МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

Федоров Глеб Владимирович

Теория функциональных непрерывных дробей в гиперэллиптических полях и ее приложения

Специальность
1.1.5 — Математическая логика, алгебра, теория чисел и дискретная математика
(физ.-мат. науки)

Диссертация на соискание учёной степени
доктора физико-математических наук

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

Москва — 2024

Аннотация

Диссертация посвящена существенному развитию и созданию нового научного направления на стыке таких областей математики как теория чисел, алгебра и арифметическая геометрия. Это стало возможным благодаря предложенным новым методам в теории функциональных непрерывных дробей и построению совершенно новой теории функциональных непрерывных дробей обобщенного типа.

Для мирового математического сообщества многие годы остается недоступным решение проблемы кручения в якобиевых многообразиях гиперэллиптических кривых над полем рациональных чисел и над полями алгебраических чисел (далее — проблема кручения). С проблемой кручения тесно связаны следующие глубокие проблемы: проблема периодичности разложения в функциональную непрерывную дробь элементов гиперэллиптических полей, проблема существования и построения фундаментальных единиц и S-единиц в гиперэллиптических полях, проблема поиска решений функциональных аналогов уравнений типа Пелля, проблема ограниченности порядков подгрупп кручения в группах классов дивизоров гиперэллиптических кривых. Эти проблемы относятся к числу важных и трудных проблем современной математики. В настоящий момент нет единого подхода, который мог бы приблизить к решению этих проблем, и каждое продвижение дается с большим трудом. Полное решение указанных проблем невозможно без построения эффективных алгоритмов и высокопроизводительных компьютерных вычислений.

В рамках указанных проблем в диссертации разработан новый подход к изучению арифметических свойств гиперэллиптических кривых и гиперэллиптических полей на основании глубокого анализа группы классов дивизоров и построенной теории функциональных непрерывных дробей обобщенного типа. Этот подход позволил обнаружить множество ярких теоретико-числовых, алгебраических и геометрических свойств и связей таких математических объектов, как функциональные аналоги уравнений Пелля, фундаментальные единицы и S-единицы, якобиевы многообразия, группы классов дивизоров и их подгруппы кручения. С помощью разработанных новых методов в диссертации решена проблема классификации эллиптических полей по признаку периодичности функциональных непрерывных дробей над полем рациональных чисел и над квадратичными полями алгебраических чисел для эллиптических полей, входящих в рациональную параметризацию модулярными кривыми.

Оглавление

Список обозначений

Ниже приведен список основных обозначений диссертационной работы. Более подробно основные понятия и обозначения определяются в Главе 2.

$\mathbb{N}$ — множество натуральных чисел;

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ — множество целых неотрицательных чисел;

$\mathbb{Z}$ — кольцо целых чисел;

$\mathbb{Q}$ — поле рациональных чисел;

$\mathbb{C}$ — поле комплексных чисел;

K — базовое поле;

K^* — мультипликативная группа поля K;

$\overline{K}$ — алгебраическое замыкание поля K;

$\mathrm{char}\ K$ — характеристика поля K (обычно $\mathrm{char}\ K \neq 2$);

$\mathrm{Gal}(K/k)$ — группа Галуа — группа автоморфизмов расширения Галуа K/k;

C или $\mathcal{C}$ — кривая, обычно заданная афинным уравнением $y^2 = f(x)$ или $Y^2 = F(X)$;

$K[C]$ — координатное кольцо кривой C над полем K;

$K(C)$ — поле функций кривой C (поле частных кольца $K[C]$);

$L = K(x)(\sqrt{f})$ — гиперэллиптическое поле — поле функций кривой $C : y^2 = f(x)$;

g — род кривой C или гиперэллиптического поля L;

i, j — целые индексы, обычно неотрицательные;

n, m, n_j, m_j — целые числа;

b, b_j — коэффициенты из поля K или числители непрерывной дроби обобщенного типа;

h, h_j — многочлены из кольца $K[x]$, обычно неприводимые в $K[x]$;

v, v_h — нормирования поля $K(x)$ или гиперэллиптического поля L;

$\overline{K(x)}_h$ — пополнение поля $K(x)$ относительно нормирования v_h;

v_h^-, v_h^+— нормирования гиперэллиптического поля L;

v_∞ — бесконечное нормирование поля $K[x]$ или гиперэллиптического поля L в случае одной точки “на бесконечности”;

v_∞^-, v_∞^+ — бесконечные нормирования поля L в случае двух точек “на бесконечности”;

$\mathcal{V}$ или $\mathcal{V}_L$ — множество нормирований гиперэллиптического поля L;

S, S_j — конечные подмножества $\mathcal{V}_L$;

$\omega, \omega_1, \omega_2$ — многочлены из кольца $K[x]$;

$\gcd(\omega_1,\ \omega_2) = \omega$ — наибольший общий делитель многочленов ω_1, ω_2; в такой записи считаем, что многочлен ω имеет единичный старший коэффициент;

$\gcd(\omega_1,\ \omega_2) \in K^*$ — условие взаимной простоты многочленов $\omega_1, \omega_2 \in K[x]$;

Σ или Σ_h — кольцо вычетов по модулю неприводимого многочлена $h \in K[x]$ или множество представителей этого кольца;
$K((x)), K((1/x)), \Sigma((h))$ — поля формальных степенных рядов;
α, β — элементы гиперэллиптического поля L или поля формальных степенных рядов $K((x))$, $K((1/x))$ или $\Sigma((h))$;
α_j, β_j — полные частные (функциональной) непрерывной дроби или функциональной непрерывной дроби обобщенного типа;
a_j — неполные частные (функциональной) непрерывной дроби или знаменатели функциональной непрерывной дроби обобщенного типа;
p_j, q_j — континуанты (функциональной) непрерывной дроби;
$(h)_\circ$ — дивизор нулей многочлена $h \in K[x]$ или плейс конечного нормирования $v_h \in \mathcal{V}$;
$(\alpha)_\circ$ — дивизор нулей функции $\alpha \in L$;
$(h)_\circ^-$, $(h)_\circ^+$ — дивизоры нулей, соответствующие нормированиям $v_h^-, v_h^+ \in \mathcal{V}$ или плейсы конечных нормирований $v_h^-, v_h^+ \in \mathcal{V}$;
∞, ∞^+, ∞^- — точки "на бесконечности" или соответствующие дивизоры;
$(h)_\infty$ — дивизор полюсов многочлена $h \in K[x]$;
$(\alpha)_\infty$ — дивизор полюсов функции $\alpha \in L$;
$(\alpha) = (\alpha)_\circ - (\alpha)_\infty$ — дивизор функции $\alpha \in L$;
Div_K — множество дивизоров, определенных над полем K (K-дивизоров);
Div_K° — множество дивизоров степени ноль, определенных над полем K;
D, D_j — дивизоры;
P, P_j — точки кривой C;
$\mathrm{Supp}\, D$ — носитель дивизора D;
$v_h(D)$, $v_h^-(D)$, $v_h^+(D)$ — кратность соответствующего плейса $(h)_\circ$, $(h)_\circ^-$, $(h)_\circ^+$ в дивизоре D;
$v_P(D)$ — кратность точки P в дивизоре D;
Princ_K — множество главных дивизоров, определенных над полем K;
Δ°, $\Delta^\circ(L)$ — группа классов дивизоров степени 0 гиперэллиптического поля L;
$\Delta_C^\circ(K)$ — группа классов K-дивизоров степени 0 кривой C;
$[D]$ — класс дивизора D в группе классов дивизоров Δ°;
$\mathrm{Ord}(D)$ — порядок класса дивизора D в группе классов дивизоров $\Delta^\circ(L)$.

В формулах часто опускаются аргументы функций, когда понятно, как их восстановить. Иногда мы не упоминаем, какие промежутки пробегают индексы i и j, когда это ясно из контекста. Всюду считаем, что сумма по пустому множеству индексов равна нулю, а произведение по пустому множеству индексов равно 1, то есть, например, при $n = 0$ справедливо $b_1 + \ldots + b_n = 0$, $b_1 \cdot \ldots \cdot b_n = 1$.

Глава 1. Введение

1.1. Общая характеристика работы

1.1.1. Объект и предмет исследования

В диссертации исследуется строение и свойства гиперэллиптических кривых и гиперэллиптических полей, а также связанных с ними теоретико-числовых, алгебраических и геометрических объектов таких, как функциональные непрерывные дроби, функциональные аналоги уравнений Пелля, фундаментальные единицы и S-единицы, якобиевы многообразия, группы классов дивизоров и их подгруппы кручения. Отдельное внимание уделяется исследованию связей и зависимостей между этими объектами и их ключевыми свойствами. Приведенные объекты рассматриваются как над произвольными полями K характеристики, отличной от 2, так и в отдельных случаях над полем рациональных чисел $\mathbb{Q}$ или над полями алгебраических чисел, являющимися конечными расширениями поля $\mathbb{Q}$.

1.1.2. Методы исследования

В работе используются как традиционные методы алгебраической теории чисел, классических направлений алгебры и арифметической геометрии, так и возникшие недавно (в том числе в работах автора) новые арифметические методы из теории функциональных непрерывных дробей, теории единиц колец целых или S-целых элементов гиперэллиптических полей, теории дивизоров гиперэллиптических кривых. Ряд результатов получен с использованием систем компьютерной алгебры и символьных компьютерных вычислений.

1.1.3. Теоретическая и практическая ценность

Диссертация носит теоретический характер. Ее результаты могут быть использованы в таких теоретических разделах математики, как алгебраическая теория чисел, диофантова геометрия и арифметическая геометрия. Также результаты диссертации могут быть использованы в области защиты информации и в системах компьютерной алгебры.

1.1.4. Степень достоверности и апробации результатов

Достоверность всех результатов исследований обоснована строгими математическими доказательствами.

Результаты диссертации многократно докладывались на научных семинарах, в частности, на семинарах отдела теоретической и прикладной алгебры и теории чисел НИИСИ РАН под руководством академика РАН В.П. Платонова; на научно-исследовательском семинаре кафедры математических и компьютерных методов анализа (под руководством профессора В.Н. Чубарикова), на научно-исследовательском семинаре кафедры высшей алгебры (под руководством профессора В.А. Аратамонова, профессора В.Н. Латышева) на научно-исследовательском семинаре "Узлы и теория представлений" (под руководством профессора О.В. Мантурова, доцента И.М. Никонова) механико-математического факультета МГУ имени М.В. Ломоносова; на отчетных семинарах научного центра информационных технологий и искусственного интеллекта Университета Сириус.

Результаты диссертации были доложены на международных и всероссийских научных конференциях, среди которых: VII-XXII Международная конференция «Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории» в 2010-2023 гг. в г. Тула, г. Саратов, г. Волгоград; I-IV Конференция памяти А. А. Карацубы по теории чисел и приложениям в 2014-2017 гг. в г. Москва; Международная научная конференция «Современные проблемы математики и механики», посвященная 80-летию академика В. А. Садовничего в 2019 году в г. Москва; Международная конференция «Аналитическая теория чисел», посвященная 75-летию Г.И. Архипова и С.М. Воронина в 2020 году в г. Москва; III-IV Конференция математических центров России в 2023-2024 году в г. Майкоп и в г. Санкт-Петербург; Конференция "Современные проблемы теории чисел" в 2024 году в пгт. Сириус и др.

Работа выполнена при частичной поддержке РНФ, проект №22-71-00101, проект №19-71-00029 (разделы 3.3, 4.3, 5.3, 5.4).

1.1.5. Цели и задачи диссертации

Главными целями диссертации являются следующие:

1. нахождение точных оценок длин периодов функциональных непрерывных дробей элементов гиперэллиптического поля, определенного над полем алгебраических чисел;

2. решение проблемы классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условием, что поле L определено над полем рациональных чисел;

3. решение проблемы классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условиями, что поле L определено над квадратичным расширением поля рациональных чисел, а соответствующая эллиптическая кривая входит в рациональную параметризацию модулярными кривыми;

4. разработка теории функциональных непрерывных дробей обобщенного типа, построенных по нормированию первой степени, доказательство критерия периодичности и нахождение эффективного алгоритма поиска и построения соответствующих фундаментальных S-единиц;

5. разработка теории функциональных непрерывных дробей обобщенного типа, построенных по двум несопряженным линейным нормированиям, доказательство критерия периодичности и нахождение эффективного алгоритма поиска и построения соответствующих фундаментальных S-единиц;

6. разработка теории функциональных непрерывных дробей обобщенного типа, построенных по нормированию второй степени, доказательство критерия периодичности и нахождение эффективного алгоритма поиска и построения соответствующих фундаментальных S-единиц.

1.1.6. Научная новизна

Все основные результаты диссертации являются новыми и получены автором самостоятельно.

Некоторые результаты диссертации опубликованы в статьях, написанных в соавторстве с научным консультантом В.П. Платоновым в ходе тесной нераздельной совместной работы (разделы 3.2, 4.1, 4.2, 5.2). Эти совместные результаты важны и имеют принципиальный характер для диссертации.

Основные результаты состоят в следующем:

1. найдены точные оценки на длины периодов функциональных непрерывных дробей элементов гиперэллиптического поля, определенного над полем алгебраических чисел;

2. решена проблема классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условием, что поле L определено над полем рациональных чисел;

3. решена проблема классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условиями, что поле L определено над квад-

ратичным расширением поля рациональных чисел, а соответствующая эллиптическая кривая входит в рациональную параметризацию модулярными кривыми;

4. разработана теория функциональных непрерывных дробей обобщенного типа для нормирования первой степени, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

5. разработана теория функциональных непрерывных дробей обобщенного типа для двух несопряженных линейных нормирований, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

6. разработана теория функциональных непрерывных дробей обобщенного типа для нормирования второй степени, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S.

1.1.7. Положения, выносимые на защиту

По результатам исследований на защиту выносятся следующие положения и утверждения:

1. точные оценки на длины периодов функциональных непрерывных дробей элементов гиперэллиптического поля, определенного над полем алгебраических чисел;

2. решение проблемы классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условием, что поле L определено над полем рациональных чисел;

3. решение проблемы классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условиями, что поле L определено над квадратичным расширением поля рациональных чисел, а соответствующая эллиптическая кривая входит в рациональную параметризацию модулярными кривыми;

4. теория функциональных непрерывных дробей обобщенного типа для нормирования первой степени, критерий периодичности функциональных непрерывных дробей обобщенного типа и эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

5. теория функциональных непрерывных дробей обобщенного типа для двух несопряженных линейных нормирований, критерий периодичности функциональных непрерывных дробей обобщенного типа и эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

6. теория функциональных непрерывных дробей обобщенного типа для нормирования второй степени, критерий периодичности функциональных непрерывных дробей обобщенного типа и эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S.

1.1.8. Публикации

Основные результаты диссертации опубликованы в 20 работах автора: [1—20]. Все указанные работы опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5 — «Математическая логика, алгебра, теория чисел и дискретная математика» и входящих в базы цитирования RSCI, Scopus, Web of Science.

1.1.9. Структура и объем работы

Диссертация состоит из введения и пяти глав. Главы разбиты на разделы, а разделы на подразделы — параграфы. Текст диссертации изложен на 298 страницах. Список литературы содержит 187 наименований. Порядок библиографии соответствует упоминанию публикаций в тексте. Нумерация утверждений, формул и замечаний подчинена нумерации глав, разбиению глав на разделы и разделов на параграфы. Номера следствий подчинены теоремам. Номера теорем во введении соответствуют нумерации в тексте диссертации.

1.2. Научные проблемы диссертации и степень их разработанности

Тематика диссертации лежит на стыке таких областей математики как теория чисел, алгебра и алгебраическая геометрия. Исследования выполнены в рамках научной школы академика РАН В.П. Платонова.

Одним из наиболее интересных и изученных направлений арифметической (диофантовой) геометрии [21; 22] является теория алгебраических кривых $C = \{(x, y) \in K \times K \mid F(x, y) = 0\}$, где $F(x, y) \in K[x, y]$ — неприводимый многочлен от двух переменных над полем K. Наши усилия сконцентрированы в первую очередь на алгебраическом и теоретико-числовом подходах изучения свойств алгебраических кривых и их полей функций над алгебраически незамкнутыми полями K. Алгебраический подход берет свое начало с работ Р. Дедекинда и Л.

Кронекера 19 века (над полем комплексных чисел $\mathbb{C}$), а далее продолжен в начале 20-го века в работах Х. Хассе, Ф.К. Шмидта и А. Вейля (подробнее см. в книках К. Шевалле [23] и М. Дойринг [24]). Теоретико-числовой подход и связь с алгебраической теорией чисел представлен, например, в работах Э. Артина [25] и М. Эйхлера [26]. Современное изложение этих подходов представлено, например, в книгах И.Р. Шафаревича [27] и Х. Стихтенота [28].

Важным аспектом наших исследований является применение для объектов в полях алгебраических функций теоретико-числовых конструкций или построение их аналогов в функциональном случае. Среди таких конструкций можно отметить теорию непрерывных дробей, решение норменных уравнений и уравнений типа Пелля, поиск единиц и S-единиц колец целых элементов, применение арифметики дивизоров.

Вдохновение к применению теоретико-числовых методов к алгебраическим и геометрическим задачам исходит от классических работ Н. Абеля и П.Л. Чебышева, в которых впервые была отмечена удивительная связь между такими фундаментальными проблемами, как проблема периодичности функциональных непрерывных дробей, проблема кручения в якобианах гиперэллиптических кривых, проблема решения норменных уравнений и уравнений типа Пелля в функциональном случае.

