениями вида (1.25) и S -единицами четных степеней.

Далее по тексту соответствие между S -единицами, подходящими дробями, норменными уравнениями для S -единиц и уравнениями вида (1.25) будет упоминаться только в этом смысле.

В классическом случае поля $k((1/x))$ элемент $\sqrt{f}$, $\deg f = 2g + 2$, квазипериодичен с квазипериодом длины N тогда и только тогда, когда фундаментальная единица может быть построена с помощью подходящих дробей на шаге разложения с номером $N - 1$ (подробнее, см. [21]). Для случая $\deg f = 2g + 1$ и $k((h))$ иногда, скажем как в примере 4, ситуация не отличается от классического случая, и фундаментальная S -единица соответствует квазипериоду в смысле, указанном выше. Но так происходит не всегда. Достаточно рассмотреть f из примера 2, или, как будет показано далее, любой пример, в котором степень соответствующей фундаментальной S -единицы является нечетным числом.

Пример 11. Пусть g, k, h, f как в примере 2 и $\deg f = 2g + 1$.

Разложение $\frac{\sqrt{f}}{x^{g+1}}$ является периодическим с длиной периода, совпадающей с длиной квазипериода и равной 2. Разложение выглядит следующим образом:

$$\left[x^{-g-1}, \overline{\frac{2}{a}x^{-g}, 2x^{-g-1}} \right].$$

Фундаментальная S -единица существует и соответствует 0-ой подходящей дроби P_0/Q_0 . А именно

$$L_0 = x^{2g+2}P_0^2 - Q_0^2f = -ax^{2g+1}, \text{ где } P_0 = x^{-g-1}, Q_0 = 1.$$

Откуда легко построить решение норменного уравнения и, соответственно, S -единицу. Отметим, что фундаментальная S -единица имеет нечетную степень и ее квадрат, но не она сама, соответствует фундаментальному решению из примера 2.

Напомним, что если n — такое минимальное неотрицательное целое число, при котором $\deg(L_n) = \nu_h(L_n)$ или, что тоже самое, $L_n = bh^r$, то с помощью подходящей дроби P_n/Q_n мы можем построить фундаментальную S -единицу. Алгоритм поиска и построения фундаментальной S -единицы базируется на последовательном вычислении L_n и сравнении его значения с bh^r . Согласно лемме 4 и следствию 13 в случае существования нетривиальной S -единицы обязательно найдется номер n , для которого будет выполнено $r = 2g + 2$, а если дополнительно известно, что фундаментальная S -единица нечетной степени, то еще и номер n , для которого $r = 2g + 1$. Оказывается, r может принимать только эти два значения: $2g + 1$ и $2g + 2$. Причем, это значение определяет четность степени S -единицы.

Предложение 30. Пусть $\deg f = 2g + 1$, и $n \geq 0$ такое число, при котором $L_n = bh^r$, $b \in k \setminus \{0\}$.

Тогда $r = 2g + 1$ или $r = 2g + 2$, причем $r = 2g + 1$ в том и только том случае, когда степень S -единицы поля $k(x)(\sqrt{f})$ является нечетным числом m , и $r = 2g + 2$ в противном случае.

В частности, указанное выполняется для фундаментальной S -единицы и минимального такого n .

Доказательство. Пусть

$$h^{2g+2}P_n^2 - Q_n^2f = ch^r, \quad c = (-1)^{n+1}b. \quad (2.11)$$

Положим $-t = \nu_h(P_n) = \nu_h(Q_n) + \nu_h(A_0) = \nu_h(Q_n) - (g + 1)$. Тогда $P_n = p_n/h^t$, а $Q_n = q_n/h^{t-(g+1)}$, где $p_n, q_n \in k[x]$. Откуда $p_n^2 - q_n^2f = ch^{r+2t-2(g+1)}$.

Согласно замечанию 10 в этом случае может быть построена фундаментальная S -единица, и ее степень будет равна $2t + r - 2(g + 1)$. Таким образом, четность степени S -единицы определяется четностью r .

Напомним, что в силу (1.15), верна оценка $r = \deg L_{n-1} \leq 2g + 2$. Предположим, что $r < 2g + 1$, и перепишем (2.11) в виде многочленов от h^{-1} (напомним, что $P_n, Q_n \in k[h^{-1}]$):

$$P_n^2 - Q_n^2Fh^{-1} = ch^{r-2(g+1)}, \quad (2.12)$$

где $F = f/h^{2g+1} \in k[h^{-1}]$.

Тогда в правой части уравнения (2.12) показатель степени h не больше чем -2 : $P_n^2 - Q_n^2Fh^{-1} = ch^{-2}h^{r'}$, $r' \leq 0$. Откуда следует, что в кольце многочленов от h^{-1} элемент h^{-1} делит P_n^2 , т.е. $P_n^2 = h^{-1}P'$, где $P' \in k[h^{-1}]$, а следовательно,

$h^{-2}|P_n^2$, откуда $h^{-1}|Q_n^2$, что невозможно, т.к. в кольце многочленов от h^{-1} в силу $Q_n P_{n-1} - P_n Q_{n-1} = (-1)^n$ элементы P_n и Q_n взаимно просты. $\square$

Отметим, что для случая четной степени f указанное предложение, вообще говоря не верно.

Пример 12. Возьмем $g = 2, k = \mathbb{Q}, h = x$ и $f = (x-1)(x+3)(x^4+2x^3-x^2+2x-3)$.

$$\begin{aligned} P_2 &= -1 - \frac{3}{x} - \frac{5}{x^2} + \frac{1}{x^3} - \frac{3}{x^4} + \frac{9}{x^5}, \\ Q_2 &= 1 + \frac{1}{x} + \frac{3}{x^2}, \\ L_2 &= (-1)^3(h^{2g+2}P^2 - Q^2f) = -4x^4. \end{aligned}$$

При этом

$$\begin{aligned} L_0 &= 4x^5 - 4x^4, \\ L_1 &= 2x^6 + 2x^5 - 3x^4. \end{aligned}$$

Откуда видим, что минимальное $n \geq 0$, для которого верно $L_n = bh^r$, это $n = 2$. При этом $\deg L_2 = 4 < 2g + 1 = 5$.

По лемме 4 получаем, что для периодического $\sqrt{f}/h^{g+1}$ обязательно встретится номер n такой, что $L_n = bh^r$, где $r = 2g + 2$. Докажем, что такой и только такой L_n соответствует квазипериоду в случае произвольной четности степени f . А в случае $\deg f = 2g + 1$, ему также соответствует S -единица четной степени.

Предложение 31. Пусть f — многочлен степени $2g + 1$ или $2g + 2$. Разложение $\alpha = \sqrt{f}/h^{g+1}$ в непрерывную дробь имеет квазипериод длины N тогда и только тогда, когда $N \geq 1$ — минимальное число такое, что $L_{N-1} = bh^{2g+2}$, $b \in k \setminus \{0\}$.

Доказательство. Пусть для некоторого $N \geq 1$ выполнено $L_{N-1} = bh^{2g+2}$. Воспользуемся формулой (1.11):

$$\alpha_N = \frac{M_{N-1} + h^{2g+2}\alpha}{L_{N-1}}, \quad (2.13)$$

где $M_{N-1} \in k[x]$, $\deg M_{N-1} \leq 2g + 2$. Отсюда $b\alpha_N = \frac{M_{N-1}}{h^{2g+2}} + \alpha$. В силу того, что степень M_{N-1} не превосходит $2g + 2$ и $\frac{M_{N-1}}{h^{2g+2}} \in k[h^{-1}]$, получаем равенство с точностью до константы “дробных” частей α и α_N . И выполнено

$$\alpha_{N+1} = \frac{1}{\alpha_N - [\alpha_N]} = b \frac{1}{\alpha - [\alpha]} = b\alpha_1.$$

Обратно, пусть разложение α квазипериодично с длиной квазипериода N , тогда в силу следствия 12 оно периодично с периодом $w \geq N$ и имеет вид (1.22), где $C_0 = \frac{1}{2}C_w$. Тогда $c\alpha_i = \alpha_{i+N}$ для некоторых i и c , откуда $c'\alpha_w = \alpha_{w+N} = \alpha_N$ для некоторого c' . В силу (1.22) получаем $C_N = c'C_w = 2c'C_0$.

Из соотношения (1.14) получаем $\nu_h(L_{j-1}) = g + 1 - \nu_h(C_j)$, откуда $\deg(L_{N-1}) = \nu_h(L_{N-1}) = 2g + 2$. $\square$

В следующем предложении запись α'_n обозначает сопряженный элемент к α_n , который вообще говоря не должен быть равен n -ому полному частному к α' . Докажем следующие стандартные соотношения.

Предложение 32. Пусть $[B_0, B_1, B_2, \dots]$, разложение $\alpha = \sqrt{f}/h^{g+1}$, где $\deg f = 2g + 1$ или $\deg f = 2g + 2$, в непрерывную дробь, квазипериодично с квазипериодом N , тогда $2c^{-1}B_0 = B_N$, для некоторого $c \in k \setminus \{0\}$. Кроме того, в случае, когда $N > 1$, для $j = 1, \dots, N - 1$ выполнены соотношения:

$$\begin{aligned} -\frac{1}{\alpha'_{N+1-j}} &= c^{(-1)^{j+1}}\alpha_j, \quad -\frac{1}{\alpha'_{N+1}} = c^{-1}(\alpha + B_0), \\ B_j &= c^{(-1)^j}B_{N-j}, \quad M_{j-1} = M_{N-j}, \quad L_{j-2} = c^{(-1)^j}L_{N-j}. \end{aligned}$$

Доказательство. Пусть разложение $\alpha = \sqrt{f}/h^{g+1}$ в непрерывную дробь квазипериодично с квазипериодом N . Если $N = 1$, то предложение следует из следствия 12. Пусть теперь $N > 1$. Тогда по следствию 12 предпериод разложения α имеет длину 1. В этом случае $\alpha_{N+1} = c\alpha_1$. Т.е.

$$\alpha = [B_0, \overline{B_1, B_2, \dots, B_N^c}].$$

Первое полное частное $\alpha_1 = \frac{1}{\alpha - B_0}$ будет чисто квазипериодично и записано следующим образом

$$\alpha_1 = [\overline{B_1, B_2, \dots, B_N^c}].$$

Из конструкции непрерывной дроби получаем $\alpha_i = B_{i+1} + \frac{1}{\alpha'_{i+1}}$ для $i = 0, \dots, N - 1$. Следовательно $\alpha'_i = B_{i+1} + \frac{1}{\alpha'_{i+1}}$. Обозначим $\beta_j = -\frac{1}{\alpha'_{N+1-j}}$ для $j = 0, \dots, N$, тогда

$$\beta_j = B_{N-j} + \frac{1}{\beta_{j+1}},$$

для $j = 0, \dots, N$. Но $\alpha_{N+1} = c\alpha_1$, откуда $\alpha'_{N+1} = c\alpha'_1$ и $\beta_N = c^{-1}\beta_0$, откуда:

$$\beta = -\frac{1}{c\alpha'_1} = -\frac{1}{\alpha'_{N+1}} = [\overline{B_N, B_{N-1}, \dots, B_1}]^c.$$

С учетом того, что $\alpha' = -\alpha$ и $\alpha_1 = -\frac{1}{(\alpha+B_0)'}$ перепишем первое равенство следующим образом: $\beta = c^{-1}(\alpha+B_0)$. Т.к. по построению $\beta_j = -\frac{1}{\alpha'_{N+1-j}}$ получаем $-\frac{1}{\alpha'_{N+1-j}} = \beta_j = (c^{-1}(\alpha+B_0))_j = c^{(-1)^{j+1}}\alpha_j$ для $j = 1, \dots, N$.

Запишем уравнение (2.13) для α_{j+1} и для α_{N-j} :

$$c^{(-1)^j} \frac{M_j + h^{2g+2}\alpha}{L_j} = c^{(-1)^j} \alpha_{j+1} = -\frac{1}{\alpha'_{N-j}} = \frac{L_{N-j-1}}{h^{2g+2}\alpha - M_{N-j-1}}.$$

В результате преобразований получаем следующее:

$$(M_j - M_{N-j-1})h^{2g+2}\alpha + ((h^{2g+2}\alpha)^2 - M_j M_{N-j-1}) = c^{(-1)^{j+1}} L_j L_{N-j-1}.$$

Откуда с учетом формулы (1.17): $L_j L_{j-1} + M_j^2 = (h^{2g+2}\alpha)^2$, получаем

$$\begin{aligned} M_j &= M_{N-j-1}, \\ L_{j-1} &= c^{(-1)^{j+1}} L_{N-j-1}, \end{aligned}$$

для $j = 0, \dots, N-1$.

В силу квазипериодичности α и следствия 12 заключаем, что $B_N = 2c^{-1}B_0$. В следствие равенства $\beta_1 = c\alpha_1$ получаем $B_i = c^{(-1)^j} B_{N-1}$, для $j = 1, \dots, N$. $\square$

С помощью следствия 13 и предложений 30, 31 и 32 докажем следующий результат.

Теорема 21. Пусть $\deg f = 2g+1$, и $\alpha = \sqrt{f}/h^{g+1}$. Фундаментальная S -единица поля $k(x)(\sqrt{f})$ существует тогда и только тогда, когда разложение α в непрерывную дробь периодически. Пусть фундаментальная S -единица существует и ее степень равна m , и пусть $n \geq 1$ — минимальное такое число, при котором $\deg L_{n-1} = \nu_h(L_{n-1})$. Возможны два случая:

1. m является четным числом, тогда $\deg L_{n-1} = 2g+2$. При этом длина квазипериода равна n , а длина периода в этом случае равна либо n либо $2n$,

2. m является нечетным числом, тогда $\deg L_{n-1} = 2g + 1$. При этом длина периода совпадает с длиной квазипериода и равна $2n$.

Доказательство. В случае четного m из предложения 31 немедленно следует, что n — квазипериод. Равенство длины периода n или $2n$ для нечетного n следует из вида квазипериодичной непрерывной дроби, а для четного n вытекает из результатов следствия 13.

Докажем утверждение теоремы в случае нечетного m . Пусть u — фундаментальная S -единица соответствующая L_{n-1} в понимании замечания 10. Рассмотрим u^2 — квадрат фундаментальной S -единицы, степень полученной S -единицы равна $2m$. С точностью до константы u^2 совпадает с S -единицей соответствующей L_{N-1} для некоторого N . По предложению 31 число $N > n$ является длиной квазипериода, т.к. не существует S -единицы четной степени меньшей $2m$.

В случае $N = 2$ утверждение теоремы очевидно. Пусть $N \geq 3$. По предложению 32 выполнено $L_{n-1} = c^{(-1)^{n+1}} L_{N-n-1}$. Откуда $\deg L_{N-n-1} = \nu_h(L_{N-n-1}) = 2g + 1$. В силу фундаментальности u и того, что не существует S -единицы нечетной степени большей m и не превосходящей $2m$, получаем $2n = N$ и $c = 1$. $\square$

Из теоремы следует, что для $\deg f = 2g + 1$ необходимым условием существования фундаментальной S -единицы нечетной степени является совпадение длины квазипериода и длины периода. Это условие не является достаточным.

Пример 13. Пусть g, k, h, f как в примере 4.

Разложение $\sqrt{f}/x^3$ в непрерывную дробь имеет период длины 2, совпадающий с квазипериодом, и выглядит следующим образом:

$$[14/x + 9/x^2 + 2/x^3 + 5, \overline{-4/5/x - 2/5, 28/x + 18/x^2 + 4/x^3 + 10}],$$

в то время, как степень фундаментальной S -единицы поля $\mathbb{Q}(x)(\sqrt{f})$ равна 8.

Замечание 11. Из доказательства предложения 30 следует, что если $\nu_h(L_{n-1}) = r$, то можно построить S -единицу степени $m = 2t + r - 2(g + 1)$, где $t = -\nu_h(P_{n-1}) = -\sum_{i=0}^{n-1} \nu_h(A_i)$. Формулу можно специфицировать с учётом (1.6) и того, что $\nu_h(A_0) = -g - 1$, следующим образом: $t = -\nu_h(Q_{n-1}) = g + 1 - \sum_{i=1}^{n-1} \nu_h(A_i)$.

По построению $v_h(A_i) \leq -1$, для $i > 0$, а $v_h(A_0) = -(g+1)$. Откуда с учетом замечания 11 получаем минимальную оценку на m : $m \geq 2(n-1) + r$. В зависимости от четности m по предложению 30 значение r может равняться или $2g+1$ или $2g+2$.

Сохраним обозначения теоремы 21. Разложим α в степенной ряд $\alpha = \sum_{i \geq -(g+1)} a_i h^i$, и обозначим через $\delta = -v_h(A_1)$ или, количество подряд идущих нулевых элементов $a_1 = \dots = a_\delta = 0, a_{\delta+1} \neq 0$. В работе [27] получена оценка: $m \leq (g+2+\delta)n$. Из указанных выше оценок и теоремы 21 следуют оценки на длину квазипериода.