В.П. Платонов в ключе рассмотрения этих трех проблем предложил ряд новых основополагающих идей, позволяющих не только установить тесную связь между этими проблемами, но и выделить новую самостоятельную область исследований, лежащую на границе теории чисел, алгебры, и геометрии. Важную роль в новом подходе, предложенном В.П. Платоновым, играют алгебраические и теоретико-числовые методы исследования фундаментальных единиц и S-единиц колец целых и S-целых элементов в гиперэллиптических полях (полях функций гиперэллиптических кривых). Тем самым, к указанным трем проблемам добавляется еще одна — проблема поиска и построения фундаментальных единиц и S-единиц в гиперэллиптических полях.

Эллиптическим кривым посвящено огромное количество книг и статей, в которых получены впечатляющие результаты, в том числе имеющие важнейшее прикладное значение в современном “цифровом мире”. Однако остаются и множество нерешенных задач. Ряд результатов, представленных в этой диссертации, также относится к разделу исследований эллиптических кривых и связанных с ними объектов (см., например, Главу 4).

Для кривых рода 2 и выше значительно меньше качественных результатов по сравнению с эллиптическими кривыми. Среди таких результатов можно, например, отметить знаменитую гипотезу Л. Морделла [29], доказанную в 1983 году Г. Фалтингсом [30]. Теорема Фалтингса утверждает, что на кривых C рода 2 и выше, определенных над полями алгебраических чисел K, может содержаться только конечное число K-точек. Но эта теорема неэффективна в том смысле, что не дает алгоритм, позволяющий найти все K-точки на кривой C. В рассмат-

риваемых нами проблемах мы также сталкиваемся с подобным разделением качественных и количественных результатов (см., например, §§3.3.3-3.3.6 диссертации).

В последние 30 лет с ростом возможностей вычислительной техники количественные результаты вышли на новый уровень, что не только взвинтило интерес к рассматриваемым проблемам, но и привело к существенному развитию теоретико-числовых методов компьютерной алгебры. В связи с этим академик В.П. Платонов отмечает, что "естественное соединение глубокой теории, математических алгоритмов, софтверной реализации и супервычислений будет играть все большую роль в математике 21 века". Отметим, что часть результатов диссертации, несмотря на свой фундаментальный теоретический характер, были бы невозможны без применения высокопроизводительных компьютерных вычислений (см., например, Главу 4 диссертации).

Путь A — абелево многообразие размерности g над полем алгебраических чисел K. Теорема Мордела-Вейля [31; 32] утверждает, что множество K-точек $A(K)$ многообразия A является конечно порожденной абелевой группой. По теореме о классификации конечнопорожденных абелевых групп группа $A(K)$ изоморфна прямому произведению свободной абелевой группы ранга r и $A(K)_{tors}$ — группы кручения K-точек многообразия A: $A(K) \simeq \mathbb{Z}^r \times A(K)_{tors}$. Естественным образом возникают две глобальные проблемы: проблема полного перечисления конечных групп, реализуемых как группа кручения $A(K)_{tors}$ многообразия A над полями алгебраических чисел K, и проблема полного описания многообразий A над полями алгебраических чисел K, реализующих данную группу кручения $A(K)_{tors}$.

В качестве абелевых многообразий в диссертации в первую очередь рассматриваются якобиевы многообразия (якобианы) $J(C)$ неособых алгебраических кривых C рода g. Проблема ограниченности подгрупп кручения (проблема кручения) в якобианах гиперэллиптических кривых рода g над полем рациональных чисел $\mathbb{Q}$ является одной из фундаментальных проблем теории чисел и алгебраической геометрии. Ее важность для современной математики подчеркивается колоссальным множеством работ, появившихся в этой области с начала XX века. В последнее время с появлением новых теоретико-числовых методов исследования, в том числе с использованием компьютерных вычислений, эта проблема получила особую актуальность. Проблему кручения в якобианах гиперэллиптических кривых над полем рациональных чисел можно разделить на две проблемы: проблема об оценке и описания подгрупп кручения якобианов кривых данного рода g и проблема нахождения порядков точек кручения.

Для эллиптических кривых E якобиан изоморфен самой кривой. В этом случае проблема кручения над полем рациональных чисел была полностью решена Б. Мазуром [33; 34] в 1978 году, а именно было доказано, что порядок m $\mathbb{Q}$-точки кручения может принимать одно из значений $1 \leq m \leq 10$, $m = 12$. Более того, были выписаны все 15 групп, которые могут быть

реализованы как подгруппы кручения $E(\mathbb{Q})_{tors}$ эллиптических кривых над полем $\mathbb{Q}$. В дальнейшем исследования подгрупп кручения эллиптических кривых были активно продолжены над полями алгебраических чисел K небольшой степени [35—40]. Эти результаты нашли применение для исследования функциональных непрерывных дробей элементов эллиптических полей и связанных с ними проблем (подробнее см. в Главе 4 диссертации).

В связи с отсутствием глобальных подходов основные усилия специалистов в этой области были направлены на решение проблемы кручения для кривых с фиксированным родом $g = 2, 3, 4$. Надо отметить, что результаты, полученные в этом направлении за последнее время, заключались в поиске кривых, якобианы которых обладают точками кручения определенного порядка. Более того, они имели частный характер и опирались на специфические свойства конкретных кривых [41].

В.П. Платонов предложил в этом направлении три новых метода, которые, в частности, позволили существенно продвинуться в поиске кривых, якобианы которых обладают точками кручения высоких порядков. Первый метод базируется на применении и исследовании теории ганкелевых матриц. Второй метод базируется на свойствах функциональных непрерывных дробей. Наконец, в основе третьего метода лежат свойства фундаментальных S-единиц и связанных с ними функциональных уравнений типа Пелля.

В рамках диссертации мы продолжаем эти исследования и предлагаем новые подходы к указанным проблемам, основанные на теории функциональных непрерывных дробей (см. Главы 3, 4 диссертации), развитом анализе дивизоров, а также на арифметике дивизоров с использованием представления Мамфорда и функциональных непрерывных дробей обобщенного типа (см. Главу 5 диссертации).

1.3. Масштаб и актуальность рассматриваемых проблем

Для мирового математического сообщества многие годы остается недоступным решение проблемы кручения в якобиевых многообразиях гиперэллиптических кривых над полем рациональных чисел и над полями алгебраических чисел. Эту проблему можно отнести к важнейшим фундаментальным проблемам теории чисел и алгебраической геометрии.

Проблема существования и поиска фундаментальных единиц в гиперэллиптических полях, проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел, проблема периодичности разложения в функциональную непрерывную дробь элементов гиперэллиптических полей относятся к числу важных и трудных проблем современной математики. Они находятся на стыке таких актуальных и глубоких областей математики, как алгебраическая теория чисел, арифметическая геометрия, диофантова геометрия. В настоящий момент нет единого подхода, который мог бы приблизить к решению этих проблем,

и каждое продвижение дается с большим трудом. Полное решение указанных проблем невозможно без построения эффективных алгоритмов и высокопроизводительных компьютерных вычислений.

В последнее время рассматриваемые проблемы получили особую практическую актуальность в связи с активным развитием компьютерной техники, цифровых технологий, высокопроизводительных вычислительных систем, новых криптографических протоколов, интеллектуальных систем защиты информации. Основанием рассматриваемой тематики можно считать классические работы Н. Абеля и П.Л. Чебышева. В этих работах была обнаружена связь функциональных непрерывных дробей с так называемыми эллиптическими интегралами. Благодаря указанным работам и работам К. Якоби [42; 43] был открыт якобиан кривой, построено отображение Абеля-Якоби кривой в ее якобиан, а также была осознана важность подгруппы кручения в якобиане. В дальнейшем фундаментальные результаты были получены в работах Дж. Тейта [44], П. Делиня [45], Ж.-П. Серра [46], Г. Фалтингса [47], Д. Мамфорда [48], Д. Кантора [49], Дж. Игузы [50] и др. Среди современных исследований можно отметить значительные достижения научной школы академика В.П. Платонова, а также работы таких авторов как У. Занье [51; 52], Н. Элкиса [53], Э. Флина [54], Ф. Лепрево [55—58], Х. Огава [59], Б. Пунен [60], В. Адамс и М. Разар [61], Т. Берри [62—64], А. Штейн [65; 66], М. Садек [67], А. Пуртен [68—71] и др. Каждый год представляются к защите PhD диссертации на близкие темы (для примера, З. Шерр [72], Мичиганский университет, 2013 г.; М. Кронберг [73], Университет Ольденбурга, 2015 г.; К. Доусуд [74], Университет штата Орегон, 2015 г.; О. Мерсерт [75], Высшая нормальная школа (Пиза), 2016 г.; Ф. Малаголи [76], Пизанский университет, 2017 г.; М.М. Петрунин [77], НИИСИ РАН, 2019 г.; В. Арул [78], Массачусетский технологический институт, 2020 г.; Д. Ричман [79], Мичиганский университет, 2020; Н.А. Каладжиева [80], Университетский колледж Лондона, 2020 г.; С.А. Линднер [81], Университет Калгари, 2020 г.; Т. Гузвич [82], Загребский университет, 2021 г.; С. Добсон [83], Оклендский университет, 2022 г.; С. Ноуэлл [84], Университетский колледж Лондона, 2022 г.; Х. Грин [85], Университетский колледж Лондона, 2023 г.).

Проблема ограниченности подгрупп кручения в якобианах гиперэллиптических кривых над полем $\mathbb{Q}$ остается открытой уже более 40 лет даже для кривых рода 2. За это время не было найдено существенных идей для решения этой проблемы в общем виде. Усилиями целого ряда математиков было доказано существование гиперэллиптических кривых рода 2, в якобианах которых есть $\mathbb{Q}$-точки порядка m, $1 \leq m \leq 30$, $m \in \{32, 33, 34, 35, 36, 39, 40, 45, 48, 60, 63, 70\}$. Эти точки были получены с использованием различных методов, индивидуальных для отдельных порядков.

В 2012 году новый метод В.П. Платонова [86] позволил завершить доказательство гипотезы о существовании $\mathbb{Q}$-точек порядков m, $m \leq 30$, в якобианах различных гиперэллип-

тических кривых рода 2. Ранее для кривых C рода $g = 2$ М. Столлом [87] был предложен p-адический алгоритм вычисления подгруппы кручения $J(\mathbb{Q})_{tors}$, который в дальнейшем был расширен для кривых рода 3 [88; 89].

Долгое время не удавалось найти кривые рода 2 над полем $\mathbb{Q}$, якобиан которых содержит $\mathbb{Q}$-точку порядка 28 [90]. Первая такая кривая была найдена в 2012 году В.П. Платоновым и М.М. Петруниным [91], тем самым было завершено доказательство вышеупомянутой гипотезы [92] о том, что для всякого $m \leq 30$ существует кривая рода 2 над полем $\mathbb{Q}$ рациональных чисел, якобиан которой содержит $\mathbb{Q}$-точку порядка m. В дальнейшем научная группа под руководством академика В.П. Платонова нашла другие примеры кривых рода 2 над полем $\mathbb{Q}$, якобиан которых содержит $\mathbb{Q}$-точки порядка 28 и других высоких порядков [93]. В 2018 году В.П. Платонов и Г.В. Федоров нашли бесконечное семейство неизоморфных гиперэллиптических кривых рода 2 над полем $\mathbb{Q}$, якобиевы многообразия которых содержат $\mathbb{Q}$-точки порядка 28.

На данный момент известны различные гиперэллиптические кривые рода 2, якобианы которых обладают $\mathbb{Q}$-точками кручения всех простых порядков вплоть до 29, причем для порядка $m = 29$ с точностью до изоморфизма до сих пор известна только одна такая кривая.

В работе К. Николса [94] приведено актуальное состояние множества известных реализуемых порядков кручения в якобианах гиперэллиптических кривых рода 2, 3, 4 над полем рациональных чисел. Среди указанных примеров якобиевых многообразий выделяются абсолютно простые, поскольку они не могут быть получены путем спаривания эллиптических кривых [95].

Основой алгебраического подхода к фундаментальной проблеме кручения в якобианах гиперэллиптических кривых является глубокая связь между нетривиальными S-единицами гиперэллиптического поля и точками конечного порядка в якобиане гиперэллиптической кривой [96]. В свою очередь, проблема поиска и построения нетривиальных S-единиц гиперэллиптического поля тесно связана с проблемой периодичности функциональных непрерывных дробей, в которые могут разлагаться элементы гиперэллиптического поля. В.П. Платонов высказал две гипотезы. Первая утверждает, что степень фундаментальной единицы в гиперэллиптических полях данного рода над полем рациональных чисел ограничена. Вторая гипотеза является обобщением первой и утверждает, что степень фундаментальных S-единиц в гиперэллиптических полях данного рода над полем рациональных чисел ограничена. Обе эти гипотезы являются трудными и глубокими.

Сформулированные проблемы важны и актуальны в мировом научном пространстве. В последние годы рассматриваемые задачи вызывают живой интерес у ведущих специалистов в современных областях математики в связи с развитием новых теоретико-числовых, алгебро-геометрических и вычислительных подходов к их решению. Результаты теоретиче-

ских и практических исследований могут быть использованы в криптографии [97—100]: при создании новых криптографических протоколов [101—103], в вопросах исследования стойкости существующих криптосистем (например, атака Винера [104], ро-алгоритм Полларда [105], алгоритм Гельфонда — Шенкса [106; 107], алгоритм индексного исчисления для абелевых многообразий [108; 109]), в теории кодирования [110; 111] для анализа псевдослучайных последовательностей [112] и в других разделах интеллектуальной защиты информации.

1.4. Краткое введение в тематику диссертации

Интерес к изучению функциональных непрерывных дробей возник еще в 19 веке. Но с развитием междисциплинарного подхода, компьютерных вычислений и нового взгляда на проблему кручения в якобианах гиперэллиптических кривых, в 21 веке теория функциональных непрерывных дробей стала мощным инструментом в проблеме поиска фундаментальных единиц и в проблеме поиска фундаментальных S-единиц в гиперэллиптических полях [61; 113; 114].

Теория числовых непрерывных дробей (цепных дробей) насчитывает многовековую историю. Одним из центральных утверждений этой теории является теорема Эйлера-Лагранжа о периодичности непрерывной дроби для любой числовой квадратичной иррациональности [115]. Основная идея [116] перехода от числовых к функциональным непрерывным дробям заключается в рассмотрении вместо кольца целых чисел — кольца многочленов $K[x]$, а вместо целой части действительного числа — целой части разложения функции в формальный степенной ряд из $K((1/x))$ [117]. В работе В. Шмидта [118] доказаны в функциональном случае аналоги теоремы Эйлера-Лагранжа о периодичности непрерывной дроби и известной в теории диофантовых приближений теоремы Серре [119] об эквивалентности иррациональных чисел.

Как известно, числовые непрерывные дроби имеют применение во многих разделах математики, таких как элементарная теория чисел, теория диофантовых приближений, теория трансцендентных чисел, геометрия фракталов, эргодическая теория, теория динамических систем, теория формальных языков, компьютерные науки. Одно из важнейших свойств числовых непрерывных дробей заключается в том, что они обеспечивают наилучшие приближения действительного числа рациональными дробями, сохраняя при этом достаточно простую алгебраическую и геометрическую структуру. В этом ключе теория непрерывных дробей получила развитие в работах А. Коркина и Г. Золотарева [120], А. Гурвица [121], Дж. В.С. Касселса [122]. В настоящее время остаются множество открытых проблем в области числовых непрерывных дробей и их приложений, а исследования по ним остаются актуальными и востребованными (см. работы О.Н. Германа [123], В.А. Быковского и Д.А. Фроленкова [124],

Н.М. Добровольского и Н.Н. Добровольского [125; 126] и др.)

Античные математики умели искать достаточно хорошие приближения к несоизмеримым величинам в виде последовательных отношений целых чисел, предвосхищая теорию наилучших приближений. Тесная связь алгоритма Евклида и числовых непрерывных дробей (цепных дробей) позволяет полагать, что применение подходящих дробей в том или ином виде началось более двух тысяч лет назад. За это время возникло огромное количество прикладных задач, которые решались с помощью приближения подходящими дробями, полученными путем разложения различных величин в непрерывные дроби. Несмотря на столь широкий интерес, на протяжении многих веков, остается масса открытых и актуальных вопросов, связанных с числовыми непрерывными дробями и их многочисленными обобщениями.

Алгоритм Евклида является одним из старейших численных алгоритмов, которые находят активное применение в современной математике. Алгоритм Евклида работает в евклидовых кольцах, в частности, в кольце целых чисел $\mathbb{Z}$ и кольце многочленов $K[X]$ над произвольным полем K. Поэтому естественным является разложение рациональной функции в конечную *функциональную непрерывную дробь* с многочленами в качестве неполных частных. Для всевозможных $a_0 \in K[X]$, $a_1, a_2, \ldots \in K[X] \setminus K$ множество всех функциональных непрерывных дробей (конечных и бесконечных) вида

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \tag{1.4.0.1}$$

образует поле, изоморфное полю формальных степенных рядов $K((1/X))$. Если поле L может быть вложено в поле $K((1/X))$, то можно говорить о разложении элементов поля L в функциональные непрерывные дроби. В частности, поле рациональных функций $K(X)$ является подполем $K((1/X))$, а его элементы (и только они) раскладываются в конечные функциональные непрерывные дроби.

Многие результаты, полученные для числовых непрерывных дробей, могут быть частично или полностью перенесены на случай функциональных непрерывных дробей, причем подход, а иногда и результат, будет сильно зависеть от базового поля K, над которым рассматриваются функциональные непрерывные дроби. Так, например, над конечными полями или над полями алгебраических чисел аналоги результатов для числовых непрерывных дробей могут иметь совершенно разные формулировки, причем для функциональных непрерывных дробей над конечным полем формулировка обычно ближе к оригинальной формулировке для числовых непрерывных дробей.

Функциональные непрерывные дроби возникли в 18 веке в очень интересном контексте, а именно в связи с задачей о выражении эллиптических интегралов через элементарные функции. В работах Н. Абеля [127] и П.Л. Чебышева [128; 129] были получены следующие резуль-

таты. Пусть $F \in \mathbb{Q}(X)$ — многочлен четной степени $2s$, не являющийся полным квадратом в $\mathbb{Q}(X)$, и с единичным старшим коэффициентом. Если существует нетривиальное решение $\omega_1, \omega_2 \in \mathbb{Q}[X]$ функционального аналога уравнения Пелля $\omega_1^2 - \omega_2^2 F = b$, $b \in \mathbb{Q}$, $b \neq 0$, то имеем $P(X) = \omega_1'/\omega_2 \in \mathbb{Q}[X]$, $\deg P = s - 1$, и

$$\int \frac{P(X)}{\sqrt{F(X)}} \mathrm{d}X = \log\bigl(\omega_1 + \omega_2\sqrt{F}\bigr) + \mathrm{Const}\,. \tag{1.4.0.2}$$

Верно и обратное утверждение: если известно, что интеграл в левой части (1.4.0.2) выражается в элементарных функциях, то существует многочлен $P \in \mathbb{Q}[X]$, $\deg P = s-1$, и многочлены $\omega_1, \omega_2 \in \mathbb{Q}[X]$, которые являются решением функционального уравнения Пелля и выполнено соотношение (1.4.0.2). Н. Абелем было доказано, что существование нетривиального решения функционального уравнения Пелля эквивалентно периодичности разложения элемента $\sqrt{F}$ в функциональную непрерывную дробь. Кроме того, фактически была указана связь между периодичностью функциональной непрерывной дроби элемента $\sqrt{F}$ и точками кручения в якобиане гиперэллиптической кривой, заданной уравнением $Y^2 = F(X)$.

Пусть K — поле характеристики отличной от 2. Рассмотрим $L = K(X)(\sqrt{F})$ — *гиперэллиптическое поле*, построенное по свободному от квадратов многочлену $F \in K[X]$ четной степени и со старшим коэффициентом $\mathrm{lc}\,(F)$, являющимся полным квадратом в поле K. Тогда $\sqrt{F} \in K((1/X))$, а, следовательно, можно считать, что $L \subset K((1/X))$, и любой элемент $\alpha \in L$ может быть разложен в функциональную непрерывную дробь вида (1.4.0.1).

Для функциональных непрерывных дробей можно рассматривать вместо свойства периодичности свойство квазипериодичности — периодичности с точностью до умножения на ненулевой постоянный множитель из поля K. Более точно, функциональная непрерывная дробь элемента $\alpha \in K((1/X))$ называется *квазипериодической*, если найдутся некоторые два ее полных частных α_n и α_m, которые связаны соотношением $\alpha_n = c\alpha_m$ для некоторой ненулевой постоянной $c \in K^*$. *Длиной квазипериода* называется значение минимальной разности $n - m$ для целых n и m таких, что $n > m$, $\alpha_n = c\alpha_m$, $c \in K^*$. Постоянная c называется *константой квазипериода*. Если функциональная непрерывная дробь элемента $\alpha \in K((1/X))$ квазипериодическая с нечетной длиной периода или, если константа квазипериода $c \in K^*$ имеет конечный порядок (т. е. существует минимальное $r \in \mathbb{N}$ такое, что $c^r = 1$), то функциональная непрерывная дробь элемента α периодическая, но длина периода может кратно отличаться от длины квазипериода (подробнее о квазипериодах и связи с периодами см. §§3.1.6-3.1.7 диссертации). В примере 3.2.3.5 диссертации указан элемент, обладающий квазипериодической, но не периодической непрерывной дробью.

Для построения числовой непрерывной дроби иррационального числа ключевой операцией является взятие целой части от очередного полного частного. Для определения аналога этой операции для функциональной непрерывной дроби, связанной с точкой P, или простым

идеалом (плейсом) $\mathcal{P}$, или нормированием v_P, необходимо наличие разложения в ряд Лорана в окрестности точки P или по нормированию v_P. В случае конечной точки P или конечного нормирования v_P функцию α нужно разложить в ряд по степеням $X - X_P$, а в случае бесконечной точки P или бесконечного нормирования v_P функцию α нужно разложить в ряд по степеням $1/X$. Тогда аналогом взятия целой части для функциональной непрерывной дроби является выделение в полученном ряде для α слагаемых с неположительными степенями $X - X_P$ или $1/X$ соответственно для конечного или бесконечного случая.

Бесконечное нормирование v_∞ поля $K(X)$ определяется следующим образом: $v_\infty(\omega_1/\omega_2) = \deg\omega_2 - \deg\omega_1$, где $\omega_1, \omega_2 \in K[X]$. Пополнение $\overline{K(X)}_\infty$ поля $K(X)$ относительно нормирования v_∞ изоморфно полю формальных степенных рядов $K((1/X))$, следовательно, нормирование v_∞ поля $K(X)$ продолжается на поле $K((1/X))$ единственным образом. Для $\alpha \in K((1/X))$ определим многочлен $a \in K[X]$ так, что $v_\infty(\alpha - a) > 0$. Обозначим $[\alpha]_\infty = a$. Тогда процесс построения функциональной непрерывной дроби элемента $\alpha \in K((1/X))$ можно формализовать следующим образом: положим $\alpha_0 = \alpha$, для $j \in \mathbb{N}_0$ последовательно определяем $a_j = [\alpha_j]_\infty$, $\alpha_{j+1} = 1/(\alpha_j - a_j)$ до тех пор, пока $\alpha_j \neq a_j$. В результате мы получим конечную или бесконечную функциональную непрерывную дробь $[a_0; a_1, a_2, \ldots]$ в поле $K((1/X))$ вида (1.4.0.1). Подходящие дроби функциональной непрерывной дроби $[a_0; a_1, a_2, \ldots]$ будут сходиться по нормированию v_∞ к элементу α, поэтому мы будем писать $\alpha = [a_0; a_1, a_2, \ldots]$ в поле $K((1/X))$ и говорить, что функциональная непрерывная дробь $[a_0; a_1, a_2, \ldots]$ построена по нормированию v_∞.

В поле $K(x)$ кроме бесконечного нормирования v_∞ существуют конечные нормирования v_h, связанные с неприводимыми многочленами $h \in K[x]$. *Конечное нормирование* v_h определяется следующим образом: $v_h(h^n\omega_1/\omega_2) = n$, где $n \in \mathbb{Z}$, $\omega_1, \omega_2 \in K[x]$, $h \nmid \omega_1$, $h \nmid \omega_2$.

Пусть $\deg h = 1$, тогда нормирование v_h будем называть *линейным*. Пополнение $\overline{K(x)}_h$ поля $K(x)$ относительно нормирования v_h изоморфно полю формальных степенных рядов $K((h))$, и, следовательно, нормирование v_h поля $K(x)$ продолжается на поле $K((h))$ единственным образом. Как и в случае бесконечного нормирования, для $\alpha \in K((h))$ определим многочлен $a \in K[1/h]$ так, что $v_h(\alpha - a) > 0$. Обозначим $[\alpha]_h = a$. Тогда процесс построения функциональной непрерывной дроби элемента $\alpha \in K((h))$ можно формализовать следующим образом: положим $\alpha_0 = \alpha$, для $j \in \mathbb{N}_0$ последовательно определяем $a_j = [\alpha_j]_h$, $\alpha_{j+1} = 1/(\alpha_j - a_j)$ до тех пор, пока $\alpha_j \neq a_j$. В результате мы получим конечную или бесконечную функциональную непрерывную дробь $[a_0; a_1, a_2, \ldots]$ в поле $K((h))$ вида (1.4.0.1). Подходящие дроби функциональной непрерывной дроби $[a_0; a_1, a_2, \ldots]$ будут сходиться по нормированию v_h к элементу α, поэтому мы будем писать $\alpha = [a_0; a_1, a_2, \ldots]$ в поле $K((h))$ и говорить, что функциональная непрерывная дробь $[a_0; a_1, a_2, \ldots]$ построена по нормированию v_h.

Для того, чтобы определить функциональную непрерывную дробь, построенную по нормированию v_h для $\deg h > 1$, обозначим $\Sigma = \Sigma_h$ множество всех многочленов из $K[x]$, степень которых меньше $\deg h$. Нормирование v_h поля $K(x)$ продолжается на множество формальных степенных рядов $\Sigma((h))$ единственным образом. Далее формальное построение функциональной непрерывной дроби по нормированию v_h аналогично построению по линейному нормированию с единственным отличием в том, что $a_j \in \Sigma[1/h]$, $j \in \mathbb{N}_0$.

Квадратичные расширения поля $K(X)$ имеют особый интерес с точки зрения непрерывных дробей, поскольку, как и в числовом случае, периодические функциональные непрерывные дроби в $K((1/X))$ или в $K((h))$, $\deg h = 1$, есть квадратичные иррациональности. Но в отличие от числового случая, обратное утверждение для функциональных непрерывных дробей неверно. Во-первых, не всякое квадратичное расширение $\mathcal{L}$ поля $K(X)$ вкладывается в $K((1/X))$ или в $K((h))$, поэтому для некоторых квадратичных иррациональностей мы просто не можем определить функциональную непрерывную дробь вида (1.4.0.1). Во-вторых, даже при условии, что есть вложение $\mathcal{L} = K(X)(\sqrt{F})$ в $K((1/X))$ или в $K((h))$, в общем случае не всякий элемент $\alpha \in \mathcal{L} \setminus K(x)$ имеет периодическое разложение в функциональную непрерывную дробь в $K((1/X))$ или в $K((h))$. Однако, бывают поля $\mathcal{L} = K(X)(\sqrt{F})$ такие, что для любого $\alpha \in \mathcal{L} \setminus K(X)$ разложение в функциональную непрерывную дробь периодическое. Например, таким полем является гиперэллиптическое поле $\mathcal{L} = \mathbb{F}_q(X)(\sqrt{F}) \subset \mathbb{F}_q((1/X))$ над конечным полем $\mathbb{F}_q$ из q элементов, где многочлен $F \in \mathbb{F}_q[X]$ четной степени, свободен от квадратов, и $\mathrm{lc}\,(F)$ является квадратичным вычетом в $\mathbb{F}_q$ [130].

Исследования по теории функциональных непрерывных дробей были начаты достаточно давно. Так, после работ Н. Абеля и П.Л. Чебышева теория функциональных непрерывных дробей в поле $K((1/x))$ получила существенные продвижения в работе Э. Артина [131] 100 лет назад. В дальнейшем развитию теории функциональных непрерывных дробей и ее приложениям была посвящена обширная литература. В XXI веке за счет развитого теоретико-числового и алгебро-геометрического аппарата теория функциональных непрерывных дробей находит новые неожиданные применения в различных областях математики. Сейчас теория функциональных непрерывных дробей является мощным инструментом в исследовании проблемы кручения в якобианах гиперэллиптических кривых и проблемы поиска фундаментальных S-единиц в гиперэллиптических полях, проблемах, лежащих на стыке различных областей математики.

1.5. Содержание работы

Диссертация посвящена исследованию четырех фундаментальных проблем алгебраической теории чисел и алгебраической геометрии, а также связи между ними: проблема кру-

чения в якобианах гиперэллиптических кривых, проблема периодичности функциональных непрерывных дробей, проблема решения норменных уравнений и уравнений типа Пелля в функциональном случае, проблема поиска и построения фундаментальных единиц и S-единиц в гиперэллиптических полях. Эти проблемы рассматриваются как над произвольными полями констант K, характеристики отличной от двух, так и в отдельных случаях над полями алгебраических чисел или над $\mathbb{Q}$.

Далее представим краткий обзор структуры и основных результатов диссертации. В каждой главе и в каждом разделе приведено более детальное описание полученных результатов, обзор основной литературы, посвященной рассматриваемой теме, и ссылки на статьи, где эти результаты были опубликованы.

Глава 1 является вводной, в ней содержится общая характеристика работы, представлено описание научных проблем диссертации, указан их масштаб и актуальность, приведены вводные и исторические сведения рассматриваемой тематики, а также описана структура и приведены основные результаты диссертации.

В Главе 2 дается краткое изложение необходимых базовых понятий и утверждений, которые используются в диссертации. Отметим, что по возможности изложение ведется на языке алгебры и алгебраической теории чисел, поскольку именно такой подход к указанным проблемам используется в диссертации. Наиболее важными являются §2.3.2 и §2.4.5, в которых дается введение в теорию нормирований и теорию дивизоров гиперэллиптических полей. В дальнейшем эти понятия используется на протяжении всей диссертации. Дополнительная литература к Главе 2: [132—138].

Глава 3 посвящена исследованию функциональных непрерывных дробей и их свойств таких, как периодичность и квазипериодичность (§3.1.6, §3.1.7, §3.2.1, §3.2.3), свойство наилучшего приближения (§3.1.8), связь с уравнениями типа Пелля (§3.1.8, §3.2.1, §3.2.2) и с нетривиальными единицами и S-единицами гиперэллиптического поля (§3.2.1, §3.3.3). Также в этой главе рассматриваются вопросы о строении функциональной непрерывной дроби: симметрии периодов и квазипериодов (§3.1.6, §3.1.7, §3.2.5), оценки на длины предпериодов, квазипериодов и периодов (§3.1.2, §§3.3.2-3.3.4). Основные результаты и утверждения снабжены показательными примерами и контрпримерами (§3.2.4, §3.2.5, §3.3.4). Исследования ведутся как элементарным методом, так и с помощью анализа дивизоров объектов, связанных с функциональными непрерывными дробями. Отдельное внимание заслуживают вычислительные приложения функциональных непрерывных дробей. Для поиска точек конечного порядка в якобиане гиперэллиптической кривой стандартной техникой является использование алгоритма Кантора (§2.4.6) и его обобщений [139]. В §3.2.4 для этой задачи предложены эффективные алгоритмы, основанные на применении функциональных непрерывных дробей (см. также §3.1.4).

Отдельно отметим раздел 3.3, в котором получены оценки сверху на длины периодов и квазипериодов функциональных непрерывных дробей произвольных элементов гиперэллиптического поля (см. теоремы 3.3.2.3, 3.3.2.4 и следствие 3.3.2.4). В теореме 3.3.3.3 и следствии 3.3.3.5 найдены точные оценки на длину периода и длину квазипериода непрерывной дроби для "ключевых" элементов вида $\sqrt{f}/x^s$ гиперэллиптического поля $L = K(x)(\sqrt{f})$, определенного над полем K алгебраических чисел.

Теорема (3.3.3.3)**.** *Пусть K — расширение поля рациональных чисел $\mathbb{Q}$ степени k. Пусть $f \in K[x]$ — свободный от квадратов многочлен, и в кольце целых элементов поля $\mathcal{L} = K(x)(\sqrt{f})$ есть фундаментальная единица $u = \Psi_1 + \Psi_2\sqrt{f}$ степени m, где $\Psi_1, \Psi_2 \in K[x]$. Пусть для $j \in \mathbb{N}$ многочлены $\Omega_1^{(j)}, \Omega_2^{(j)} \in K[x]$ определены соотношениями*

$$\Omega_1^{(j)} + \Omega_2^{(j)}\sqrt{f} = \left(\Psi_1 + \Psi_2\sqrt{f}\right)^j.$$

1. *Если хотя бы одно из значений $v_x(f), v_x(\Psi_1), v_x(\Psi_2)$ отлично от нуля, то непрерывная дробь элемента $\sqrt{f}/x^s$, построенная в $K((1/x))$, периодическая тогда и только тогда, когда*

$$-v_x(\Psi_1) - v_x(\Psi_2) \le s \le v_x(\Psi_1) + v_x(\Psi_2) + v_x(f).$$

   В случае периодичности непрерывной дроби $\sqrt{f}/x^s$, длина квазипериода N не превосходит $m - \delta$, где значение δ определено при некотором $f_1 \mid f$, $\deg f_1 < \deg f$,

$$\delta = \max\bigl(0, |g + 1 - s| - 1\bigr) + \max\bigl(0, |s + g + 1 - \deg f_1| - 1\bigr).$$

2. *Если $v_x(f) = v_x(\Psi_1) = v_x(\Psi_2) = 0$, то непрерывная дробь элемента $\sqrt{f}/x^s$, построенная в $K((1/x))$, периодическая тогда и только тогда, когда найдется такой номер n, что $v_x\left(\Omega_2^{(1)}\right) = \ldots = v_x\left(\Omega_2^{(n-1)}\right) = 0$, $|s| \le v_x\left(\Omega_2^{(n)}\right)$ и $\phi(n) \mid 2k$. В случае периодичности непрерывной дроби $\sqrt{f}/x^s$, длина квазипериода N не превосходит $nm - \delta$.*

Найденные оценки являются точными как в случае, когда гиперэллиптическое поле задается многочленом четной степени, так и в случае, когда гиперэллиптическое поле задается многочленом нечетной степени. Особенность четного случая заключается в том, что длина квазипериода может быть в несколько раз больше степени фундаментальной S-единицы (см. соответствующие примеры в §3.3.4). В связи с этим неожиданным свойством, в §3.3.6 доказано, что в каждом гиперэллиптическом поле, обладающим периодическими элементами, найдется такой элемент, длина периода которого больше любого наперед заданного числа. В §3.3.5 для гиперэллиптического поля L, определенного над полем K алгебраических чисел, доказана теорема 3.3.5.1 о конечности множества таких дискриминантов D, что найдется элемент $\alpha \in L$ с дискриминантом D, обладающий квазипериодическим разложением в непрерывную дробь. В §3.3.7 найденные результаты проиллюстрированы на случае, когда базовое поле K является квадратичным расширением поля $\mathbb{Q}$.