Следствие 19. Пусть $\deg f = 2g+1$, и пусть $k(x)(\sqrt{f})$ обладает фундаментальной S -единицей степени m . И пусть N — длина квазипериода разложения α в непрерывную дробь. Тогда

$$N + 2g - 1 \leq m \leq (g + 2 + \delta)N.$$

Более того, если m — нечетное число, то выполнено соотношение

$$N + 2g - 1 \leq m \leq (g + 2 + \delta)N/2,$$

иначе выполнено

$$2(N + g) \leq m \leq (g + 2 + \delta)N.$$

Приведем примеры, на которых указанные оценки становятся точными. Более того, в каждом из последующих примеров реализована сравнительно редкая ситуация, в которой верхняя и нижняя граница соответствующей оценки будут равны между собой и достигнуты одновременно.

Пример 14. Пусть g, k, h, f как в примере 2 и $\deg f = 2g+1$.

Рассмотрим разложение $\alpha = \sqrt{f}/x^{g+1}$ в ряд Лорана:

$$\alpha = \sqrt{f}/x^{g+1} = x^{-(g+1)} + \frac{a}{2}x^{-g} + \dots,$$

откуда $\delta = g-1$. Разложение $\alpha = [x^{-(g+1)}, \frac{2}{a}x^{-g}, 2x^{-(g+1)}]$ в непрерывную дробь обладает длиной квазипериода $N = 2$. Получаем $N + 2g - 1 = (g + 2 + \delta)N/2 = 2g + 1$. Степень фундаментальной S -единицы равна $2g+1$.

В предыдущем примере степень S -единицы была нечетной. Элемент, для которого нижняя и верхняя границы для четного m становятся точными, дает нам пример 4.

Пример 15. Пусть g, k, h, f как в примерах 4, 13.

Рассмотрим разложение $\alpha = \sqrt{f}/x^3$ в ряд Лорана:

$$\alpha = 2x^{-3} + 9x^{-2} + 14x^{-1} + 5 - \frac{5}{4}x + \dots$$

Откуда заключаем, что $\delta = 0$. Напомним, что длина квазипериода равна 2, а степень фундаментальной S -единицы равна 8. В результате получаем $2(N + g) = 8 = m = (g + 2 + \delta)N$.

Полезно будет привести еще один пример для четного m с $\delta \neq 0$.

Пример 16. Возьмем $g = 2, k = \mathbb{Q}, h = x$ и

$$f = 220x^5 + 224x^4 - 1054x^3 + 1072x^2 - 468x + 81.$$

Разложение элемента $\alpha = \sqrt{f}/x^3$ в ряд выглядит следующим образом:

$$\alpha = 9x^{-3} - 26x^{-2} + 22x^{-1} + 5 - 25/18x^3 + \dots$$

Откуда заключаем, что $\delta = 2$. Степень фундаментальной S -единицы равна 6, длина периода равна 2, а длина квазипериода N равна 1. Разложение $\alpha = \sqrt{f}/x^3$ выглядит следующим образом:

$$\alpha = [5 + 22x^{-1} - 26x^{-2} + 9x^{-3}, \\ -2/5 - 44/25x^{-1} + 52/25x^{-2} - 18/25x^{-3}, 10 + 44x^{-1} - 52x^{-2} + 18x^{-3}].$$

Получаем $2(N + g) = 6 = m = (g + 2 + \delta)N$.

Глава 3. Построение S -единиц больших степеней

Как мы видели в параграфе §1.2.4 вид фундаментальной S -единицы в общем случае позволяет получить информацию о кручении в якобиане соответствующей гиперэллиптической кривой. Кроме того, в параграфе §2.3 обсуждался алгоритм вычисления S -единицы, что в свою очередь позволяет построить решения уравнения (1.20) и делать выводы о квазипериодичности элементов гиперэллиптического поля в случае $\deg h = 1$. В этой главе мы обсудим различные алгоритмы построения S -единицы, а также их эффективность и способы их оптимизации. С помощью упомянутых алгоритмов будут построены S -единицы больших степеней для гиперэллиптических полей рода 2 с полем рациональных чисел в качестве поля констант. В текущем параграфе мы сосредоточимся на случае нечётной степени многочлена f , и будем полагать $\deg f = 2g + 1$ на протяжении всего параграфа.

3.1 Случай линейного нормирования

В случае линейного нормирования становится возможным применения метода непрерывных дробей. Указанный метод в сравнении с другими методами обладает высокой эффективностью, и в силу этого требует отдельного рассмотрения. Ниже будет показано, что существование большинства известных к настоящему моменту порядков кручения в якобианах гиперэллиптических кривых рода 2 с полем рациональных чисел в качестве поля констант может быть доказано путём построения S -единицы соответствующей степени, где S состоит из линейного нормирования и бесконечного нормирования.

3.1.1 Базовый алгоритм метода непрерывных дробей

В [13] и параграфе §2.3 отмечено, что теорема 20 дает алгоритм для вычисления фундаментальной S -единицы в случае $\deg h = 1$. Пусть $d_1, \dots, d_r$ —

все делители многочлена f степени, не превосходящей $1/2 \deg f$. Будем последовательно вычислять подходящие дроби к $\sqrt{f}$, $\sqrt{f}/d_1, \dots, \sqrt{f}/d_r$ и для каждой подходящей дроби P_n/Q_n проверять, выполняется ли равенство (2.8):

$$\frac{f}{d_i} \beta_1^2 - d_i \alpha_1^2 = b h^t, \quad \frac{P_n}{Q_n} = \frac{\alpha_1}{\beta_1}.$$

Алгоритм заканчивает работу, как только мы найдем подходящую дробь P_n/Q_n , удовлетворяющую (2.8). Тогда по формулам (2.9) находим решение α, β нормального уравнения (2.7). В этом случае либо $\alpha + \beta\sqrt{f}$, либо $\alpha - \beta\sqrt{f}$ будет фундаментальной S -единицей.

Выше отмечалось, что в случае существования фундаментальной S -единицы существует единственный делитель $d \in \{1, d_1, \dots, d_r\}$, для которого в приведенном алгоритме найдется соответствующая подходящая дробь P_n/Q_n , дающая решение (2.8).

Алгоритм позволяет проверить, удаётся ли построить S -единицу за заранее фиксированное число шагов n . С вычислительной точки зрения алгоритм имеет следующие особенности. Во-первых, на предварительном этапе нам потребуется вычислить $O(n^2)$ коэффициентов каждого $\sqrt{f}/d$ для нахождения подходящей дроби P_n/Q_n . Во-вторых, количество коэффициентов, вычисляемых при проверке равенства (2.8) и нахождении дробно-рациональных функций P_n, Q_n на каждом шаге, растет линейным образом, а следовательно, общее количество коэффициентов растет квадратичным образом относительно текущего шага алгоритма. Кроме того, существенным этапом является этап разложения многочлена f на множители, и поиск делителей. На эту тему имеется большое количество литературы (см., например, [31] и цитируемую там литературу), и обсуждение этого вопроса выходит за рамки настоящего текста.

На практике реализация этого алгоритма с полем $\mathbb{Q}$ в качестве поля констант не позволяет вычислить P_n, Q_n для достаточно больших n за разумное время.

Ниже будут приведены два алгоритма, каждый из которых с вычислительной точки зрения существенно превосходит указанный алгоритм. В частности, оба алгоритма требуют вычисления фиксированного количества коэффициентов на каждом шаге, включая предварительные вычисления.

3.1.2 Алгоритм с вычислением коэффициентов подходящих дробей

В основе нижеприведенного алгоритма лежит следующее замечание. Оказывается, функция $L_n = L_n(P_n, Q_n)$ имеет вид (2.8), если вместо β_1 и α_1 подставить P_n и Q_n . Как показано выше, L_n – многочлен, и его степень согласно (1.15) не превосходит $\deg f$. В этом случае, наша задача сводится к вычислению и проверке того, что L_n имеет вид bh^t , $b \in k$, $t \in \mathbb{N}$, на каждом шаге с номером n . Для этого нам достаточно вычислять ограниченное число коэффициентов у каждой из функций L_n, M_n, A_n, Q_n и P_n .

В этом параграфе запись $z(h)$ для произвольной рациональной функции z подчеркивает, что функция z разложена по степеням многочлена h . И когда речь идёт о коэффициентах функции z подразумеваются коэффициенты именно в этом разложении, если не указано иное.

Рассмотрим данный алгоритм подробнее. Для каждого делителя $d = d_j$ многочлена f , $0 \leq \deg d_j \leq g$, $\deg f = 2g + 1$, достаточно вычислить разложения

$$\frac{f}{d} = c_\gamma h^\gamma + \dots + c_0, \quad d = b_\kappa h^\kappa + \dots + b_0,$$

где $\gamma = \deg f - \deg d > \deg d = \kappa$, а также необходимо знать $2(g + 1)$ коэффициентов степенного ряда $\sqrt{f}$.

На каждом шаге вычисляем коэффициенты многочленов

$$L_n = L_n(h) = (-1)^n \left(dP_n^2 - \frac{f}{d}Q_n^2 \right), \quad 0 < \deg L_n(h) \leq \gamma, \quad L_n(0) = 0,$$

$$M_n = M_n(h) = (-1)^{n+1} \left(dP_nP_{n-1} - \frac{f}{d}Q_nQ_{n-1} \right), \quad 0 \leq \deg M_n(h) \leq \gamma,$$

причем достаточно знать $\kappa + 1$ “старших” коэффициентов числителя дробно-рациональных функций $P_{n-1} = P_{n-1}(h)$, $P_n = P_n(h)$ и $\gamma + 1$ “старших” коэффициентов числителя дробно-рациональных функций $Q_{n-1} = Q_{n-1}(h)$ и $Q_n = Q_n(h)$, где функции P_n и Q_n имеют вид

$$P_n = \frac{p_{n,t_n}h^{t_n} + p_{n,t_n-1}h^{t_n-1} + \dots + p_{n,0}}{h^{t_n}},$$

$$Q_n = \frac{q_{n,t_n}h^{t_n} + q_{n,t_n-1}h^{t_n-1} + \dots + q_{n,0}}{h^{t_n}},$$

$$t_n = \nu_h(P_n) = \nu_h(Q_n) = \sum_{j=1}^n \nu_h(A_j).$$

Если $\nu_h(L_n) = \deg L_n(h)$, то подходящая дробь P_n/Q_n дает решение (2.8), тем самым алгоритм завершает работу.

Формула (1.11) дает возможность вычислить коэффициенты A_{n+1} , причем $s_{n+1} = \nu_h(L_n)$,

$$\begin{aligned}\xi_{n+1}L_n &= M_n + \sqrt{f}, & A_{n+1} &= [\xi_{n+1}], \\ A_{n+1} &= A_{n+1,s_{n+1}}h^{-s_{n+1}} + \dots + A_{n+1,0}.\end{aligned}$$

Далее из рекуррентных формул 1.2 для $n + 1$:

$$P_{n+1} = A_{n+1}P_n + P_{n-1}, \quad Q_{n+1} = A_{n+1}Q_n + Q_{n-1}$$

находим соответственно $\kappa + 1$ и $\gamma + 1$ “старших” коэффициентов числителей дробно-рациональных функций $P_{n+1} = P_{n+1}(h)$ и $Q_{n+1} = Q_{n+1}(h)$.

Суммарно к n -ому шагу в данном алгоритме будет вычислено не более $5n(2s + 2) + O(1)$ коэффициентов.

С вычислительной точки зрения, приведённый алгоритм значительно повысил скорость работы его программной реализации. Однако, на практике скорости работы всё ещё не достаточно для вычисления S -единиц больших степеней с $k = \mathbb{Q}$ в качестве поля констант.

3.1.3 Алгоритм без вычисления коэффициентов подходящих дробей

Следующим этапом развития данного подхода являлось использование рекуррентных равенств для вычисления коэффициентов многочленов L_n и M_n , что позволило не вычислять P_n и Q_n явно. В настоящем параграфе мы сформулируем улучшенный алгоритм.

На очередном шаге с номером $n + 1$ вычислим коэффициенты A_{n+1} по формуле (1.11). Далее вычисляем коэффициенты многочленов L_{n+1} и M_{n+1} по рекуррентным формулам (1.16), (1.18)

$$M_{n+1} = A_{n+1}L_n - M_n, \quad L_{n+1} = L_{n-1} + A_{n+1}(M_n - M_{n+1}).$$

Если $\nu_h(L_n) = \deg L_n(h)$, то подходящая дробь P_n/Q_n дает решение (2.8), тем самым алгоритм завершает работу.

Суммарно к n -ому шагу в данном алгоритме будет вычислено не более $3n(2s + 2) + O(1)$ коэффициентов.

Существенное уменьшение числа вычисляемых коэффициентов и, как следствие, числа арифметических операций, а также отсутствие необходимости вычислять P_n, Q_n позволило значительно сократить время работы алгоритма и построить S -единицы больших степеней с $k = \mathbb{Q}$ в качестве поля констант.

3.1.4 S -единицы больших степеней над $\mathbb{Q}$ в качестве поля констант

С помощью вышеуказанного алгоритма метода непрерывных дробей удаётся построить S -единицы больших порядков, где $S = \{\nu_h^+, \nu_\infty\}$, $\deg h = 1$.

Рассмотрим многочлены

$$\begin{aligned} f_{20} &= (4x^4 - 2x + 1)(2x + 1) \\ h_{20} &= x - 1. \end{aligned}$$

Теорема 22. Пусть $S_{20} = \{\nu_{h_{20}}^+, \nu_\infty\}$, тогда поле $L_{20} = \mathbb{Q}(x)(\sqrt{f_{20}})$ обладает фундаментальной S_{20} -единицей, степень которой равна 20 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{20}}$.

Доказательство. Коэффициенты $u_{20} = \alpha_{20} - \beta_{20}\sqrt{f_{20}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{20} &= -\frac{1}{4}h_{20}^{10} - 16h_{20}^9 - 172h_{20}^8 - \frac{3009}{4}h_{20}^7 - \frac{14087}{8}h_{20}^6 - \frac{4925}{2}h_{20}^5 - \\ &\quad - \frac{17349}{8}h_{20}^4 - \frac{9765}{8}h_{20}^3 - \frac{3429}{8}h_{20}^2 - \frac{1377}{16}h_{20} - \frac{243}{32}, \\ \beta_{20} &= h_{20}^7 + \frac{149}{8}h_{20}^6 + \frac{685}{8}h_{20}^5 + \frac{1273}{8}h_{20}^4 + \frac{303}{2}h_{20}^3 + \frac{1269}{16}h_{20}^2 + \frac{351}{16}h_{20} + \frac{81}{32}, \\ \alpha_{20}^2 - f_{20}\beta_{20}^2 &= \frac{1}{16}h_{20}^{20}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f_{21} &= 8x^5 - 7x^4 + 6x^3 - x^2 + 2x + 1 \\ h_{21} &= x - 1. \end{aligned}$$

Теорема 23. Пусть $S_{21} = \{\nu_{h_{21}}^+, \nu_\infty\}$, тогда поле $L_{21} = \mathbb{Q}(x)(\sqrt{f_{21}})$ обладает фундаментальной S_{21} -единицей, степень которой равна 21 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{21}}$.

Доказательство. Коэффициенты $u_{21} = \alpha_{21} - \beta_{21}\sqrt{f_{21}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{21} &= -25 h_{21}^{10} - 332 h_{21}^9 - \frac{6087}{4} h_{21}^8 - \frac{31711}{8} h_{21}^7 - \frac{110055}{16} h_{21}^6 - \frac{135999}{16} h_{21}^5 - \\ &\quad - \frac{61749}{8} h_{21}^4 - \frac{82215}{16} h_{21}^3 - \frac{19683}{8} h_{21}^2 - \frac{12393}{16} h_{21} - \frac{2187}{16}, \\ \beta_{21} &= h_{21}^8 + 37 h_{21}^7 + \frac{787}{4} h_{21}^6 + \frac{3663}{8} h_{21}^5 + \frac{10881}{16} h_{21}^4 + \frac{2619}{4} h_{21}^3 + \frac{7047}{16} h_{21}^2 + \\ &\quad + \frac{729}{4} h_{21} + \frac{729}{16}, \\ \alpha_{21}^2 - f_{21} \beta_{21}^2 &= -8 h_{21}^{21}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned}f_{22} &= (16x^4 - 16x^3 + x + 1)(x + 1) \\ h_{22} &= x - 1.\end{aligned}$$

Теорема 24. Пусть $S_{22} = \{\nu_{h_{22}}^+, \nu_\infty\}$, тогда поле $L_{22} = \mathbb{Q}(x)(\sqrt{f_{22}})$ обладает фундаментальной S_{22} -единицей, степень которой равна 22 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{22}}$.