Глава 4 посвящена проблеме классификации эллиптических полей $L = K(x)(\sqrt{f})$ по признаку периодичности непрерывных дробей для ключевых элементов вида $\sqrt{f}/x^s$, $s \in \mathbb{Z}$. Проблема классификации впервые была поставлена академиком В.П. Платоновым в 2017 году. Наиболее важной и трудной в проблеме классификации является задача о поиске полей $L = K(x)(\sqrt{f})$, в которых элемент $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в поле формальных степенных рядов $K((x))$. Если рассматривать непрерывные дроби в поле формальных степенных рядов $K((1/x))$ и многочлены f четной степени, то этой задаче посвящено много работ .

Для случая поля формальных степенных рядов $K((x))$ сначала различными методами удавалось найти только примеры полей $L = K(x)(\sqrt{f})$, в которых элемент $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь (см. §4.1.1 и [140—142]). В разделе 4.1 найдено полное решение проблемы классификации для кубических эллиптических полей над полем рациональных чисел. В теореме 4.1.3.1 доказано, что за исключением тривиальных случаев с точностью до изоморфизма существует только 3 эллиптических поля $L = \mathbb{Q}(x)(\sqrt{f})$, в которых элемент $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в $\mathbb{Q}((x))$. Позднее коллективом под руководством В.П. Платонова удалось существенно продвинуться в этой задаче для кубических эллиптических полей, определенных над конечными расширениями K поля рациональных чисел, $[K : \mathbb{Q}] \leq 6$ (см. [143]), а также вне зависимости от поля K с органичениями на степень фундаментальной S-единицы (см. [144; 145]).

В разделе 4.2 найдено полное решение проблемы классификации для эллиптических полей, заданных многочленом четвертой степени над полем рациональных чисел. В теореме 4.2.1.1 доказано, что с точностью до изоморфизма существует 4 бесконечные серии и еще ровно 7 эллиптических полей $L = \mathbb{Q}(x)(\sqrt{f})$, в которых элемент $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в $\mathbb{Q}((x))$.

Теорема (4.2.1.1)**.** *С точностью до отношения эквивалентности, определенного допустимыми заменами многочлена $f(x)$ на $a^2 f(bx)$ для $a, b \in \mathbb{Q}^*$, множество свободных от квадратов многочленов $f \in \mathbb{Q}[x]$, $\deg f = 4$, для которых разложение $\sqrt{f}$ в непрерывную дробь в*

поле $\mathbb{Q}((x))$ *периодично, описывается семью многочленами*

$$(1-2x)(1+6x+32x^3),$$
$$(1-2x)(1+6x+96x^3),$$
$$(1-2x)(1+6x+32x^3/3),$$
$$1-2x-2x^2-3x^3-3x^4/4,$$
$$(1+10x)(1-6x+32x^2-128x^3),$$
$$(27+144x+320x^2)(9-72x+400x^2)/243,$$
$$(1-10x)(1+14x+224x^2+5600x^3),$$

и четырьмя семействами многочленов:

$$c_1x^4+1,$$
$$-c_2^2x^4+2c_2x^2+1,$$
$$(-c_3x^2+1)(3c_3x^2+1),$$
$$-c_4^2x^4/3+2c_4x^2+1,$$

где параметр $c_1 \in \mathbb{Z}\setminus\{0\}$ *свободен от четвертых степеней, параметры* $c_2, c_3, c_4 \in \mathbb{Z}\setminus\{0\}$ *свободны от квадратов.*

Отмеченные в разделе 3.3 особенности, возникающие для гиперэллиптических полей L, заданных многочленом f четной степени, существенно повлияли на доказательство теоремы 4.2.1.1 (по сравнению с теоремой 4.1.3.1), что отразилось не только в более сложных рассуждениях, но и существенно увеличило символьные компьютерные вычисления, необходимые для рассмотрения всех случаев.

В разделе 4.3 решена проблема классификации для эллиптических полей, заданных многочленом четвертой степени над квадратичными полями алгебраических чисел K и входящих в рациональную параметризацию модулярными кривыми. В теореме 4.3.1.1 для всех квадратичных числовых полей K приведено полное описание свободных от квадратов многочленов $f(x)\in K[x]$ степени 4 таких, что $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в поле формальных степенных рядов $K((x))$, а эллиптическое поле $L=K(x)(\sqrt{f})$ обладает фундаментальной S-единицей степени m, $2\le m\le 12$, $m\ne 11$, где множество S состоит из двух линейных сопряженных нормирований, определенных на поле L.

Теорема (4.3.1.1). *Обозначим через* $\mathcal{U}_0^{(4)}$ *множество пар* $[f(x),\ K]$, *состоящих из числового поля* K *и свободного от квадратов многочлена* $f\in K[x]$ *с минимальным представлением степени* 4, *имеющего периодическое разложение* $\sqrt{f}$ *в непрерывную дробь в поле* $K((x))$, *с точностью до отношения эквивалентности, определенного допустимыми заменами многочлена* $f(x)$ *на* $a^2f(bx)$ *для* $a,b\in K^*$ *и заменой* $f(x)$ *на* $f^\sigma(x)$, *где* $\sigma\in Gal(K/\mathbb{Q})$. *Обозначим за*

$\mathcal{U}^{(4)}$ множество троек $[m,\ f(x),\ K]$, где $[f(x),\ K] \in \mathcal{U}_0^{(4)}$ и m — степень соответствующей фундаментальной S-единицы кольца S-целых элементов поля $L = K(x)(\sqrt{f})$.

Множество троек $[m,\ f(x),\ K] \in \mathcal{U}^{(4)}$, таких, что $[K : \mathbb{Q}] \leq 2$, $m \leq 12$, $m \neq 11$, описывается следующим образом

$$
\begin{aligned}
&m = 3, \quad f_1 = -4x^4 - 4x^3 - 3x^2 - 2x + 1, \quad K = \mathbb{Q},\\
&m = 3, \quad f_2 = -12x^4 - 12x^3 - 3x^2 - 2x + 1, \quad K = \mathbb{Q},\\
&m = 3, \quad f_3 = -\frac{4x^4}{3} - \frac{4x^3}{3} - 3x^2 - 2x + 1, \quad K = \mathbb{Q},\\
&m = 3, \quad f_4 = -4x^4\left(3 - 2\sqrt{2}\right) - 4x^3\left(3 - 2\sqrt{2}\right) - 3x^2 - 2x + 1, \quad K = \mathbb{Q}(\sqrt{2}),\\
&m = 3, \quad f_5 = -4x^4\left(7 - 4\sqrt{3}\right) - 4x^3\left(7 - 4\sqrt{3}\right) - 3x^2 - 2x + 1, \quad K = \mathbb{Q}(\sqrt{3}),\\
&m = 3, \quad f_6 = -4x^4\left(5 - 2\sqrt{5}\right) - 4x^3\left(5 - 2\sqrt{5}\right) - 3x^2 - 2x + 1, \quad K = \mathbb{Q}(\sqrt{5}),\\
&m = 3, \quad f_7 = -\frac{4x^4\left(5 - 2\sqrt{5}\right)}{5} - \frac{4x^3\left(5 - 2\sqrt{5}\right)}{5} - 3x^2 - 2x + 1, \quad K = \mathbb{Q}(\sqrt{5}),\\
&m = 4, \quad f_8 = -\frac{3x^4}{4} - 3x^3 - 2x^2 - 2x + 1, \quad K = \mathbb{Q},\\
&m = 4, \quad f_9 = \frac{36 - 21\sqrt{3}}{2}x^4 + (15 - 9\sqrt{3})x^3 + (4 - 3\sqrt{3})x^2 - 2x + 1, \quad K = \mathbb{Q}(\sqrt{3}),\\
&m = 5, \quad f_{10} = -5x^4 - 3x^3 - \frac{7x^2}{4} - x + 1, \quad K = \mathbb{Q},\\
&m = 6, \quad f_{11} = \frac{108x^4}{5} + \frac{324x^3}{25} + \frac{69x^2}{25} - \frac{6x}{5} + 1, \quad K = \mathbb{Q},\\
&m = 7, \quad f_{12} = -\frac{28x^4}{5} - \frac{84x^3}{25} + \frac{21x^2}{25} - \frac{2x}{5} + 1, \quad K = \mathbb{Q},\\
&m = 7, \quad f_{13} = \frac{(35 - 9\sqrt{-7})x^4}{2} + \frac{(33 - 3\sqrt{-7})x^3}{2} +\\
&\qquad + \frac{(41 + 5\sqrt{-7})x^2}{8} - \frac{(3 + \sqrt{-7})x}{2} + 1, \quad K = \mathbb{Q}(\sqrt{-7}),\\
&m = 7, \quad f_{14} = -\frac{x^4\left(32\sqrt{21} + 147\right)}{15} - \frac{x^3\left(621 + 136\sqrt{21}\right)}{75} -\\
&\qquad - \frac{x^2\left(304\sqrt{21} + 1469\right)}{300} - \frac{x\left(33 + 8\sqrt{21}\right)}{15} + 1, \quad K = \mathbb{Q}(\sqrt{21}).
\end{aligned}
$$

В Главе 5 развита теория обобщенных функциональных непрерывных дробей, а также рассмотрено применение этой теории к проблеме поиска фундаментальных S-единиц в гиперэллиптических полях и к проблеме кручения в якобианах гиперэллиптических кривых. Теория функциональных непрерывных дробей, построенная в Главе 3, оказывается менее эффективной для случаев, когда нормирование v_h, по которому строится непрерывная дробь, имеет степень выше 1. В частности, при $\deg h \geq 2$ не выполнено свойство наилучшего приближения у подходящих дробей.

В серии статей 2015-2024 гг. в соавторстве с В.П. Платоновым был развит теоретико-числовой подход к проблеме поиска и построения фундаментальных S-единиц гиперэллиптических полей, основанный на теории функциональных непрерывных дробей в поле формальных степенных рядов $K((x))$. В частности, было показано, что теория функциональных непрерывных дробей позволяет существенно продвинуться в поиске нетривиальных S-единиц и в изучении их строения в гиперэллиптических полях над произвольным числовым полем в качестве поля констант для множества S состоящего из двух нормирований. В Главах 3 и 5 рассмотрены следующие случаи:

- множество S состоит из двух сопряженных (относительно гиперэллиптической инволюции) нормирований первой степени (Глава 3);
- множество S состоит из единственного бесконечного нормирования (когда $v_\infty^- = v_\infty^+$) и конечного нормирования первой степени, не связанного с точками Вейерштрасса (нетрадиционный подход, основанный на рассмотрении непрерывных дробей обобщенного типа, см. в разделе 5.2);
- множество S состоит из двух несопряженных нормирований первой степени (см. раздел 5.3);
- множество S состоит из двух сопряженных нормирований второй степени (см. раздел 5.4).

В частности, из решения проблемы поиска и построения S-единиц в указанных случаях следует полное алгоритмическое решение проблемы кручения в якобианах гиперэллиптических кривых рода 2.

В разделе 5.2 теория функциональных непрерывных дробей обобщенного типа (h-дробей) была применена для традиционного случая, когда непрерывная дробь строится по нормированию v_h, $\deg h = 1$. В теореме 5.2.2.1 доказан критерий периодичности (квазипериодичности) функциональных непрерывных дробей обобщенного типа, дающий эффективный алгоритм поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях (см. §5.2.3).

Теорема (5.2.2.1)**.** *Пусть K — поле характеристики, отличной от 2, и $h \in K[x]$, $\deg h = 1$. Пусть $f \in K[x]$ — свободный от квадратов многочлен нечетной степени $2g+1$, $g \geq 1$, и $S = \{v_h, v_\infty\}$. Пусть элемент $\alpha \in L = K(x)(\sqrt{f})$ имеет вид*

$$\alpha = \frac{\sqrt{f} + V}{U},$$

где $U = h^g$, $V = h^g \cdot \left[\sqrt{f} h^{-g}\right]_h$. *Определим*

$$R = \frac{f - V^2}{U \cdot h}, \quad a = [\alpha]_h, \quad W = aU - V, \quad T = \frac{f - W^2}{U \cdot h}, \quad \beta = \frac{\sqrt{f} + W}{T},$$
$$V_{-1} = V,\ U_{-1} = R,\ U_0 = U,\ V_0 = W,\ U_1 = T.$$

Существуют и однозначно определены эффективные дивизоры $D_R, D_U, D_T \in \mathrm{Div}(L)$ *такие, что главные дивизоры многочленов* $R, U, T \in K[x]$ *и функций* $\sqrt{f} - V, \sqrt{f} - W \in L$ *имеют вид*

$$(R) = D_R + \iota D_R + r\big(v_h + \iota v_h\big) - 2g \cdot \infty, \quad v_h(R) = r,$$
$$(U) = D_U + \iota D_U + s\big(v_h + \iota v_h\big) - 2g \cdot \infty, \quad v_h(U) = s,$$
$$(T) = D_T + \iota D_T + t\big(v_h + \iota v_h\big) - 2g \cdot \infty, \quad v_h(T) = t,$$
$$\left(\sqrt{f} - V\right) = D_R + (r + s + 1)v_h + \iota D_U - (2g + 1) \cdot \infty,$$
$$\left(\sqrt{f} - W\right) = D_U + (s + t + 1)v_h + \iota D_T - (2g + 1) \cdot \infty;$$

Положим

$$D_{-1} = D_R,\ D_0 = D_U,\ D_1 = D_T,\ s_{-1} = r,\ s_0 = s,\ s_1 = t.$$

Пусть справедливы построения

$$\alpha_{j+1} = \frac{V_j + \sqrt{f}}{U_{j+1}}, \quad f - V_j^2 = U_j \cdot h \cdot U_{j+1},$$
$$a_{j+1} = [\alpha_{j+1}]_h, \quad V_{j+1} = a_{j+1}U_{j+1} - V_j,$$
$$s_{j+1} = v_h(U_{j+1}) = -v_h(a_{j+1}) = -v_h(\alpha_{j+1}),$$
$$(U_j) = D_j + \iota D_j + s_j\big(v_h + \iota v_h\big) - 2g \cdot \infty,$$
$$\left(V_j - \sqrt{f}\right) = D_j + (s_j + s_{j+1} + 1)v_h + \iota D_{j+1} - (2g + 1) \cdot \infty.$$

Тогда следующие условия эквивалентны

1. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $D_n = 0$*;*
2. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $V_n = V_0$ *и* $U_n = ch^g$ *для некоторой постоянной* $c \in K^*$*;*
3. *класс дивизора* $\big(v_h - \infty\big)$ *имеет конечный порядок* m *в группе классов дивизоров* $\Delta^\circ(L)$*;*
4. *класс дивизора* $\big(v_h - \iota v_h\big)$ *имеет конечный порядок* m_h *в группе классов дивизоров* $\Delta^\circ(L)$*;*
5. *непрерывная дробь элемента* α *обобщенного типа квазипериодическая с длиной квазипериода* n*.*

Если существуют $n, m, m_h \in \mathbb{N}$*, указанные в эквивалентных условиях 1.-5., то*

- *непрерывная дробь α чисто периодическая с длиной периода либо n, если в пункте 2. постоянная $c = 1$, либо с длиной периода $2n$ и коэффициентом квазипериода $1/c$, если $c \neq 1$;*

- *справедливы соотношения*
$$m = \sum_{j=0}^{n-1}(2s_j + 1), \quad \text{где } s_j = -v_h(\alpha_j) = -v_h(a_j) = v_h(U_j),\ j \in \mathbb{N}_0;$$

- *для минимального $t \in \mathbb{N}$, такого, что $D_{2t} = 0$, справедливы соотношения $m_h = t + \sum_{j=0}^{2t-1} s_j$;*

- *если m четно, то $m_h = m/2$, если m нечетно, то $m_h = m$.*

В разделе 5.3 построена теория функциональных непрерывных дробей обобщенного типа для двух несопряженных линейных нормирований. Особенность таких обобщенных непрерывных дробей в том, что они сходятся к элементу как по первому, так и по второму линейному нормированию (см. предложение 5.3.3.3). В теореме 5.3.4.1 для функциональных непрерывных дробей обобщенного типа, построенным по двум несопряженным линейным нормированиям, доказан критерий периодичности для ключевых элементов гиперэллиптических полей.