Доказательство. Коэффициенты $u_{22} = \alpha_{22} - \beta_{22}\sqrt{f_{22}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{22} &= -\frac{1}{3} h_{22}^{11} - 24 h_{22}^{10} - 284 h_{22}^9 - \frac{7729}{6} h_{22}^8 - \frac{8738}{3} h_{22}^7 - \frac{44425}{12} h_{22}^6 - \\ &\quad - \frac{270361}{96} h_{22}^5 - \frac{64021}{48} h_{22}^4 - \frac{1591}{4} h_{22}^3 - \frac{437}{6} h_{22}^2 - \frac{15}{2} h_{22} - \frac{1}{3}, \\ \beta_{22} &= h_{22}^8 + \frac{257}{12} h_{22}^7 + \frac{1343}{12} h_{22}^6 + 214 h_{22}^5 + \frac{17969}{96} h_{22}^4 + \frac{347}{4} h_{22}^3 + \\ &\quad + \frac{89}{4} h_{22}^2 + 3 h_{22} + \frac{1}{6}, \\ \alpha_{22}^2 - f_{22} \beta_{22}^2 &= \frac{1}{9} h_{22}^{22}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f_{23} &= -24x^5 + 153x^4 - 36x^3 - 8x^2 - 8x + 4 \\ h_{23} &= x - 1. \end{aligned}$$

Теорема 25. Пусть $S_{23} = \{\nu_{h_{23}}^+, \nu_\infty\}$, тогда поле $L_{23} = \mathbb{Q}(x)(\sqrt{f_{23}})$ обладает фундаментальной S_{23} -единицей, степень которой равна 23 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{23}}$.

К сожалению, предъявить здесь S -единицы степеней 23 и выше не представляется возможным, ввиду величины и количества коэффициентов. Однако, для того, чтобы у читателя возникло представление о значениях коэффициентов указанной единицы, приведём их частично.

Доказательство. Коэффициенты $u_{23} = \alpha_{23} - \beta_{23}\sqrt{f_{23}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{23} &= -63h_{23}^{11} + 1626h_{23}^{10} - \frac{10809}{2}h_{23}^9 - \frac{156621}{4}h_{23}^8 + \frac{1280743}{48}h_{23}^7 + \dots, \\ \beta_{23} &= h_{23}^9 - 82h_{23}^8 + \frac{1601}{2}h_{23}^7 + \frac{11527}{12}h_{23}^6 - \frac{173331}{16}h_{23}^5 - \frac{558495}{16}h_{23}^4 - \\ &\quad - \frac{2899719}{64}h_{23}^3 - \frac{3851307}{128}h_{23}^2 - \frac{649539}{64}h_{23} - \frac{177147}{128}, \\ \alpha_{23}^2 - f_{23}\beta_{23}^2 &= 24h_{23}^{23}. \end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned} f_{24} &= (8x^4 - 5x^3 + 14x^2 - 12x + 8)(3x + 2) \\ h_{24} &= x - 2. \end{aligned}$$

Теорема 26. Пусть $S_{24} = \{\nu_{h_{24}}^+, \nu_\infty\}$, тогда поле $L_{24} = \mathbb{Q}(x)(\sqrt{f_{24}})$ обладает фундаментальной S_{24} -единицей, степень которой равна 24 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{24}}$.

Доказательство. Коэффициенты $u_{24} = \alpha_{24} - \beta_{24}\sqrt{f_{24}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{24} &= -\frac{4}{19}h_{24}^{12} - 57h_{24}^{11} - 2576h_{24}^{10} - \frac{887888}{19}h_{24}^9 - \frac{8633472}{19}h_{24}^8 - \dots, \\ \beta_{24} &= h_{24}^9 + \frac{1620}{19}h_{24}^8 + 2016h_{24}^7 + \frac{398720}{19}h_{24}^6 + \frac{2234112}{19}h_{24}^5 + \dots, \\ \alpha_{24}^2 - f_{24}\beta_{24}^2 &= \frac{16}{361}h_{24}^{24}. \end{aligned}$$



Рассмотрим многочлены

$$\begin{aligned} f_{25} &= 972 x^5 + 900 x^4 - 900 x^3 + 165 x^2 + 30 x + 1 \\ h_{25} &= x - \frac{1}{3}. \end{aligned}$$

Теорема 27. Пусть $S_{25} = \{\mathbf{v}_{h_{25}}^+, \mathbf{v}_\infty\}$, тогда поле $L_{25} = \mathbb{Q}(x)(\sqrt{f_{25}})$ обладает фундаментальной S_{25} -единицей, степень которой равна 25 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{25}}$.

Доказательство. Коэффициенты $u_{25} = \alpha_{25} - \beta_{25}\sqrt{f_{25}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{25} &= -\frac{175}{3} h_{25}^{11} + \frac{775}{27} h_{25}^{10} - \frac{7250}{243} h_{25}^9 + \frac{648125}{177147} h_{25}^8 - \frac{880625}{531441} h_{25}^7 - \dots, \\ \beta_{25} &= h_{25}^{10} - \frac{35}{27} h_{25}^9 + \frac{440}{243} h_{25}^8 - \frac{20675}{19683} h_{25}^7 + \frac{321175}{531441} h_{25}^6 - \frac{105475}{531441} h_{25}^5 + \dots, \\ \alpha_{25}^2 - f_{25} \beta_{25}^2 &= -972 h_{25}^{25}. \end{aligned}$$



Рассмотрим многочлены

$$\begin{aligned} f_{26} &= -(4x^4 - 21x^3 + 24x^2 + 9x - 18)(3x + 2) \\ h_{26} &= x - 2. \end{aligned}$$

Теорема 28. Пусть $S_{26} = \{\mathbf{v}_{h_{26}}^+, \mathbf{v}_\infty\}$, тогда поле $L_{26} = \mathbb{Q}(x)(\sqrt{f_{26}})$ обладает фундаментальной S_{26} -единицей, степень которой равна 26 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{26}}$.

Доказательство. Коэффициенты $u_{26} = \alpha_{26} - \beta_{26}\sqrt{f_{26}}$ имеют следующий вид:

$$\begin{aligned} \alpha_{26} &= \frac{3}{8} h_{26}^{13} - 16 h_{26}^{12} + \frac{236}{3} h_{26}^{11} + \frac{1504}{9} h_{26}^{10} - \frac{26945}{27} h_{26}^9 - \frac{49780}{81} h_{26}^8 + \dots, \\ \beta_{26} &= h_{26}^{10} - \frac{95}{6} h_{26}^9 + \frac{343}{6} h_{26}^8 + \frac{254}{27} h_{26}^7 - \frac{19114}{81} h_{26}^6 - \frac{11}{9} h_{26}^5 + \frac{11269}{27} h_{26}^4 + \dots, \\ \alpha_{26}^2 - f_{26} \beta_{26}^2 &= \frac{9}{64} h_{26}^{26}. \end{aligned}$$



Рассмотрим многочлены

$$f_{27} = 16x^5 + 57x^4 + 70x^3 + 39x^2 + 10x + 1$$

$$h_{27} = x.$$

Теорема 29. Пусть $S_{27} = \{\nu_{h_{27}}^+, \nu_\infty\}$, тогда поле $L_{27} = \mathbb{Q}(x)(\sqrt{f_{27}})$ обладает фундаментальной S_{27} -единицей, степень которой равна 27 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{27}}$.

Доказательство. Коэффициенты $u_{27} = \alpha_{27} - \beta_{27}\sqrt{f_{27}}$ имеют следующий вид:

$$\alpha_{27} = -49h_{27}^{13} - \frac{4891}{4}h_{27}^{12} - \frac{17981}{2}h_{27}^{11} - \frac{121825}{4}h_{27}^{10} - 57842h_{27}^9 - 69044h_{27}^8 - \dots,$$

$$\beta_{27} = h_{27}^{11} + \frac{293}{4}h_{27}^{10} + \frac{3195}{4}h_{27}^9 + \frac{12091}{4}h_{27}^8 + \frac{10621}{2}h_{27}^7 + \frac{21089}{4}h_{27}^6 + \dots,$$

$$\alpha_{27}^2 - f_{27}\beta_{27}^2 = -16h_{27}^{27}.$$

□

Рассмотрим многочлены

$$f_{28} = (9x^3 - 8x^2 + 20x + 16)(4x^2 + x + 4)$$

$$h_{28} = x - \frac{4}{3}.$$

Теорема 30. Пусть $S_{28} = \{\nu_{h_{28}}^+, \nu_\infty\}$, тогда поле $L_{28} = \mathbb{Q}(x)(\sqrt{f_{28}})$ обладает фундаментальной S_{28} -единицей, степень которой равна 28 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{28}}$.