Теорема (5.3.4.1)**.** *Пусть K — поле характеристики, отличной от 2. Пусть свободный от квадратов многочлен $f \in K[x]$, такой, что линейные нормирования v_x и v_h поля $K(x)$ имеют по два неэквивалентных продолжения $v_x^- \neq v_x^+$ и $v_h^- \neq v_h^+$ на поле $L = K(x)(\sqrt{f})$. Пусть $D_0 \in \mathrm{Div}(L)$ — такой приведенный дивизор, что $r_0 = v_x^-(D_0) = g$ или $s_0 = v_h^-(D_0) = g$. Пусть $(U_{-1}xh, V_{-1})$ — представление Мамфорда дивизора $D_0 + (x)_\circ^- + (h)_\circ^-$ и для $j \in \mathbb{N}_0$ справедливы построения*

$$U_j = T_j x^{s_j - r_j} h^{r_j - s_j}, \quad V_j = e_j T_j x^{-r_j} h^{-s_j} - V_{j-1},$$
$$f - V_j^2 = U_j x h T_{j+1}, \quad \deg U_j \leq g, \quad \deg T_{j+1} \leq g, \quad \deg V_j \leq g+1,$$
$$(U_{j-1})_{[g]} = D_j + \iota D_j - g(\infty^- + \infty^+),$$
$$(T_j)_{[g]} = E_j + \iota E_j - g(\infty^- + \infty^+),$$
$$D_j = \mathrm{gcdiv}\left(\left(V_{j-1} - \sqrt{f}\right)_{[g+1]},\ (U_{j-1})_{[g]}\right),$$
$$E_j = \mathrm{gcdiv}\left(\left(V_{j-1} - \sqrt{f}\right)_{[g+1]},\ (T_j)_{[g]}\right),$$
$$\left(V_{j-1} - \sqrt{f}\right)_{[g+1]} = D_j + (x)_\circ^- + (h)_\circ^- + E_j,$$
$$D_{j+1} = \iota E_j - r_j((x)_\circ^+ - (h)_\circ^-) - s_j((h)_\circ^+ - (x)_\circ^-),$$

где $r_j = v_x(T_j)$, $s_j = v_h(T_j)$, $U_j, T_j, V_j, e_j \in K[x]$, $U_j \neq 0$, $T_j \neq 0$, $e_j \neq 0$, *дивизоры* $D_j, E_j \in \mathrm{Div}(L)$ *приведенные.*

Тогда следующие условия эквивалентны

1. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $D_n = D_0$;
2. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $U_{n-1} = cU_{-1}$ *для некоторой постоянной* $c \in K^*$;
3. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $V_{n-1} = V_{-1}$ *и* $T_n = c^{-1}T_0$ *для некоторой постоянной* $c \in K^*$;
4. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $E_n = E_0$;
5. *классы эквивалентных дивизоров* $(h)_\circ^- - (x)_\circ^+ \sim (x)_\circ^- - (h)_\circ^+$ *имеют конечный порядок* m *в группе классов дивизоров* $\Delta^\circ(L)$;
6. *непрерывные дроби обобщенного типа элементов* $\sqrt{f}/x^g$ *и* $\sqrt{f}/h^g$, *квазипериодические с длиной квазипериода* n;
7. *в гиперэллиптическом поле* L *существует фундаментальная* S*-единица степени* m, *где* $S = \{v_x^-, v_h^+\}$;
8. *для некоторого* $b \in K^*$ *уравнение*
$$\mu_1^2 - \mu_2^2 f = bx^m h^m, \qquad \max\bigl(2\deg\mu_1,\ 2\deg\mu_2 + \deg f\bigr) = 2m,$$
имеет решение $\mu_1, \mu_2 \in K[x]$ *такое, что* $v_x(\mu_2) = v_h(\mu_2) = 0$, $\mu_2 \neq 0$.

Если существуют $n, m \in \mathbb{N}$, *указанные в эквивалентных условиях 1.-6., то они связаны соотношением*

$$m = \sum_{j=0}^{n-1}(1 + r_j + s_j), \quad \text{где для } j \in \mathbb{N}_0$$
$$r_j = -v_x^-(\alpha_j) = -v_x(a_j) = v_x^-(E_j) = v_x(T_j) = v_h(U_j) = v_h^-(D_{j+1}),$$
$$s_j = -v_h^-(\alpha_j) = -v_h(a_j) = v_h^-(E_j) = v_h(T_j) = v_x(U_j) = v_x^-(D_{j+1}).$$

В качестве следствия сформулирован эффективный алгоритм поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях (см. §5.4.6). В §5.3.6 в качестве иллюстрации построенного метода найдены новые примеры S-единиц для множеств S, состоящих из двух несопряженных линейных нормирований.

В разделе 5.3 построена теория непрерывных h-дробей — функциональных непрерывных дробей обобщенного типа, построенных по нормированию v_h, $\deg h = 2$. Ранее теория непрерывных дробей не применялась для поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях, когда в множестве S содержалось нормирование второй степени. В теореме 5.4.4.1 для непрерывных h-дробей, $\deg h = 2$, доказан критерий периодичности для ключевых элементов гиперэллиптических полей.

Теорема (5.4.4.1)**.** *Пусть $h \in K[x]$ неприводимый многочлен второй степени. Пусть свободный от квадратов многочлен $f \in K[x]$, $\deg f \geq 5$, такой, что нормирование v_h поля $K(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле $L = K(x)(\sqrt{f})$. Пусть $D_0 \in \mathrm{Div}(L)$ — такой приведенный дивизор, что $s_0 = v_h^-(D_0) = [g/2]$. Пусть $(U_0 \cdot h, V_0)$ — представление Мамфорда дивизора $D_0 + (h)_\circ^-$ и для $j \in \mathbb{N}_0$ справедливы построения*

$$U_{j+1} = \frac{f - V_j^2}{U_j \cdot h}, \quad \alpha_{j+1} = \frac{V_j + \sqrt{f}}{U_{j+1}}, \quad a_{j+1} = [\alpha_{j+1}]_h^-,$$

$$s_{j+1} = v_h(U_{j+1}) = -v_h(a_{j+1}) = -v_h^-(\alpha_{j+1}), \quad V_{j+1} = a_{j+1}U_{j+1} - V_j,$$

$$D_j = (U_j)_\circ^- - s_j(h)_\circ^+ + s_j(h)_\circ^-, \quad \left(V_j - \sqrt{f}\right)_\circ = D_j + (h)_\circ^- + (U_{j+1})_\circ^+,$$

$$(U_{j+1})_\circ^- + (U_j)_\circ + (h)_\circ^- = \left(V_j + \sqrt{f}\right)_\circ + (U_j)_\circ^- + (s_j + 1)\big((h)_\circ^- - (h)_\circ^+\big).$$

Тогда следующие условия эквиваленты

1. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $D_n = D_0$;*
2. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $V_n = V_0$ и $U_n = cU_0$ для некоторой постоянной $c \in K^*$;*
3. *класс дивизора $\big((h)_\circ^- - \infty^- - \infty^+\big)$ имеет конечный порядок m в группе классов дивизоров $\Delta^\circ(L)$;*
4. *класс дивизора $\big((h)_\circ^- - (h)_\circ^+\big)$ в группе классов дивизоров $\Delta^\circ(L)$ имеет конечный порядок m_h;*
5. *для элемента α,*
$$\alpha = \alpha_0 = \frac{\sqrt{f} - V_0}{U_0} + \left[\frac{\sqrt{f} + V_0}{U_0}\right]_h^-,$$
непрерывная дробь обобщенного типа квазипериодическая с длиной квазипериода n.

Если существуют $n, m, m_h \in \mathbb{N}$, указанные в эквивалентных условиях 1.-5., то

- *непрерывная дробь α чисто периодическая с длиной периода либо n, если постоянная $c = 1$ из пункта 2., либо с длиной периода $2n$ и коэффициентом квазипериода $1/c$, если $c \neq 1$;*

- *справедливы соотношения*

$$m = \sum_{j=0}^{n-1}(2s_j + 1), \quad \text{где } s_j = -v_h^-(\alpha_j) = -v_h(a_j) = v_h^-(D_j) = v_h(U_j),\ j \in \mathbb{N}_0;$$

- *для минимального* $t \in \mathbb{N}$, *такого, что* $D_{2t} = D_0$, *справедливы соотношения* $m_h = t + \sum_{j=0}^{2t-1} s_j$;

- *либо* $m_h = m/2$, *если* m *четно, либо* $m_h = m$, *если* m *нечетно.*

В качестве следствия сформулирован эффективный алгоритм поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях (см. §5.4.6). В §5.4.7 в качестве иллюстрации построенного метода найдены новые примеры S-единиц для множеств S, состоящих из двух сопряженных нормирований второй степени.

Разработанные в диссертации теоретические методы и подходы подкреплены соответствующими компьютерными вычислениями. В частности, получены быстрые алгоритмы поиска и построения фундаментальных S-единиц с помощью метода функциональных непрерывных дробей и функциональных непрерывных дробей обобщенного типа. С применением больших символьных компьютерных вычислений построены многочисленные примеры и контрпримеры, подтверждающие основные результаты диссертации.

1.6. Благодарности

Автор выражает глубокую благодарность научному консультанту, академику РАН, профессору Владимиру Петровичу Платонову за переданный неоценимый опыт в выборе задач, искусство ведения математических исследований и подготовки публикаций, постоянное внимание к работе, неугасимый математический энтузиазм и заразительный преданный интерес к науке.

Автор выражает благодарность коллективу отдела теоретической и прикладной алгебры и теории чисел ФГУ ФНЦ НИИСИ РАН за замечательную научную и рабочую атмосферу.

Глава 2. Основы теории алгебраических кривых

В этой главе дается краткое изложение необходимых базовых понятий и утверждений, которые используются в диссертации. Отметим, что по возможности изложение ведется на языке алгебры и алгебраической теории чисел, поскольку именно такой подход к указанным проблемам используется в диссертации. Наиболее важными являются §2.3.2 и §2.4.5, в которых дается введение в теорию нормирований и теорию дивизоров гиперэллиптических полей. В дальнейшем эти понятия используется на протяжении всей диссертации.

2.1. Алгебраические кривые и функциональные поля

В этом разделе представлено краткое введение в теорию алгебраических кривых и алгебраических функциональных полей. Более подробно базовые понятия и утверждения с полными доказательствами см., например, [27; 28; 132—134], [135—138].

2.1.1. Афинные многообразия

Пусть K — алгебраически замкнутое поле.

Множество $\mathbb{A}^n = \mathbb{A}^n(K)$ всех наборов из n элементов поля K называется n-мерным *афинным пространством*. Элемент $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$ называется *точкой*, $a_1, \ldots, a_n$ — *координаты* точки P. Подмножество $V \subseteq \mathbb{A}^n$ называется *алгебраическим множеством*, если есть такое подмножество $M \subseteq K[X_1, \ldots, X_n]$ кольца многочленов $K[X_1, \ldots, X_n]$ от n переменных, что

$$V = \{P \in \mathbb{A}^n \mid F(P) = 0, \text{ для всех } F \in M\}.$$

Для данного алгебраического множества $V \in \mathbb{A}^n$ множество многочленов

$$I(V) = \{F \in K[X_1, \ldots, X_n] \mid F(P) = 0, \text{ для всех } P \in V\}$$

называется *идеалом* V. Множество $I(V)$ действительно является идеалом кольца $K[X_1, \ldots, X_n]$, и идеал $I(V)$ порожден конечным числом многочленов $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$. Таким образом,

$$V = \{P \in \mathbb{A}^n \mid F_1(P) = \ldots = F_r(P) = 0\}.$$

Алгебраическое множество V называется *неприводимым*, если не существует таких собствен-

ных подмножеств $V_1, V_2 \subset V$, что $V = V_1 \cup V_2$. Алгебраическое множество неприводимо тогда и только тогда, когда идеал $I(V)$ является простым. *Афинным многообразием* называется неприводимое афинное множество $V \subseteq \mathbb{A}$.

Координатным кольцом афинного многообразия V называется факторкольцо $\Gamma(V) = K[X_1, \ldots, X_n]/I(V)$. Пусть алгебраическое множество V неприводимо, тогда идеал $I(V)$ простой, и $\Gamma(V)$ является областью целостности, содержащей поле K. Каждый класс $F + I(V) \in \Gamma(V)$ индуцирует единственную функцию $f : V \to K$ с помощью подстановки $f(P) = F(P)$, $P \in V$. Поле частных $K(V)$ кольца $\Gamma(V)$ называется *полем рациональных функций* (или *функциональным полем*) V. *Размерностью* V называется трансцендентная степень $K(V)/K$.

Для точки $P \in V$ положим

$$\mathcal{O}_P(V) = \{f \in K(V) \mid f = g/h,\ g, h \in \Gamma(V),\ h(P) \neq 0\}.$$

Это локальное кольцо с полем частных $K(V)$, оно обладает единственным максимальным идеалом

$$\mathcal{M}_P(V) = \{f \in K(V) \mid f = g/h,\ g, h \in \Gamma(V),\ h(P) \neq 0,\ g(P) = 0\}.$$

Множество $\mathcal{O}_P(V)$ называется *локальным кольцом* V в точке P.

2.1.2. Проективные многообразия

На множестве $\mathbb{A}^{n+1} \setminus \{(0, \ldots, 0)\}$ введем отношение эквивалентности

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n),$$

если найдется такое $0 \neq \lambda \in K$, что $b_i = \lambda a_i$, $0 \leq i \leq n$; класс эквивалентности обозначим $(a_0 : \ldots : a_n)$. Множество $\mathbb{P}^n = \mathbb{P}^n(K)$ всех классов эквивалентности $(a_0 : \ldots : a_n)$ с не всеми нулевыми a_i называется n-мерным *проективным пространством*; элемент $(a_0 : \ldots : a_n) \in \mathbb{P}^n$ называется *точкой*, числа $a_0, \ldots a_n$ называются ее *однородными координатами*.

Мономом степени d называется многочлен $G \in K[X_0, \ldots, X_n]$ вида

$$G = a \prod_{i=0}^{n} X_i^{d_i}, \quad 0 \neq a \in K, \quad \sum_{i=0}^{n} d_i = d.$$

Многочлен F называется *однородным*, если он равен сумме мономов одной и той же степени. Идеал $I \subseteq K[X_0, \ldots, X_n]$, порожденный однородными многочленами, называется *однородным*.

Пусть даны точка $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$ и однородный многочлен $F \in K[X_0, \ldots, X_n]$. Определим значение в точке $F(P) = 0$, если $F(a_0, \ldots, a_n) = 0$.

Множество $V \subseteq \mathbb{P}^n$ называется *проективным алгебраическим множеством*, если найдется такое множество однородных многочленов $M \subseteq K[X_0, \ldots, X_n]$, что

$$V = \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ для всех } F \in M\}.$$

Идеал $I(V)$, порожденный всеми такими однородными многочленами F, что $F(P) = 0$ для любой точки $P \in V$, называется *идеалом* V. Идеал $I(V)$ является однородным идеалом. Неприводимость в проективном случае определяется точно также, как в афинном. Аналогично афинному случаю, проективное алгебраическое множество $V \subseteq \mathbb{P}^n$ неприводимо тогда и только тогда, когда однородный идеал $I(V)$ является простым в кольце $K[X_0, \ldots, X_n]$. Неприводимое проективное алгебраическое множество называется *проективным многообразием*.

Для данного непустого многообразия $V \subseteq \mathbb{P}^n$ определим *однородное координатное кольцо* следующим образом

$$\Gamma_h(V) = K[X_0, \ldots, X_n]/I(V).$$

Так как идеал $I(V)$ простой, то $\Gamma_h(V)$ является областью целостности, содержащей поле K. Элемент $f \in \Gamma_h(V)$ будем называть *формой* степени d, если $f = F + I(V)$ для некоторого однородного многочлена $F \in K[X_0, \ldots, X_n]$, причем степень F равна d. *Поле функций* V определим следующим образом

$$K(V) = \left\{ \frac{g}{h} \mid g, h \in \Gamma_h(V) \text{ есть формы одинаковой степени и } h \neq 0 \right\}.$$

Поле функций $K(V)$ является подполем поля частных кольца $\Gamma_h(V)$. *Размерностью* V назовем трансцендентную степень $K(V)$ над K.

Пусть даны точка $P = (a_0 : \ldots : a_n) \in \mathbb{P}_n$ и форма $f \in K(V)$. Запишем $f = g/h$, где $g = G + I(V), h = H + I(V) \in \Gamma_h(V)$ и G, H являются однородными многочленами степени d. Если $H(P) \neq 0$, то мы можем корректно определить *значение* f в точке P следующим образом: $f(P) = G(a_0, \ldots, a_n)/H(a_0, \ldots, a_n) \in K$. В этом случае будем говорить, что форма f *определена* в точке P.

Для точки $P \in V$ положим

$$\mathcal{O}_P(V) = \{f \in K(V) \mid f \text{ определена в точке } P\} \subseteq K(V).$$

Это локальное кольцо с единственным максимальным идеалом

$$\mathcal{M}_P(V) = \{f \in \mathcal{O}_P(V) \mid f(P) = 0\}.$$

Множество $\mathcal{O}_P(V)$ называется *локальным кольцом* V в точке P.

2.1.3. Покрытие проективного многообразия афинными

Определим отображения

$$\varphi_i(a_0, \ldots, a_{n-1}) = (a_0 : \ldots : a_{i-1} : 1 : a_i : \ldots : a_{n-1}), \quad 0 \leq i \leq n,$$

которые являются биекциями $\varphi_i : \mathbb{A}^n \to U_i$, где

$$U_i = \{(c_0 : \ldots : c_n) \in \mathbb{P}^n \mid c_i \neq 0\}.$$

Ясно, что $\mathbb{P}^n = \bigcup_{i=0}^n U_i$, то есть $\mathbb{P}^n$ покрывается $n+1$ копией афинного пространства $\mathbb{A}^n$.

Пусть дано проективное многообразие $V \subseteq \mathbb{P}^n$, тогда $V = \bigcup_{i=0}^n (V \cap U_i)$. Если $V \cap U_i \neq \varnothing$, то $V_i = \varphi_i^{-1}(V \cap U_i) \subseteq \mathbb{A}^n$ является афинным многообразием с идеалом $I(V_i)$, заданным следующим образом:

$$I(V_i) = \{F(X_0, \ldots, X_{i-1}, 1, X_i, \ldots, X_n) \mid F \in I(V)\}.$$

Случай $i = n$ рассматривается отдельно (если $V \cap U_n \neq \varnothing$). Дополнение $H_n = \mathbb{P}^n \setminus U_n = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n \mid a_n = 0\}$ называется *гиперплоскостью на бесконечности*, и точки $P \in V \cap H_n$ называются *точками V на бесконечности*.

Существует натуральный K-изоморфизм $\alpha : K(V) \to K(V_n)$, где $K(V_n)$ — поле функций афинного многообразия $V_n = \varphi_n^{-1}(V \cap U_n)$. Его можно определить следующим образом. Пусть $f = g/h \in K(V)$, где $g, h \in \Gamma_h(V)$ — формы одинаковой степени и $h \neq 0$. Выберем однородные многочлены $G, H \in K[X_0, \ldots, X_n]$, которые являются представителями классов g и h соответственно. Положим $G_* = G(X_0, \ldots, X_{n-1}, 1)$ и $H_* = H(X_0, \ldots, X_{n-1}, 1)$ — многочлены в $K[X_0, \ldots, X_{n-1}]$. Пусть g_* и h_* — классы вычетов в $\Gamma(V_n)$ соответственно G_* и H_*. Тогда $\alpha(f) = g_*/h_*$. Данный изоморфизм отображает локальное кольцо точки $P \in V \cap U_n$ в локальное кольцо точки $\varphi_n^{-1}(P) \in V_n$, следовательно, эти локальные кольца изоморфны.

2.1.4. Проективное замыкание афинного многообразия

Для многочлена $F = F(X_0, \ldots, X_{n-1}) \in K[X_0, \ldots, X_{n-1}]$ степени d мы положим $F^* = X_n^d \cdot F(X_0/X_n, \ldots, X_{n-1}/X_n) \in K[X_0, \ldots, X_n]$ — однородный многочлен степени d от $n+1$ переменной.

Пусть дано афинное многообразие $V \in \mathbb{A}^n$ и соответствующий ему идеал $I(V) \subseteq K[X_0, \ldots, X_{n-1}]$ Определим проективное многообразие $\overline{V} \subseteq \mathbb{P}^n$ следующим образом:

$$\overline{V} = \{P \in \mathbb{P}^n \mid F^*(P) = 0 \text{ для всех } F \in I(V)\}.$$

Это многообразие называется *проективным замыканием V*. Можно и обратно построить афинное многообразие V по многообразию $\overline{V}$, а именно, $V = \varphi_n^{-1}(\overline{V} \cap U_n) = (\overline{V})_n$. Следовательно, поля функций V и $\overline{V}$ изоморфны, а также V и $\overline{V}$ имеют одинаковую размерность.

2.1.5. Рациональные отображения и морфизмы

Пусть даны проективные многообразия $V \subseteq \mathbb{P}^m$ и $W \subseteq \mathbb{P}^n$. Предположим, что $F_0, \ldots, F_n \in K[X_0, \ldots, X_m]$ — однородные многочлены, удовлетворяющие следующим свойствам:

1) $F_0, \ldots, F_n$ имеют одинаковую степень;

2) не все F_i принадлежат идеалу $I(V)$;

3) для любого $H \in I(W)$ справедливо $H(F_0, \ldots, F_n) \in I(V)$.

Пусть точка $Q \in V$ такая, что $F_i(Q) \neq 0$ хотя бы для одного номера i, $0 \leq i \leq n$. Тогда точка $(F_0(Q) : \ldots : F_n(Q)) \in \mathbb{P}^n$ принадлежит W. Пусть $(G_0, \ldots, G_n)$ — другой набор из n однородных многочленов, удовлетворяющий свойствам 1), 2) и 3). Будем называть наборы $(G_0, \ldots, G_n)$ и $(F_0, \ldots, F_n)$ эквивалентными, если

4) $F_i G_j \equiv F_j G_i \pmod{I(V)}$ для $0 \leq i, j \leq n$.

Класс эквивалентных наборов $(F_0, \ldots, F_n)$ будем обозначать $\phi = (F_0 : \ldots : F_n)$ и называть его *рациональным отображением* из V в W.

Рациональное отображение $\phi = (F_0 : \ldots : F_n)$ *регулярно* (или *определено*) в точке $P \in V$, если существует такие однородные многочлены $G_0, \ldots, G_n \in K[X_1, \ldots, X_m]$, что $\phi = (G_0 : \ldots : G_n)$ и $G_i(P) \neq 0$ хотя бы для одного номера i, $0 \leq i \leq n$. В этом случае точка $\phi(P) = (G_0(P) : \ldots : G_n(P)) \in W$ определена корректно.

Два многообразия V_1 и V_2 *бирационально эквивалентны*, если есть рациональные отображения $\phi_1 : V_1 \to V_2$ и $\phi_2 : V_2 \to V_1$ такие, что $\phi_1 \circ \phi_2$ и $\phi_2 \circ \phi_1$ — тождественные отображения V_2 и V_1 соответственно. Многообразия V_1 и V_2 бирационально эквивалентны тогда и только тогда, когда поля функций $K(V_1)$ и $K(V_2)$ являются K-изоморфными.

Регулярное во всех точках $P \in V$ рациональное отображение $\phi : V \to W$ называется *морфизмом*. Если дополнительно есть морфизм $\psi : W \to V$ такой, что $\phi \circ \psi$ и $\psi \circ \phi$ — тождественные отображения V и W соответственно, то ϕ называется *изоморфизмом* многообразий. Ясно, что изоморфные многообразия барицинально эквивалентны, однако в общем случае обратное утверждение не верно.

2.1.6. Алгебраические кривые

Алгебраическим полем функций L/K от одной переменной над полем K называется поле L, являющееся конечным алгебраическим расширением $K(x)$ для некоторого трансцендентного над K элемента $x \in L$.

Проективной (афинной) алгебраической кривой V называется проективное (афинное) многообразие размерности один. В этом случае поле $K(V)$ рациональных функций на V является алгебраическим полем функций от одной переменной.

Точка $P \in V$ называется *неособой* (или *простой*), если локальное кольцо $\mathcal{O}_P(V)$ является кольцом дискретного нормирования, то есть $\mathcal{O}_P(V)$ является кольцом главных идеалов с единственным максимальным ненулевым идеалом. На кривой существует только конечное число особых точек. Кривая V называется *неособой* (или *гладкой*), если все точки $P \in V$ неособые.

Афинная кривая $V \subseteq \mathbb{A}^2$ называется *плоской афинной кривой*. Ее идеал $I(V) \subseteq K[X_0, X_1]$ порожден единственным (с точностью до умножения на константу) неприводимым многочленом $G \in K[X_0, X_1]$. Справедливо и обратное утверждение: для данного неприводимого многочлена $G \in K[X_0, X_1]$ множество $V = \{P \in \mathbb{A}^2 \mid G(P) = 0\}$ является плоской афинной кривой, и многочлен G порождает идеал $I(V)$. Точка $P \in V$ неособая тогда и только тогда, когда либо $G'_{X_0}(P) \neq 0$, либо $G'_{X_1}(P) \neq 0$ (*критерий Якоби*).

Аналогичным образом определяется *плоская проективная кривая* $V \subseteq \mathbb{P}^2$, ее идеал $I(V)$ порожден неприводимым однородным многочленом $H \in K[X_0, X_1, X_2]$. Точка $P \in V$ неособая тогда и только тогда, когда $H'_{X_i}(P) \neq 0$ хотя бы для одного номера i, $0 \leq i \leq 2$.

Если $V = \{P \in \mathbb{A}^2 \mid G(P) = 0\}$ — плоская афинная кривая с неприводимым многочленом $G \in K[X_0, X_1]$ степени d, то проективным замыканием $\overline{V} \subseteq \mathbb{P}^2$ является множество нулей однородного многочлена $G^* = X_2^d \cdot G(X_0/X_2, X_1/X_2)$.

Для $\phi : V \to W$ — рационального отображения проективных кривых V и W справедливы следующие утверждения.

1. Отображение ϕ определено во всех неособых точках $P \in V$. Если V неособая кривая, то ϕ — морфизм.

2. Если V неособая кривая и ϕ непостоянное отображение, то ϕ сюръективно.

Пусть V — проективная кривая. Существует неособая проективная кривая V' и бирациональный морфизм $\phi' : V' \to V$, причем пара (V', ϕ') является единственной в следующем смысле: если есть другая кривая V'' и бирациональный морфизм $\phi'' : V'' \to V$, то существует единственный изоморфизм $\phi : V' \to V''$ такой, что $\phi' = \phi'' \circ \phi$. Кривая V' (или более точно пара (V', ϕ')) называется *неособой моделью* кривой V. Если $\phi' : V' \to V$ — неособая модель V и точка $P \in V$ неособая, то существует единственная точка $P' \in V'$ такая, что $\phi'(P') = P$; для особой точки $P \in V$ количество $P' \in V'$ с условием $\phi'(P') = P$ конечно.

Если дано алгебраическое поле функций L/K, то существует единственная с точностью до изоморфизма неособая проективная кривая V, чье поле функций $K(V)$ совпадает (K-изоморфно) с L. Построить V можно следующим образом. Выберем $x, y \in L$ такие, что $L = K(x, y)$ (см., например, предложение 3.10.2 [28],). Существует $G(X, Y) \in K[X, Y]$ — неприводимый многочлен с условием $G(x, y) = 0$. Пусть $W = \{P \in \mathbb{A}^2 \mid G(P) = 0\}$ и $\overline{W} \subseteq \mathbb{P}^2$ — проективное замыкание W. Если V — неособая модель $\overline{W}$, то $K(V) \simeq L$.

2.1.7. Многообразия над не алгебраически замкнутым полем

Предположим теперь, что K произвольное совершенное поле (не обязательно алгебраически замкнутое).

Будем говорить, что афинное многообразие $V \subseteq \mathbb{A}^n(\overline{K})$ *определено над* K, если его идеал $I(V) \subseteq \overline{K}[X_1, \ldots, X_n]$ порожден многочленами $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$. Если V определено над K, то множество

$$V(K) = V \cap \mathbb{A}^n(K) = \{P = (a_1, \ldots, a_n) \in V \mid \text{все } a_i \in K\}$$

называется *множеством K-рациональных точек (K-точек)* V.

Аналогично, проективное многообразие $V \subseteq \mathbb{P}^n(\overline{K})$ *определено над* K, если его идеал $I(V)$ порожден однородными многочленами $F_1, \ldots, F_r \in K[X_0, \ldots, X_n]$. Точка $P \in V$ называется *K-точкой*, если можно выбрать ее координаты $a_0, \ldots, a_n \in K$. Множество всех K-точек V обозначим $V(K)$.

Пусть дано афинное многообразие $V \subseteq \mathbb{A}^n(\overline{K})$, определенное над K. Определим идеал $I(V/K) = I(V) \cap K[X_1, \ldots, X_n]$ и его кольцо вычетов $\Gamma(V/K) = K[X_1, \ldots, X_n]/I(V/K)$. Поле частных кольца $\Gamma(V/K)$ обозначается $K(V)$ и называется *полем K-рациональных функций* V. Расширение полей $K(V)/K$ конечно, его трансцендентная степень равна размерности V. Подобным образом определяются *K-точки* и *поле K-рациональных функций* проективного многообразия.

Рассмотрим два многообразия $V \subseteq \mathbb{P}^m(\overline{K})$ и $W \subseteq \mathbb{P}^n(\overline{K})$. Рациональное отображение $\phi : V \to W$ *определено над* K, если найдутся такие многочлены $F_1, \ldots, F_n \in K[X_0, \ldots, X_m]$, удовлетворяющие условиям 1), 2) и 3) параграфа 2.1.5, что $\phi = (F_0 : \ldots : F_n)$.

2.2. Гиперэллиптические кривые

В этом разделе определены гиперэллиптические кривые и рассмотрены их основные свойства. Более подробно с полными доказательствами см., например, [28; 97; 132—134; 146]. Случай гиперэллиптических кривых нечетной степени см. в [147; 148].

В этой главе мы будем работать с базовым полем констант K — произвольным совершенным полем. Как и ранее, $\overline{K}$ — алгебраическое замыкание поля K.

2.2.1. Определение и базовые свойства

Пусть $h, f \in K[x]$. Уравнение

$$y^2 + h(x)y = f(x) \tag{2.2.1.1}$$

называется *уравнением гиперэллиптической кривой*, если выполнены следующие условия:

1. множество точек $(x, y) \in \overline{K}^2$, удовлетворяющих (2.2.1.1), не содержит особых точек, то есть справедливо одно из условий:

   1.1. $h = 0$ и $\gcd(f,\ f') \in K^*$, или

1.2. $h \neq 0$ и $\gcd(h^2 + 4f,\ 2f' + hh') \in K^*$;

2. уравнение (2.2.1.1) является $\overline{K}$-неприводимым, то есть $y^2 + h(x)y - f(x)$ нельзя представить в виде $(y - \omega_1(x))(y - \omega_2(x))$, где $\omega_1, \omega_2 \in \overline{K}[x]$; для этого достаточно, чтобы не существовало точек $P = (x_P, y_P)$ таких, что

2.1. $y_P^2 + h(x_P)y_P = f(x_P)$,

2.2. $h'(x_P)y_P = f'(x_P)$ и $2y_P + h(x_P) = 0$.

Отображение $\iota(x, y) = (x, -y - h(x))$ называется *гиперэллиптической инволюцией* (или просто *инволюцией*).

С помощью проективизации $\rho : (x, y) \to (X/Z, Y/Z)$ из (2.2.1.1) получается *уравнение проективной гиперэллиптической кривой*, образующее множество точек C в $\mathbf{P}^2_{\overline{K}}$, которое называется *гиперэллиптической кривой*. Скажем, что точка $P = (x_P, y_P) \in \overline{K}^2$ лежит на кривой C, если она удовлетворяет уравнению гиперэллиптической кривой (2.2.1.1). Множество K-точек гиперэллиптической кривой C обозначим $C(K)$. Точки вида $(X : Y : 0)$, лежащие на кривой C, называются *бесконечными точками*. Далее мы уточним количество и вид точек гиперэллиптической кривой на бесконечности.

Из определения гиперэллиптической кривой C следует, что это действительно кривая, так как C геометрически неприводимое многообразие размерности один без особых точек (см. §2.1.6).

Уравнение гиперэллиптической кривой эквивалентно над K (задает то же множество точек) уравнению вида

$$y^2 + (h_{s+1}x^{s+1} + h_s x^s + \ldots + h_0)y = f_{2s+2}x^{2s+2} + f_{2s+1}x^{2s+1} + \ldots + f_0, \tag{2.2.1.2}$$

где $\max(\deg h,\ \lceil(\deg f)/2\rceil) = s + 1$ и выполнено хотя бы одно из четырех условий:

1. $h_{s+1} = 0$ и $f_{2s+2} \neq 0$;

2. $h_{s+1} = 0$ и $f_{2s+1} \neq 0$;

3. $h_{s+1} \neq 0$ и $f_{2s+2} \neq (h_{s+1}/2)^2$;

4. $h_{s+1} \neq 0$ и $f_{2s+1} \neq h_{s+1}h_s/2$.

Для исследования поведения кривой на бесконечности удобно рассмотреть следующую проективную модель гиперэллиптической кривой.

Взвешанным проективным гиперэллиптическим уравнением называется уравнение

$$Y^2 + (h_{s+1}X^{s+1} + h_s X^s Z + \ldots + h_0 Z^{s+1})Y = f_{2s+2}X^{2s+2} + f_{2s+1}X^{2s+1}Z + \ldots + f_0 Z^{2s+2} \tag{2.2.1.3}$$

во взвешанном проективном пространстве с весами X, Y, Z соответственно 1, $s+1$, 1. Уравнение (2.2.1.3) получается из уравнения (2.2.1.2) с помощью замены $(x, y) = (X/Z, Y/Z^{s+1})$.

Точки на бесконечности уравнения (2.2.1.3) имеют вид $(1 : \kappa : 0)$, где $\kappa \in \overline{K}$ удовлетворяет уравнению

$$\kappa^2 + h_{s+1}\kappa - f_{2s+2} = 0. \tag{2.2.1.4}$$

В силу условий в определении гиперэллиптического уравнения, точки на бесконечности являются неособыми. Кроме того алгебраическое множество, заданное уравнением (2.2.1.3), $\overline{K}$-неприводимо, имеет размерность 1 и бирационально эквивалентно гиперэллиптической кривой C. Таким образом, неособую проективную кривую заданную уравнением (2.2.1.3), мы можем также называть *гиперэллиптической кривой*. Число $g = \max\Big(\deg h - 1,\ [(\deg f - 1)/2]\Big) = s$ называется *родом гиперэллиптической кривой*.

Если уравнение (2.2.1.4) имеет два различных корня в $\overline{K}$, то обозначим точки на бесконечности $\infty^- = (1 : \kappa^- : 0)$ и $\infty^+ = (1 : \kappa^+ : 0)$, иначе $\infty = (1 : \kappa : 0)$. Если существует единственная точка на бесконечности, то уравнение (2.2.1.3) называется *разветвленной моделью гиперэллиптической кривой*. Если существует две различные точки на бесконечности, то при $\infty^-, \infty^+ \in K$ уравнение (2.2.1.3) называется *расщепленной моделью гиперэллиптической кривой*, а при $\infty^-, \infty^+ \notin K$ — *нейтральной моделью гиперэллиптической кривой*.

Нас в наибольшей степени будут интересовать гиперэллиптические кривые с разветвленной или с расщепленной моделью. Для разветвленной модели гиперэллиптической кривой необходимо и достаточно выполнение одного из условий:

1. $\deg h < s+1$ и $\deg f = 2s+1$, или
2. $\deg h = s+1$, $\deg f = 2s+2$ и $f_{2s+2} = -(h_{s+1}/2)^2$.

Отметим, что если $\operatorname{Char} K \neq 2$ и $h \neq 0$, то заменой переменных $(x, y) \to (x, y - h/2)$ кривая C преобразуется в $y^2 = f(x)$, причем в случае разветвленной модели будем иметь $\deg f = 2s+1$.

В общем случае для гиперэллиптической кривой $C:\ y^2 + h(x)y = f(x)$ над полем K рассмотрим точку $P \in C(K)$ и отображение

$$\rho_P(x,\ y) = \Big(1/(x - x_P),\ y/(x - x_P)^{s+1}\Big). \tag{2.2.1.5}$$

Тогда $\rho_P:\ C \to C'$, где C' также гиперэллиптическая кривая, изоморфная C, причем,

1. если $P = \iota(P)$, то C бирациональна над K гиперэллиптической кривой с разветвленной моделью;
2. если $P \neq \iota(P)$, то C бирациональна над K гиперэллиптической кривой с расщепленной моделью.