Доказательство. Коэффициенты $u_{28} = \alpha_{28} - \beta_{28}\sqrt{f_{28}}$ имеют следующий вид:

$$\alpha_{28} = -\frac{18}{49}h_{28}^{14} - 49h_{28}^{13} - \frac{3430}{3}h_{28}^{12} - \frac{325703}{27}h_{28}^{11} - \frac{19033756}{243}h_{28}^{10} - \dots,$$

$$\beta_{28} = h_{28}^{11} + 42h_{28}^{10} + \frac{4819}{9}h_{28}^9 + \frac{874006}{243}h_{28}^8 + \frac{103701248}{6561}h_{28}^7 + \dots,$$

$$\alpha_{28}^2 - f_{28}\beta_{28}^2 = \frac{324}{2401}h_{28}^{28}.$$

□

Рассмотрим многочлены

$$f_{29} = 32x^5 - 47x^4 + 20x^3 + 2x^2 - 4x + 1$$

$$h_{29} = x - 1.$$

Теорема 31. Пусть $S_{29} = \{\nu_{h_{29}}^+, \nu_\infty\}$, тогда поле $L_{29} = \mathbb{Q}(x)(\sqrt{f_{29}})$ обладает фундаментальной S_{29} -единицей, степень которой равна 29 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{29}}$.

Доказательство. Коэффициенты $u_{29} = \alpha_{29} - \beta_{29}\sqrt{f_{29}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{29} &= -89 h_{29}^{14} - 3670 h_{29}^{13} - 45230 h_{29}^{12} - 263316 h_{29}^{11} - 882052 h_{29}^{10} - \dots, \\ \beta_{29} &= h_{29}^{12} + 122 h_{29}^{11} + 2332 h_{29}^{10} + 16648 h_{29}^9 + 59244 h_{29}^8 + 121872 h_{29}^7 + \dots, \\ \alpha_{29}^2 - f_{29}\beta_{29}^2 &= -32 h_{29}^{29}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned}f_{30} &= -(32x^4 - 33x^3 - 123x^2 - 63x - 9)(x + 1) \\ h_{30} &= x + \frac{3}{4}.\end{aligned}$$

Теорема 32. Пусть $S_{30} = \{\nu_{h_{30}}^+, \nu_\infty\}$, тогда поле $L_{30} = \mathbb{Q}(x)(\sqrt{f_{30}})$ обладает фундаментальной S_{30} -единицей, степень которой равна 30 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{30}}$.

Доказательство. Коэффициенты $u_{30} = \alpha_{30} - \beta_{30}\sqrt{f_{30}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{30} &= -\frac{8}{21} h_{30}^{15} + 42 h_{30}^{14} - \frac{11525}{16} h_{30}^{13} + \frac{5202887}{1344} h_{30}^{12} - \frac{20529531}{3584} h_{30}^{11} - \dots, \\ \beta_{30} &= h_{30}^{12} - \frac{11507}{336} h_{30}^{11} + \frac{369799}{1344} h_{30}^{10} - \frac{489975}{896} h_{30}^9 - \frac{1502455}{4096} h_{30}^8 + \dots, \\ \alpha_{30}^2 - f_{30}\beta_{30}^2 &= \frac{64}{441} h_{30}^{30}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned}f_{32} &= -(16x^4 - 99x^3 - 228x^2 - 135x - 18)(3x + 2) \\ h_{32} &= x.\end{aligned}$$

Теорема 33. Пусть $S_{32} = \{\nu_{h_{32}}^+, \nu_\infty\}$, тогда поле $L_{32} = \mathbb{Q}(x)(\sqrt{f_{32}})$ обладает фундаментальной S_{32} -единицей, степень которой равна 32 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{32}}$.

Доказательство. Коэффициенты $u_{32} = \alpha_{32} - \beta_{32}\sqrt{f_{32}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{32} &= \frac{24}{53} h_{32}^{16} - 53 h_{32}^{15} + \frac{2467}{3} h_{32}^{14} - \frac{2631595}{3816} h_{32}^{13} - \frac{766708927}{45792} h_{32}^{12} - \dots, \\ \beta_{32} &= h_{32}^{13} - \frac{5447}{159} h_{32}^{12} + \frac{187943}{1272} h_{32}^{11} + \frac{4859569}{5724} h_{32}^{10} + \frac{64444735}{40704} h_{32}^9 + \dots, \\ \alpha_{32}^2 - f_{32}\beta_{32}^2 &= \frac{576}{2809} h_{32}^{32}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned}f_{34} &= -(32x^3 - 59x^2 + 28x - 4)(27x^2 - 20x + 4) \\ h_{34} &= x.\end{aligned}$$

Теорема 34. Пусть $S_{34} = \{\nu_{h_{34}}^+, \nu_\infty\}$, тогда поле $L_{34} = \mathbb{Q}(x)(\sqrt{f_{34}})$ обладает фундаментальной S_{34} -единицей, степень которой равна 34 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{34}}$.

Доказательство. Коэффициенты $u_{34} = \alpha_{34} - \beta_{34}\sqrt{f_{34}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{34} &= \frac{432}{277} h_{34}^{17} - 277 h_{34}^{16} + \frac{220136}{27} h_{34}^{15} - \frac{235233784}{2493} h_{34}^{14} + \frac{472487072}{831} h_{34}^{13} - \dots, \\ \beta_{34} &= h_{34}^{14} - \frac{432496}{7479} h_{34}^{13} + \frac{799052}{831} h_{34}^{12} - \frac{53823040}{7479} h_{34}^{11} + \frac{24331952}{831} h_{34}^{10} - \dots, \\ \alpha_{34}^2 - f_{34}\beta_{34}^2 &= \frac{186624}{76729} h_{34}^{34}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned}f_{36} &= (3x^4 + 28x^3 - 8x^2 - 8x + 12)(4x + 3) \\ h_{36} &= x + 2.\end{aligned}$$

Теорема 35. Пусть $S_{36} = \{\nu_{h_{36}}^+, \nu_\infty\}$, тогда поле $L_{36} = \mathbb{Q}(x)(\sqrt{f_{36}})$ обладает фундаментальной S_{36} -единицей, степень которой равна 36 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{36}}$.

Доказательство. Коэффициенты $u_{36} = \alpha_{36} - \beta_{36}\sqrt{f_{36}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{36} &= -\frac{1}{9}h_{36}^{18} - 54h_{36}^{17} - \frac{24491}{6}h_{36}^{16} - \frac{23181596}{243}h_{36}^{15} - \frac{108463667}{243}h_{36}^{14} + \dots, \\ \beta_{36} &= h_{36}^{15} + \frac{25799}{162}h_{36}^{14} + \frac{1597891}{243}h_{36}^{13} + \frac{6849617}{81}h_{36}^{12} - \frac{1056283}{9}h_{36}^{11} - \dots, \\ \alpha_{36}^2 - f_{36}\beta_{36}^2 &= \frac{1}{81}h_{36}^{36}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned}f_{39} &= 192x^5 + 337x^4 - 1056x^3 + 852x^2 - 288x + 36 \\ h_{39} &= x - \frac{3}{4}.\end{aligned}$$

Теорема 36. Пусть $S_{39} = \{\nu_{h_{39}}^+, \nu_\infty\}$, тогда поле $L_{39} = \mathbb{Q}(x)(\sqrt{f_{39}})$ обладает фундаментальной S_{39} -единицей, степень которой равна 39 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{39}}$.

Доказательство. Коэффициенты $u_{39} = \alpha_{39} - \beta_{39}\sqrt{f_{39}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{39} &= -345h_{39}^{19} - \frac{851171}{24}h_{39}^{18} - \frac{268660479}{256}h_{39}^{17} - \frac{55600732287}{4096}h_{39}^{16} - \dots, \\ \beta_{39} &= h_{39}^{17} + \frac{7373}{24}h_{39}^{16} + \frac{3800211}{256}h_{39}^{15} + \frac{1055613113}{4096}h_{39}^{14} + \frac{132974896587}{65536}h_{39}^{13} + \dots, \\ \alpha_{39}^2 - f_{39}\beta_{39}^2 &= -192h_{39}^{39}.\end{aligned}$$

□

3.2 Случай нелинейного нормирования

Метод непрерывных дробей является эффективным методом вычисления S -единиц, для S указанного выше вида. Однако, как отмечалось ранее, в указанном виде он эффективно работает только в случае $\deg h = 1$. Следовательно, для некоторых кривых непосредственное его применение не имеет смысла. Для более общего случая можно использовать метод матричной линеаризации из [13].

Точно также как и в случае метода непрерывных дробей авторами метода были доказаны результаты для случая поля $\mathbb{F}_q$ в качестве поля констант. Приведём основные результаты, относящиеся к данному методу для случая поля $\mathbb{Q}$ в качестве поля констант.

3.2.1 Метод матричной линеаризации Платонова и Беньш-Кривеца

Каждый элемент из пополнения $k(x)_{\nu_h}$ можно представить в виде формального степенного ряда с коэффициентами из Σ , где Σ — выбранная в $k[x]$ фиксированная система представителей смежных классов по идеалу (h) , состоящая из всех многочленов степени меньшей, чем $\deg h$ (подробнее см. [13; 28]).