Из этого следует, что если $C(K) \neq \varnothing$, то кривая C бирационально эквивалента гиперэллиптической кривой с разветвленной или расщепленной моделью.

Заметим, что для гиперэллиптической кривой C с разветвленной или расщепленной моделью существует и обратное отображение, переводящее бесконечную точку в конечную точку P с данной координатой X_P:

$$(x, y) \to \left(\frac{1}{X - X_P}, \frac{Y}{(X - X_P)^{s+1}} \right), \tag{2.2.1.6}$$

причем $P = \iota P$, если кривая C имела разветвленную модель. В связи с этим в разветвленной модели мы будем считать, что $\infty = \iota\infty$.

2.2.2. Полиномы и рациональные функции

В этом параграфе определены полиномы и рациональные функции на гиперэллиптической кривой. Мы зафиксируем слово "полином" для специальных определенных далее объектов поля функций гиперэллиптической кривой, чтобы не возникало путаницы с понятием обычного многочлена.

Пусть $\operatorname{Char} K \neq 2$ и $C : y^2 = f(x)$ — гиперэллиптическая кривая.

Координатным кольцом кривой C над полем K или над полем $\overline{K}$ соответственно называется кольцо

$$K[C] = K[x, y]/\big(y^2 - f(x)\big), \quad \overline{K}[C] = \overline{K}[x, y]/\big(y^2 - f(x)\big),$$

где $\big(y^2 - f(x)\big)$ — идеал кольца $K[x, y]$ или $\overline{K}[x, y]$ соответственно, порожденный многочленом $y^2 - f(x)$. Элемент кольца $\overline{K}[C]$ называется *полиномом* на кривой C.

Многочлен $y^2 - f(x) \in K[x, y]$ неприводим над $\overline{K}$, поэтому кольцо $\overline{K}[C]$ является областью целостностью. Полином $G \in \overline{K}[C]$ может быть единственным образом записан в виде

$$G = G(x, y) = \omega_1(x) - \omega_2(x)y, \quad \omega_1, \omega_2 \in \overline{K}[x]. \tag{2.2.2.1}$$

Сопряженным к полиному $G \in \overline{K}[C]$ вида (2.2.2.1) называется полином $\overline{G} = \overline{G}(x, y) = \omega_1 + \omega_2 y$. *Нормой* полинома G называется $N(G) = G\overline{G}$.

Ясно, что $N(G) \in \overline{K}[x]$. Кроме того, если $G \in K[C]$, то $N(G) \in K[x]$. Норма полинома обладает обычными свойствами: если $G, G_1, G_2 \in \overline{K}[C]$, то $N(\overline{G}) = N(G)$ и $N(G_1G_2) = N(G_1)N(G_2)$. Отображение $N = N_{K[C]/K[x]} : K[C] \to K[x]$ называется *норменным отображением.*

Уравнение вида

$$\omega_1^2 - \omega_2^2 f = \omega, \quad \omega_1, \omega_2, \omega \in K[x] \tag{2.2.2.2}$$

называется *норменным уравнением* полинома $G = \omega_1 - \omega_2 y \in K[C]$.

Полем функций $K(C)$ или $\overline{K}(C)$ кривой C называется поле, состоящее из дробей вида

$R = G_1/G_2$, где $G_2 \neq 0$, $G_1, G_2 \in K[C]$ или $G_1, G_2 \in \overline{K}[C]$ соответственно. Элемент $\overline{K}(C)$ называется *рациональной функцией* на кривой C.

Рациональная функция $R \in \overline{K}(C)$ определена в конечной точке $P \in C$, если найдутся полиномы $G_1, G_2 \in \overline{K}[C]$ такие, что $R = G_1/G_2$ и $G_2(P) \neq 0$; иначе функция R не определена в P.

Степенью полинома $G \in \overline{K}[C]$ вида (2.2.2.1) называется число

$$\deg_C G = \max\Big(2\deg\omega_1,\ \deg f + 2\deg\omega_2\Big).$$

В случае разветвленной модели гиперэллиптической кривой C для полиномов $G, G_1, G_2 \in \overline{K}[C]$ справедливы следующие соотношения

$$\deg_C G = \deg N(G), \quad \deg(G_1 G_2) = \deg G_1 + \deg G_2, \quad \deg G = \deg \overline{G}.$$

Пусть $R = G_1/G_2 \in \overline{K}(C)$ — рациональная функция, тогда $\overline{R} = \overline{G_1}/\overline{G_2} \in \overline{K}(C)$ — *сопряженная* к ней. Определим для разветвленной модели гиперэллиптической кривой C значение рациональной функции на бесконечности, то есть в точке $P = \infty$.

1. Если $\deg_C G_1 < \deg_C G_2$, то R определена в точке ∞ и $R(\infty) = 0$.
2. Если $\deg_C G_1 > \deg_C G_2$, то R не определена в точке ∞.
3. Если $\deg_C G_1 = \deg_C G_2$, то R определена в точке ∞ и значение $R(\infty)$ равно отношению старших (относительно $\deg_C$) коэффициентов полиномов G_1 и G_2.

В общем случае разветвленной модели или расщепленной модели значения в точках $P = \infty$, или $P = \infty^-$, или $P = \infty^+$, соответственно, определяется как

$$\frac{G_1(P)}{G_2(P)} = \lim_{Z\to 0} \frac{G_1(X/Z, Y/Z^{s+1})}{G_2(X/Z, Y/Z^{s+1})}\bigg|_{X=1,\ Y=\kappa}, \tag{2.2.2.3}$$

где κ — корень (2.2.1.4), соответствующий точке P.

2.2.3. Нули и полюса

В этом параграфе определены униформизующие в различных точках гиперэллиптической кривой C, а также порядки нулей и полюсов рациональных функций.

Пусть даны рациональная функция $R \in \overline{K}(C)^*$ и точка $P \in C$ (конечная или бесконечная). Если $R(P) = 0$, то P является *нулем* R; если R не определена в точке P, то P является *полюсом* R.

Пусть полином $G \in \overline{K}[C]$ вида (2.2.2.1) имеет ноль в точке P, тогда $\overline{G}(\iota P) = 0$. Если, кроме того, $\omega_2(x_P) \neq 0$, то $\overline{G}(P) = 0$ тогда и только тогда, когда $P = \iota P$.

Теорема 2.2.3.1. *Пусть $P \in C$ (P конечная или бесконечная точка). Тогда существует такая рациональная функция $U \in \overline{K}(C)$, что $U(P) = 0$ и выполнено следующее условие: для*

любого полинома $G \in \overline{K}[C]^*$ *существует целое* r *и рациональная функция* $G_0 \in \overline{K}(C)$*, для которой точка* P *не является ни нулем, ни полюсом, и* $G = U^r G_0$.

Доказательство. См., например, [133], §10.1.2. □

В теореме 2.2.3.1 число $r = v_P(G)$ по абсолютной величине не зависит от выбора U и называется *кратностью* точки P в G. Функция U называется *униформизующей* в точке P.

Заметим, что, если U — униформизующая в точке P, то U^{-1} также является униформизующей в точке P. Для определенности мы будем считать, что униформизующие в конечных точках P выбираются так, что $v_P(G) \geq 0$ при $G \in \overline{K}[x]$, а в бесконечных точках P — так, что $v_P(G) \leq 0$ при $G \in \overline{K}[x]$.

В случае разветвленной модели в качестве униформизующей U в точке P можно, например, выбрать следующие значения

1. если $P = \iota P \neq \infty$, то $U = y - y_P$;
2. если $P \neq \iota P$, то $U = x - x_P$;
3. если $P = \infty$, то $U = x^s/y$.

В случае расщепленной модели в качестве униформизующей U в точке P можно, например, выбрать следующие значения

1. если $P = \iota P$, то $U = y - y_P$;
2. если $P \neq \iota P$, то $U = x - x_P$;
3. если $P = \infty^-$ или $P = \infty^+$, то $U = x^s/(y - \kappa x)$, где κ — корень (2.2.1.4), соответствующий точке P.

Дадим альтернативное определение порядка полинома в точке.

Пусть дан полином $G \in \overline{K}[C]^*$ вида (2.2.2.1) и точка $P \in C$.

Пусть точка P конечная. Если r — максимальная степень $x - x_P$, делящая многочлены ω_1 и ω_2, то положим $G = (x - x_P)^r G_0$, $G_0 = \omega_3 - \omega_4 y$. Если $\omega_3(x_P) - \omega_4(x_P) y_P \neq 0$, положим $m = 0$; иначе m — максимальная степень $x - x_P$, делящая $N(G_0)$. Если $P \neq \iota P$, то кратность точки P в G есть $v_P(G) = r + m$. Если $P = \iota P$, то кратность точки P в G есть $v_P(G) = 2r + m$.

Теперь предположим, что точка P бесконечная. В случае разветвленной модели положим $v_P(G) = -\deg_C G$, а в случае расщепленной модели $v_P(G) = -\frac{1}{2}\deg_C G$, если

$$Z^{\frac{1}{2}\deg_C G} G\left(\frac{X}{Z}, \frac{Y}{Z^{s+1}}\right)\Big|_P \neq 0, \tag{2.2.3.1}$$

и $v_P(G) = \deg N(G) - \frac{1}{2}\deg_C G$ иначе. Здесь значение выражения (2.2.3.1) понимается в смысле (2.2.2.3).

Пусть точка $P \in C$ и $G, G_1, G_2 \in \overline{K}[C]^*$, $v_P(G_1) = r_1$, $v_P(G_2) = r_2$, тогда справедливы следующие утверждения.

1. $v_P(G) = v_{\iota P}\left(\overline{G}\right)$.
2. $v_P(G_1 G_2) = v_P(G_1) + v_P(G_2)$.
3. Предположим $G_1 \neq G_2$. Если $r_1 \neq r_2$, то $v_P(G_1 + G_2) = \min(r_1,\ r_2)$. Если $r_1 = r_2$, то $v_P(G_1 + G_2) \geq \min(r_1,\ r_2)$.

Теорема 2.2.3.2. *Полином $G \in \overline{K}[C]^*$ имеет конечное число нулей и полюсов. Более того, $\sum_P v_P(G) = 0$.*

Доказательство. См., например, [97]. □

Пусть $R = G_1/G_2 \in \overline{K}(C)^*$ и $P \in C$. Тогда *кратность* точки P в R есть $v_P(R) = v_P(G_1) - v_P(G_2)$.

2.3. Группа S-единиц

В этом разделе рассмотрены основы теории нормирований и S-единиц в гиперэллиптическом поле L (подробнее см., например, [28; 133; 146]). В частности, мы напоминаем понятие продолжения нормирования на квадратичное расширение, свойства S-единиц для произвольного множества нормирований S. Мы даем определение степени S-единицы для произвольного множества нормирований S и находим связь степени S-единицы с порядком класса дивизоров в группе классов дивизоров степени ноль гиперэллиптического поля L. Более подробно об S-единицах гиперэллиптических полей можно посмотреть, например, в [17; 130].

Мы будем называть S-единицу *и простой*, если ее нельзя представить с точностью до постоянной в виде некоторой степени другой S-единицы. В этой главе доказано, что для фиксированного конечного множества нормирований S наименьшее общее кратное $N(S)$ степеней всех простых S-единиц конечно, в то время, как при $|S| \geq 3$ количество простых S-единиц может быть бесконечно.

Пусть K — произвольное поле, характеристики отличной от 2. Обозначим K^* мультипликативную группу поля K. Символом $\mathrm{lc}(\omega)$ мы обозначаем старший коэффициент многочлена $\omega \in \mathbb{Q}[x]$.

2.3.1. Плейсы

Алгебраическим полем функций L/K от одной переменной над полем K называется конечное расширение поля рациональных функций $K(x)$, где $x \in L$ трансцендентный элемент

над K (ср. с полем функций алгебраической кривой в §2.1.6 и полем функций гиперэллиптической кривой в §2.2.2).

Часто L/K мы будем кратко называть *полем функций*. Множество $\hat{K}$ алгебраических над K элементов поля L/K будем называть *полем констант* поля L/K. Как правило в рассматриваемых далее случаях $\hat{K} = K$.

Кольцом нормирования алгебраического поля функций L/K называется кольцо $\mathcal{O}$, $K \subsetneqq \mathcal{O} \subsetneqq L$, обладающее свойством: для каждого элемента $\alpha \in L$ справедливо $\alpha \in \mathcal{O}$ или $\alpha^{-1} \in \mathcal{O}$.

Кольцо нормирования является локальным кольцом, то есть имеет единственный максимальный идеал $\mathcal{P} = \mathcal{O} \backslash \mathcal{O}^{\times}$, где $\mathcal{O}^{\times} = \{\alpha \in \mathcal{O} \mid$ существует такой элемент $\beta \in \mathcal{O},$ что $\alpha \cdot \beta = 1\}$ — группа единиц (обратимых элементов) кольца $\mathcal{O}$. Более того, $\mathcal{O}$ — кольцо главных идеалов.

Плейсом $\mathcal{P}$ алгебраического поля функций L/K называется максимальный идеал некоторого кольца нормирования $\mathcal{O}$ поля L/K (см. подробнее в [28]). Каждый элемент $h \in \mathcal{P}$ такой, что $\mathcal{P} = h\mathcal{O}$ называется *простым* элементом $\mathcal{P}$ (также говорят *локальный параметр* или *униформизующая*). Множество всех плейсов поля L/K обозначим $\mathbb{P}_L$.

Дискретным нормированием поля L/K называется функция $v : L \to \mathbb{Z} \cup \{\infty\}$, обладающая следующими свойствами:

1. $v(\alpha) = \infty$ тогда и только тогда, когда $\alpha = 0$;
2. $v(\alpha \cdot \beta) = v(\alpha) + v(\beta)$ для любых $\alpha, \beta \in L$;
3. $v(\alpha + \beta) \geq \min(v(\alpha),\ v(\beta))$ для любых $\alpha, \beta \in L$;
4. существует элемент $h \in L$ такой, что $v(h) = 1$;
5. $v(a) = 0$ для любого $a \in K$, $a \neq 0$.

Пусть $\mathcal{P} \in \mathbb{P}_L$, $\mathcal{O}_{\mathcal{P}}$ — его кольцо нормирования и $h \in \mathcal{P}$ — простой элемент. Для любого $\alpha \in L$, $\alpha \neq 0$, имеется единственное представление $\alpha = h^n u$, где $n \in \mathbb{Z}$, $u \in \mathcal{O}_{\mathcal{P}}^{\times}$. Тогда функция $v_h = v_{\mathcal{P}} : L \to \mathbb{Z} \cup \{\infty\}$, определенная по правилу $v_{\mathcal{P}}(\alpha) = n$, $v_{\mathcal{P}}(0) = \infty$, является дискретным нормированием поля L/K; элемент $\kappa \in L$ простой для $\mathcal{P}$ тогда и только тогда, когда $v_{\mathcal{P}}(\kappa) = 1$. Справедливо и обратное утверждение: если v — некоторое дискретное нормирование поля L/K, то множество $\mathcal{P} = \{\alpha \in L \mid v(\alpha) > 0\}$ является плейсом и $\mathcal{O}_{\mathcal{P}} = \{\alpha \in L \mid v(\alpha) \geq 0\}$ — соответствующее ему кольцо нормирования.

Полем классов вычетов плейса $\mathcal{P} \in \mathbb{P}_L$ называется $L_{\mathcal{P}} = \mathcal{O}/\mathcal{P}$. *Степень плейса* $\mathcal{P}$ определяется как $\deg \mathcal{P} = [L_{\mathcal{P}} : K]$. Плейс степени один называется *рациональным плейсом*. Если $0 \neq y \in \mathcal{P}$, то $\deg \mathcal{P} \leq [L : K(y)] < \infty$.

Скажем, что плейс $\mathcal{P} \in \mathbb{P}_L$ является *нулем* (*полюсом*) элемента $\alpha \in L$, если $v_P(\alpha) > 0$ ($v_{\mathcal{P}}(\alpha) < 0$); если $v_{\mathcal{P}}(\alpha) = m$, то говорят, что P является нулем (полюсом) α *кратности* m.

Из теоремы 2.2.3.2 следует, что каждый элемент $\alpha \in L$ имеет конечное число нулей и полюсов. Более того,

$$\sum_{\mathcal{P}\in\mathbb{P}_L} v_{\mathcal{P}}(\alpha) = 0. \tag{2.3.1.1}$$

Пример 2.3.1.1. *Рассмотрим рациональное поле функций $L = K(x)$, где x трансцендентный над K. Для данного неприводимого над K многочлена $h(x) \in K[x]$ с единичным старшим коэффициентом кольцо*

$$\mathcal{O}_{h(x)} = \left\{ \frac{\omega_1}{\omega_2} \;\middle|\; \omega_1, \omega_2 \in K[x],\ h \nmid \omega_2 \right\}$$

поля $K(x)/K$ является кольцом нормирования с максимальным идеалом

$$\mathcal{P}_h = \mathcal{P}_{h(x)} = \left\{ \frac{\omega_1}{\omega_2} \mid \omega_1, \omega_2 \in K[x],\ h \mid \omega_1,\ h \nmid \omega_2 \right\}.$$

В этом случае плейс $\mathcal{P}_h$ называется конечным. *Дискретное нормирование v_h поля $K(x)$, соответствующее плейсу $\mathcal{P}_h$, заданно равенством*

$$v_h\left(\frac{\omega_1}{\omega_2}\right) = v_h\left(h^m \frac{\varphi(x)}{\psi(x)}\right) = m,$$

где $\varphi, \psi \in K[x]$, $h \nmid \varphi$, $h \nmid \psi$, $m \in \mathbb{Z}$. Будем полагать, что $v_h(0) = \infty$.

Определим степень нормирования v_h *в поле $K(x)$ равной степени многочлена h, то есть* $\deg v_h = \deg h$. *В случае* $\deg h = 1$ *нормирование v_h будем называть* линейным.