Введем следующее обозначение. Если $\alpha(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_r x^r \in k[x]$, то через $\hat{\alpha} = (\alpha_0, \dots, \alpha_r)^t$ будем обозначать вектор-столбец коэффициентов α .

Для дальнейшего изложения необходимо привести здесь аналоги некоторых важных утверждений из [13] для случая произвольного поля k характеристики отличной от 2 в качестве поля констант.

Предложение 33 ([13], Предложение 3.2). Пусть $h(x) = h_0 + h_1 x + \dots + h_l x^l$, $h_l \neq 0$, — фиксированный неприводимый многочлен и пусть $a(x) = a_0 + a_1 x + \dots + a_{l-1} x^{l-1}$, $b(x) = b_0 + b_1 x + \dots + b_{l-1} x^{l-1}$ — многочлены из $k[x]$. Разделим ab на h с остатком: $ab = qh + r$, где $q = q_0 + q_1 x + \dots + q_{l-2} x^{l-2}$, $r = r_0 + r_1 x + \dots + r_{l-1} x^{l-1}$. Тогда существуют $(l \times l)$ -матрицы $A_h(a)$ и $B_h(a)$, коэффициенты которых являются линейными функциями от $a_0, \dots, a_{l-1}$ с коэффициентами из $\mathbb{Q}$, такие, что

$$\hat{r} = A_h(a)\hat{b}, \quad \begin{pmatrix} \hat{q} \\ 0 \end{pmatrix} = B_h(a)\hat{b}.$$

Предложение 34 ([13], Предложение 3.3). Пусть $u_1 = \sum_{i=s_1}^{\infty} a_i h^i$, $u_2 = \sum_{i=s_2}^{\infty} b_i h^i$ — два элемента из пополнения $k(x)_{\nu_h}$. Положим $C_h(a_{s_1}) = A_h(a_{s_1})$ и $C_h(a_i) = A_h(a_i) + B_h(a_{i-1})$ при $i > s_1$. Тогда $u_1 u_2 = \sum_{j=s_1+s_2}^{\infty} L_j h^j$, где

$$\hat{L}_j = \sum_{i+s=j} C_h(a_i)\hat{b}_s.$$

Предположим, что для заданного m норменное уравнение (9) имеет решение в многочленах $\alpha, \beta \in k[x]$, $\beta \neq 0$. Поскольку нормирование ν_h имеет два

продолжения на L , то $\sqrt{f} \in k(x)_{\nu_h}$. Представим α , β , $\sqrt{f}$ в виде формальных степенных рядов:

$$\alpha = \alpha_0 + \alpha_1 h + \cdots + \alpha_r h^r, \quad \beta = \beta_0 + \beta_1 h + \cdots + \beta_e h^e, \quad \sqrt{f} = \sum_{i=0}^{\infty} f_i h^i,$$

где $\alpha_i, \beta_i, f_i \in \Sigma$. Сравнение степеней левой и правой части в (9) показывает, что

$$m \geq \frac{\deg f}{\deg h}, \quad r = \left\lfloor \frac{m}{2} \right\rfloor, \quad e = \left\lfloor \frac{m \deg h - \deg f}{2 \deg h} \right\rfloor,$$

где $[z]$ означает целую часть числа z . Кроме того, степени многочленов α_r и β_e должны удовлетворять следующим соотношениям:

$$r_1 = \deg \alpha_r = \left\lfloor \left(\frac{m}{2} - r \right) \deg h \right\rfloor = \begin{cases} 0, & \text{если } m \text{ четно,} \\ \left\lfloor \frac{\deg h}{2} \right\rfloor, & \text{если } m \text{ нечетно,} \end{cases}$$

$$e_1 = \deg \beta_e = \left\lfloor \frac{1}{2} R \right\rfloor,$$

где R — остаток от деления $m \deg h - \deg f$ на $2 \deg h$. Положим $C_h(f_i) = C_i$ и рассмотрим матрицу

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

Пусть D_m — матрица, которая получается из $\overline{D}_m$ вычеркиванием первых $r_1 + 1$ строк и столбцов с номерами $e_1 + 2, \dots, \deg h$ (если $e_1 + 2 > \deg h$, то столбцы не вычеркиваются).

Следующая теорема является основой для матричного алгоритма нахождения фундаментальной S -единицы.

Теорема 37 ([13], Теорема 3.4). Для натурального $m \geq \deg f / \deg h$ норменное уравнение (9) имеет решение в многочленах $\alpha, \beta \in k[x]$, $\beta \neq 0$, тогда и только тогда, когда ранг матрицы D_m меньше, чем $e \deg h + e_1 + 1$.

3.2.2 Алгоритм метода матричной линеаризации

Приведём здесь алгоритм, основанный на методе матричной линеаризации, из [13].

Чтобы найти фундаментальную S -единицу поля L , вначале нужно разложить $\sqrt{f}$ в формальный степенной ряд. Затем, вычисляя последовательно ранг матрицы D_m , начиная с $m \geq \deg f / \deg h$, находим минимальное натуральное m такое, что ранг D_m меньше, чем $e \deg h + e_1 + 1$. После этого, решая однородную систему линейных уравнений с матрицей D_m , находим ненулевой многочлен β , а по формулам

$$\hat{\alpha}_i = - \sum_{j+j'=i, j' \leq e} C_j \hat{\beta}_{j'}, \quad 0 \leq i < r, \quad \tilde{\alpha}_r = - \sum_{p=0}^e \tilde{C}_{r-p} \hat{\beta}_p,$$

где $\tilde{C}_i$ — матрица, которая состоит из первых $r_1 + 1$ строк матрицы C_i , находим многочлен α . Искомая фундаментальная S -единица имеет вид $\alpha + \beta \sqrt{f}$.

3.2.3 S -единицы больших степеней

С помощью метода матричной линеаризации удаётся построить S -единицы больших порядков, где $S = \{\nu'_h, \nu_\infty\}$, в том случае, когда для данной кривой подходящего нормирования первой степени не существует.

Рассмотрим многочлены

$$f_{40} = -(64x^4 - 125x^3 - 250x^2 - 160x - 32)(5x + 2)$$

$$h_{40} = x^2 - \frac{14}{5}x - \frac{8}{5}.$$

Теорема 38. Пусть $S_{40} = \{\nu_{h_{40}}^+, \nu_\infty\}$, тогда поле $L_{40} = \mathbb{Q}(x)(\sqrt{f_{40}})$ обладает фундаментальной S_{40} -единицей, степень которой равна 40 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{40}}$.

Доказательство. Коэффициенты $u_{40} = \alpha_{40} - \beta_{40}\sqrt{f_{40}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{40} &= -\frac{128}{913} h_{40}^{20} + \frac{75}{1826} h_{40}^{19}(120x - 721) + \frac{(8390045x - 160114702)}{1460800} h_{40}^{18} + \dots, \\ \beta_{40} &= -\frac{1}{913} h_{40}^{18}(60x - 913) - \frac{17}{36520000} h_{40}^{17}(7475085x - 26535266) - \dots, \\ \alpha_{40}^2 - f_{40}\beta_{40}^2 &= \frac{16384}{833569} h_{40}^{40}.\end{aligned}$$

□

Рассмотрим многочлены

$$\begin{aligned}f_{48} &= (64x^4 + 225x^3 + 264x^2 + 117x + 18)(x + 2) \\ h_{48} &= x^2 + \frac{1}{4}x - \frac{3}{2}.\end{aligned}$$

Теорема 39. Пусть $S_{48} = \{\mathbf{v}_{h_{48}}^+, \mathbf{v}_\infty\}$, тогда поле $L_{48} = \mathbb{Q}(x)(\sqrt{f_{48}})$ обладает фундаментальной S_{48} -единицей, степень которой равна 48 и совпадает с порядком соответствующей $\mathbb{Q}$ -точки якобиана $J_{f_{48}}$.

Доказательство. Коэффициенты $u_{48} = \alpha_{48} - \beta_{48}\sqrt{f_{48}}$ имеют следующий вид:

$$\begin{aligned}\alpha_{48} &= -\frac{64}{344387} h_{48}^{24} - \frac{255}{688774} h_{48}^{23}(1020x + 346073) - \dots, \\ \beta_{48} &= \frac{1}{344387} h_{48}^{22}(510x + 344387) + \frac{(4454762690x + 429814442277)}{22040768} h_{48}^{21} + \dots, \\ \alpha_{48}^2 - f_{48}\beta_{48}^2 &= \frac{4096}{118602405769} h_{48}^{48}.\end{aligned}$$

□

Заключение

В диссертации были получены результаты о периодичности разложений в непрерывную дробь ключевых элементов, связанных с элементом $\sqrt{f}$, где многочлен f определяет гиперэллиптическое поле, а k — поле характеристики отличной от 2. Показано, что эти элементы играют важную роль при изучении квазипериодических непрерывных дробей в гиперэллиптических полях. Доказана периодичность квазипериодических разложений в непрерывную дробь элементов вышеуказанного типа. Для S , состоящего из конечного и бесконечного нормирования, получены оценки, связывающие степень фундаментальной S -единицы гиперэллиптического поля и квазипериод разложения в непрерывную дробь некоторого элемента гиперэллиптического поля. Отметим, что степень S -единицы связана с порядком некоторой точки кручения якобиана соответствующей гиперэллиптической кривой. Исследование свойств разложения этого элемента в непрерывную дробь позволяет ответить на вопрос о существовании S -единиц в гиперэллиптическом поле. В диссертационной работе получили развитие алгоритмы В. П. Платонова и В. В. Беняш-Кривеца поиска и построения фундаментальных S -единиц в гиперэллиптических полях. Была разработана массивно-параллельная программная реализация указанных алгоритмов, показавшую свою эффективность в получении фундаментальных S -единиц новых степеней. Полученные S -единицы позволили построить $\mathbb{Q}$ -точки кручения соответствующих больших порядков в якобианах кривых рода 2.

Благодарности

Соискатель искренне благодарит научного руководителя, академика РАН, профессора В. П. Платонова за постановку задач, многочисленные научные идеи, полезные и вдохновляющие советы, терпение и поддержку. Соискатель выражает благодарность коллективу отдела теоретической и прикладной алгебры и теории чисел ФГУ ФНЦ НИИСИ РАН за замечательную научную и рабочую атмосферу.

Список литературы

1. *Artin E., Whaples G.* Axiomatic characterization of fields by the product formula for valuations // Bulletin of the American Mathematical Society. — 1945. — Vol. 51, no. 7. — P. 469—492.
2. *Mazur B.* Rational points on modular curves // Modular Functions of one Variable V / ed. by J.-P. Serre, D. B. Zagier. — Springer Berlin Heidelberg, 1977. — P. 107—148. — (Lecture Notes in Mathematics).
3. *Flynn E. V.* Large rational torsion on abelian varieties // J. Number Theory. — 1990. — Vol. 36, no. 3. — P. 257—265.
4. *Leprévost F.* Famille de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 13 // C. R. Acad. Sci. Paris Sér. I Math. — 1991. — Vol. 313, no. 7. — P. 451—454.
5. *Leprévost F.* Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 15, 17, 19 ou 21 // C. R. Acad. Sci. Paris Sér. I Math. — 1991. — Vol. 313, no. 11. — P. 771—774.
6. *Leprévost F.* Jacobiennes de certaines courbes de genre 2: torsion et simplicité // J. Théor. Nombres Bordeaux. — 1995. — Vol. 7, no. 1. — P. 283—306.
7. *Ogawa H.* Curves of genus 2 with a rational torsion divisor of order 23 // Proc. Japan Acad. Ser. A Math. Sci. — 1994. — Vol. 70, no. 9. — P. 295—298.
8. *Elkies N. D.* Curves of genus 2 over $\mathbb{Q}$ whose Jacobians are absolutely simple abelian surfaces with torsion points of high order // preprint Harvard University. — 2010.
9. *Howe E. W., Leprévost F., Poonen B.* Large torsion subgroups of split Jacobians of curves of genus two or three // Forum Math. — 2000. — Vol. 12, no. 3. — P. 315—364.
10. *Howe E. W.* Genus-2 Jacobians with torsion points of large order // Bull. Lond. Math. Soc. — 2015. — Vol. 47, no. 1. — P. 127—135.
11. *Bernard N., Leprévost F., Pohst M.* Jacobians of genus-2 curves with a rational point of order 11 // Experiment. Math. — 2009. — Vol. 18, no. 1. — P. 65—70.

12. *Платонов В. П.* Арифметика квадратичных полей и кручение в якобианах // Доклады Академии наук. — 2010. — Т. 430, № 3. — С. 318—320.
13. *Беняш-Кривец В. В., Платонов В. П.* Группы S-единиц в гиперэллиптических полях и непрерывные дроби // Математический сборник. — 2009. — Т. 200, № 11. — С. 15—44.
14. *Платонов В. П., Петрунин М. М.* Новые порядки точек кручения в якобианах кривых рода 2 над полем рациональных чисел // Доклады Академии наук. — 2012. — Т. 443, № 6. — С. 664—667.
15. *Платонов В. П., Петрунин М. М.* О проблеме кручения в якобианах кривых рода 2 над полем рациональных чисел // Доклады Академии наук. — 2012. — Т. 446, № 3. — С. 263—264.
16. *Платонов В. П., Петрунин М. М.* Фундаментальные S-единицы в гиперэллиптических полях и проблема кручения в якобианах гиперэллиптических кривых // Доклады Академии наук. — 2015. — Т. 465, № 1. — С. 23—25.
17. *Abel N.* Ueber die Integration der Differential-Formel $\rho dx / \sqrt{R}$ wenn R und ρ ganze Functionen sind // Journal für die reine und angewandte Mathematik. — 1826. — Vol. 1. — P. 185—221.
18. *Tchebicheff P.* Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynome du troisieme ou du quatrieme degré' // Journal des math. pures et appl. — 1857. — Vol. 2. — P. 168—192.
19. *Adams W. W., Razar M. J.* Multiples of point on elliptic curves and continued fractions // Proc. London Math. Soc. — 1980. — Vol. 41, no. 3. — P. 481—498.
20. *Schmidt W. M.* On continued fractions and Diophantine approximation in power series fields // Acta arithmetica. — 2000. — Vol. 95, no. 2. — P. 139—166.
21. *Платонов В. П.* Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // УМН. — 2014. — Т. 69:1, № 415. — С. 3—38.
22. *Платонов В. П., Федоров Г. В.* О периодичности непрерывных дробей в эллиптических полях // Доклады Академии наук. — 2017. — Т. 475, № 2. — С. 133—136.

23. *Платонов В. П., Федоров Г. В.* О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Математический сборник. — 2018. — Т. 209, № 4. — С. 54—94.
24. *Платонов В. П., Жгун В. С., Федоров Г. В.* О периодичности непрерывных дробей в гиперэллиптических полях над квадратичным полем констант // Доклады Академии наук. — 2018. — Т. 482, № 2. — С. 137—141.
25. *Платонов В. П., Федоров Г. В.* О периодичности непрерывных дробей в гиперэллиптических полях // Доклады Академии наук. — 2017. — Т. 474, № 5. — С. 540—544.
26. *Платонов В. П., Жгун В. С., Федоров Г. В.* Непрерывные дроби в гиперэллиптических полях и представление Мамфорда // Доклады Академии наук. — 2016. — Т. 471, № 6. — С. 640—644.
27. *Платонов В. П., Федоров Г. В.* S-единицы и периодичность непрерывных дробей в гиперэллиптических полях // Доклады Академии наук. — 2015. — Т. 465, № 5. — С. 537—541.
28. *Ленг С.* Алгебра. — Мир, 1968.
29. *Artin E.* Quadratische Körper im Gebiete der höheren Kongruenzen. I. // Mathematische Zeitschrift. — 1924. — Vol. 19, no. 1. — P. 153—206.
30. *Stichtenoth H.* Algebraic function fields and codes. Т. 254. — Springer Science & Business Media, 2009.
31. *Hart W., Hoeij M. van, Novocin A.* Practical polynomial factoring in polynomial time // ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation. — ACM, New York, 2011. — С. 163—170.

Публикации автора по теме диссертации

Статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности

32. *Петрунин М. М.* Вычисление фундаментальных S-единиц в гиперэллиптических полях рода 2 и проблема кручения в якобианах гиперэллиптических кривых // Чебышевский Сборник. — 2015. — Т. 16, № 4. — С. 250—283.

33. *Петрунин М. М., Платонов В. П. S-единицы в гиперэллиптических полях и периодичность непрерывных дробей // Доклады Академии наук. — 2016. — Т. 470, № 3. — С. 260—265.*
34. *Петрунин М. М. S-единицы и периодичность квадратного корня в гиперэллиптических полях // Доклады Академии наук. — 2017. — Т. 474, № 2. — С. 155—158.*
35. *Петрунин М. М., Платонов В. П. Группы S-единиц и проблема периодичности непрерывных дробей в гиперэллиптических полях // Тр. МИАН. — 2018. — Т. 302. — С. 354—376.*

В прочих изданиях

36. *Петрунин М. М. Квазипериодические, но не периодические функциональные непрерывные дроби малых квазипериодов // Труды Научно-Исследовательского Института Системных Исследований Российской Академии Наук. — 2017. — Т. 7, № 3. — С. 14—20.*