Кроме конечных плейсов в поле $K(x)$ есть еще только один плейс $\mathcal{P}_\infty$, называемый бесконечным плейсом*; его кольцо нормирование и максимальный идеал имеют вид*

$$\mathcal{O}_\infty = \left\{ \frac{\omega_1}{\omega_2} \mid \omega_1, \omega_2 \in K[x],\ \deg\omega_1 \le \deg\omega_2 \right\},$$

$$\mathcal{P}_\infty = \left\{ \frac{\omega_1}{\omega_2} \mid \omega_1, \omega_2 \in K[x],\ \deg\omega_1 < \deg\omega_2 \right\}.$$

Дискретное нормирование, соответствующее плейсу $\mathcal{P}_\infty$, будем обозначать v_∞. Нормирование v_∞ называется бесконечным нормированием *и задается равенством*

$$v_\infty\left(\frac{\omega_1}{\omega_2}\right) = \deg\omega_2 - \deg\omega_1, \qquad \omega_1, \omega_2 \in K[x],\ \omega_2 \neq 0.$$

Степень бесконечного нормирования v_∞ в поле $K(x)$ равна 1.

2.3.2. Продолжение нормирований

Пусть $h \in K[x]$ — неприводимый над K многочлен и v_h — соответствующее ему дискретное нормирование поля $K(x)$ (см. пример 2.3.1.1).

Пусть $\overline{K(x)}_h$ — пополнение поля $K(x)$ относительно нормирования v_h. Нормирование v_h единственным образом продолжается на пополнение $\overline{K(x)}_h$, поэтому продолженное нормирование по-прежнему будем обозначать v_h. Обозначим через $\mathcal{O}_h = \{\omega \in K(x) :\ v_h(\omega) \ge 0\}$

кольцо нормирования v_h поля $K(x)$, а через $\rho_h = \{\omega \in K(x) : v_h(\omega) > 0\}$ — идеал нормирования v_h. Выберем в $\mathcal{O}_h$ фиксированную систему Σ представителей смежных классов по идеалу $\rho_h = h \cdot \mathcal{O}_h$, состоящую из всех многочленов степени, меньшей чем $\deg h$. Тогда каждый элемент $\beta \in \overline{K(x)}_h$ единственным образом можно представить в виде формального степенного ряда (см., например, [28], теорема 4.2.6):

$$\beta = \sum_{j=r}^{\infty} \sigma_j h^j, \quad \text{где} \quad \sigma_j \in \Sigma, \quad r \in \mathbb{Z}. \tag{2.3.2.1}$$

Множество формальных степенных рядов вида (2.3.2.1) обозначим $\Sigma_K((h))$.

Пусть $f(x) \in K[x]$ — свободный от квадратов многочлен, $2g+1 \le \deg f \le 2g+2$, $g \ge 1$. Поле функций гиперэллиптической кривой $C : y^2 = f(x)$ изоморфно алгебраическому полю функций $L = K(x)(\sqrt{f})$ — квадратичному расширению поля $K(x)$. Произвольный элемент $\beta \in L$ можно единственным образом представить в виде

$$\beta = \frac{\omega_1 + \omega_2\sqrt{f}}{\omega_3}, \quad \omega_1, \omega_2, \omega_3 \in K[x], \quad \operatorname{lc}(\omega_3) = 1, \quad \gcd(\omega_1,\ \omega_2,\ \omega_3) \in K^*, \tag{2.3.2.2}$$

где символом $\operatorname{lc}(\omega)$ мы обозначаем старший коэффициент многочлена $\omega \in K[x]$, а символом $\gcd(\omega_1,\ \omega_2,\ \omega_3)$ — наибольший общий делитель (определенный с точностью до умножения на константу из K^*) многочленов $\omega_1, \omega_2, \omega_3 \in K[x]$. Определим $\overline{x}$ — образ элемента x в поле вычетов $K_h = \mathcal{O}_h/\rho_h$.

Нас интересует вопрос, каким образом нормирование v_h поля $K(x)$ можно продолжить на поле L. В случае алгебраически замкнутого поля K можно воспользоваться леммой Гензеля.

Лемма ([149]). *Пусть K — алгебраически замкнутое поле, $\mathcal{O}$ — кольцо нормирования v в $\overline{K(x)}_v$, ρ — его максимальный идеал. Пусть T — трансцендентный элемент над $\mathcal{O}$, $\Omega \in \mathcal{O}[T]$ и $\overline{\Omega} \equiv \Omega \pmod{\rho}$, $\overline{\Omega} \in K[T]$. Если существует корень $\gamma \in K$ многочлена $\overline{\Omega}$ такой, что $\overline{\Omega}'(\gamma) \ne 0$, то существует единственный элемент $\alpha \in \mathcal{O}$, который является корнем $\Omega(T)$ и $\overline{\alpha} = \gamma$.*

Для произвольного поля K рассмотрим три случая.

1) Если $f(\overline{x}) = w^2$ для некоторого $0 \ne w \in K_h$ (а это означает, что точка $(\overline{x}, w)$ является K_h-точкой гиперэллиптической кривой C), то нормирование v_h поля $K(x)$ имеет два неэквивалентных продолжения на поле L: v_h^- и v_h^+. Естественно считать, что $v_h^-(h) = 1$ и $v_h^+(h) = 1$. В этом случае $h \nmid f$, $\sqrt{f} \in \overline{K(x)}$ и

$$v_h^-\left(\omega_1 + \omega_2\sqrt{f}\right) = v_h^+\left(\omega_1 - \omega_2\sqrt{f}\right),$$

$$v_h^-\left(\omega_1 + \omega_2\sqrt{f}\right) + v_h^-\left(\omega_1 - \omega_2\sqrt{f}\right) = v_h\left(\omega_1^2 - \omega_2^2 f\right), \tag{2.3.2.3}$$

$$v_h^+\left(\omega_1 + \omega_2\sqrt{f}\right) + v_h^+\left(\omega_1 - \omega_2\sqrt{f}\right) = v_h\left(\omega_1^2 - \omega_2^2 f\right), \tag{2.3.2.4}$$

где $\omega_1, \omega_2 \in K[x]$, поскольку поле L может быть вложено в поле формальных степенных рядов $\Sigma_K((h))$ двумя способами, которые могут быть получены друг из друга *инволюцией* ι, заданной отображением $\iota : \sqrt{f} \to -\sqrt{f}$.

2) Если $f(\overline{x}) = 0$, то нормирование v_h имеет единственное продолжение $v_h^{L/K(x)}$ на поле L. В этом случае для универсальности записи мы также будем использовать обозначения v_h^- и v_h^+, но теперь нормирования v_h^- и v_h^+ эквивалентны на поле L, то есть значения v_h^- и v_h^+ на элементах поля L совпадают, в том числе

$$v_h^-\left(\omega_1 - \omega_2\sqrt{f}\right) = v_h^-\left(\omega_1 + \omega_2\sqrt{f}\right) = v_h^+\left(\omega_1 + \omega_2\sqrt{f}\right) = v_h^+\left(\omega_1 - \omega_2\sqrt{f}\right)$$

для $\omega_1, \omega_2 \in K[x]$. Мы будем считать, что $v_h^-(h) = v_h^+(h) = 1$, но $v_h^{L/K(x)}(h) = 2$. Имеем

$$v_h^-\left(\omega_1 \pm \omega_2\sqrt{f}\right) + v_h^+\left(\omega_1 \pm \omega_2\sqrt{f}\right) = v_h^{L/K(x)}\left(\omega_1 \pm \omega_2\sqrt{f}\right) = v_h\left(\omega_1^2 - \omega_2^2 f\right). \quad (2.3.2.5)$$

где $\omega_1, \omega_2 \in K[x]$, а вместо "$\pm$" знаки можно выбирать любым способом. Если в контексте ясно, в каком поле рассматривается нормирование, то продолжение $v_h^{L/K(x)}$ мы также будем обозначать v_h.

3) Если $f(\overline{x}) \neq 0$ и $f(\overline{x})$ не является квадратом в K_h, то существует алгебраическое расширение $\hat{K}$ поля K, в котором найдется элемент $0 \neq w \in \hat{K}_h$ такой, что $f(\overline{x}) = w^2$. Это верно, поскольку поле K_h является конечным алгебраическим расширением поля K, значит и поле $\hat{K}_h = K_h(\sqrt{f(\overline{x})})$ также является конечным расширением поля K. Следовательно, в качестве $\hat{K}$ можно взять, например, $\hat{K}_h$. Многочлен h необязательно неприводим над полем $\hat{K}$. Для каждого неприводимого делителя $h_j \mid h$ над $\hat{K}$ существуют два продолжения $v_{h_j}^-$ и $v_{h_j}^+$ на поле $\hat{L} = \hat{K}(x)(\sqrt{x})$ которые определяются, как в случае 1). В то же время над полем K существует единственное продолжение $v_h^{L/K(x)}$ нормирования v_h поля $K(x)$, которое определяется как в случае 2). Для элементов $\omega_1 + \omega_2\sqrt{f} \in L$ рассматриваемых в поле $\hat{L}$ справедливы соотношения

$$v_h^-\left(\omega_1 + \omega_2\sqrt{f}\right) + v_h^-\left(\omega_1 - \omega_2\sqrt{f}\right) = v_h^{L/K(x)}\left(\omega_1 \pm \omega_2\sqrt{f}\right) = v_h\left(\omega_1^2 - \omega_2^2 f\right), \quad (2.3.2.6)$$

$$v_h^+\left(\omega_1 + \omega_2\sqrt{f}\right) + v_h^+\left(\omega_1 - \omega_2\sqrt{f}\right) = v_h^{L/K(x)}\left(\omega_1 \pm \omega_2\sqrt{f}\right) = v_h\left(\omega_1^2 - \omega_2^2 f\right), \quad (2.3.2.7)$$

Определим продолжение бесконечного нормирования v_∞ поля $K(x)$ на поле L. Рассмотрим отображение $\phi : L \to \mathcal{L}$, заданное заменой $\phi : x \to 1/X$. Положим $F(X) = X^{2g+2} f(1/X) \in K[X]$, тогда $\mathcal{L} = K(X)(\sqrt{F})$ и

$$\phi : \mathcal{O}_\infty^{K(x)} \to \mathcal{O}_X^{K(X)}, \quad \phi : \rho_\infty^{K(x)} \to \rho_X^{K(X)}, \quad (2.3.2.8)$$

то есть в поле $K(x)$ справедливо соотношение $v_\infty = v_X \circ \phi$. Значит, продолжение нормирования v_∞ поля $K(x)$ на поле L естественно определить следующим образом: $v_\infty^- = v_X^- \circ \phi$ и $v_\infty^+ = v_X^+ \circ \phi$, причем, если нормирование v_X поля $K(X)$ имеет единственное продолжение на поле $\mathcal{L}$, то

$v_\infty^{L/K(x)} = v_X^{\mathcal{L}/K(X)} \circ \phi$. В частности, если многочлен $f(x)$ имеет нечетную степень, $\deg f = 2g+1$, получаем, что нормирование v_∞ поля $K(x)$ имеет единственное продолжение на L. Если ясно, что единственное бесконечное нормирование рассматривается в поле L, то будем обозначать его также через v_∞.

В поле L определим *степени конечных нормирований* $\deg v_h^\pm = \deg h$ и $\deg v_h^{L/K(x)} = 2\deg h$ в случае, если $v_h^- = v_h^+$. В случае $\deg h = 1$ нормирования v_h^-, v_h^+ будем называть *линейными*. *Степень бесконечных нормирований* определим как $\deg v_\infty^- = \deg v_\infty^+ = 1$ и $\deg v_\infty^{L/K(x)} = 2$ в случае, если $v_\infty^- = v_\infty^+$.

Обозначим $\mathcal{V}^{K(x)}$ множество конечных нормирований поля $K(x)$. Обозначим $\mathcal{V}^{L/K(x)}$ множество всех продолжений конечных и бесконечных нормирований поля $K(x)$. Нормирования v_h^-, v_h^+ и v_∞^-, v_∞^+ соответственно будем называть *сопряженными* и обозначать $v_h^- = \iota v_h^+$, $v_\infty^- = \iota v_\infty^+$. Тем самым инволюция $\iota : \mathcal{V}^{L/K(x)} \to \mathcal{V}^{L/K(x)}$ продолжается на множество нормирований. Из (2.3.1.1) следует, что для каждого элемента $\alpha \in L$ справедливо соотношение

$$\sum_{v \in \mathcal{V}^{K(x)/L}} v(\alpha) = \sum_{v \in \mathcal{V}^{K(x)}} \big(v^-(\alpha) + v^+(\alpha)\big) + \big(v_\infty^-(\alpha) + v_\infty^+(\alpha)\big) = 0. \tag{2.3.2.9}$$

Предложение 2.3.2.1. *Пусть $\alpha = \omega_1 + \omega_2\sqrt{f}$, где $\omega_1, \omega_2 \in K[x]$, $\omega_1 \neq 0$, $\omega_2 \neq 0$, $\gcd(\omega_1, \omega_2) \in K^*$, и пусть $h \in K[x]$ — неприводимый многочлен. Тогда справедливы следующие утверждения:*

1. *если v_h имеет два продолжения v_h^- и v_h^+ на поле L, то $v_h^-(\alpha) \cdot v_h^+(\alpha) = 0$;*
2. *если $h \nmid f$ и v_h имеет единственное продолжение $v_h^{L/K(x)}$ на поле L, то $v_h^{L/K(x)}(\alpha) = 0$;*
3. *если $h \mid f$, то v_h имеет единственное продолжение $v_h^{L/K(x)}$ на поле L; в этом случае если $h \nmid \omega_1$, то $v_h(\alpha) = 0$; если $h \mid \omega_1$, то $v_h^{L/K(x)}(\alpha) = 1$.*

Доказательство. Аналогично доказательству предложения 2.1 из [130].

Пусть v_h имеет два продолжения v_h^- и v_h^+ на поле L, и $v_h^-(\alpha) > 0$, $v_h^+(\alpha) > 0$. Используя обозначения пункта 1), введенные выше, запишем

$$\begin{cases} \omega_1(\overline{x}) + \omega_2(\overline{x}) \cdot \omega = 0, \\ \omega_1(\overline{x}) - \omega_2(\overline{x}) \cdot \omega = 0. \end{cases}$$

Поскольку $\omega \neq 0$, то получаем $\omega_1(\overline{x}) = \omega_2(\overline{x}) = 0$, что противоречит условию $\gcd(\omega_1, \omega_2) \in K^*$.

Пусть теперь нормирование v_h поля $K(x)$ имеет единственное продолжение на поле L. Если $h \nmid f$, то используя обозначения пункта 1), введенные выше, имеем $f(\overline{x}) = \omega^2$, $\omega \in \hat{K}_h \setminus K_h$, откуда $\omega_1(\overline{x}) \pm \omega_2(\overline{x}) \cdot \omega \neq 0$, поскольку $\omega_1(\overline{x}), \omega_2(\overline{x}) \in K_h$. Если $h \mid f$, то $\omega = 0$, и $\alpha(\overline{x}) = 0$ тогда и только тогда, когда $\omega_1(\overline{x}) = 0$. Наконец, значения $v_h(\alpha)$ в пунктах 2 и 3 легко находятся по формуле (2.3.2.5). $\square$

Предложение 2.3.2.2 ([17]). *Пусть бесконечное нормирование v_∞ поля $K(x)$ имеет два продолжения v_∞^- и v_∞^+ на поле L. Пусть $\omega_1, \omega_2 \in K[x]$, $\alpha = \omega_1 + \omega_2\sqrt{f}$, $N(\alpha) = \alpha \cdot \overline{\alpha} = \omega_1^2 - \omega_2^2 f$, $\max\left(\deg(\omega_1^2),\ \deg(\omega_2^2 f)\right) = 2m_1$. Тогда*

$$\min\left(v_\infty^-(\alpha),\ v_\infty^+(\alpha)\right) = -m_1, \quad \max\left(v_\infty^-(\alpha),\ v_\infty^+(\alpha)\right) = v_\infty(N(\alpha)) + m_1,$$

где в поле $K(x)$ имеем $v_\infty(N(\alpha)) = -\deg N(\alpha)$.

Доказательство. Предположим, что $\deg(\omega_1^2) \le \deg(\omega_2^2 f)$, тогда

$$-m_1 \le \min\left(v_\infty^-(\alpha),\ v_\infty^-(\overline{\alpha})\right) \le v_\infty^-(\alpha - \overline{\alpha}) = -\deg(\omega_2^2 f)/2 = -m_1,$$

следовательно, $\min\left(v_\infty^-(\alpha),\ v_\infty^+(\alpha)\right) = -m_1$. В случае, если $\deg(\omega_1^2) > \deg(\omega_2^2 f)$, имеем

$$-m_1 \le \min\left(v_\infty^-(\alpha),\ v_\infty^-(\overline{\alpha})\right) \le v_\infty^-(\alpha + \overline{\alpha}) = -\deg(\omega_1^2)/2 = -m_1,$$

откуда, снова $\min\left(v_\infty^-(\alpha),\ v_\infty^+(\alpha)\right) = -m_1$. Теперь остается заметить, что $v_\infty^-(\alpha) + v_\infty^+(\alpha) = v_\infty(\alpha \cdot \overline{\alpha}) = v_\infty(N(\alpha))$.

Предложение 2.3.2.2 доказано. □

2.3.3. Свойства S-единиц

Пусть многочлен f свободен от квадратов и $L = K(x)(\sqrt{f})$. Пусть S — произвольное конечное множество неэквивалентных нормирований поля L.

Обозначим через $\mathcal{O}_S$ кольцо S-целых элементов в L, то есть таких элементов $\alpha \in L$, что $v(\alpha) \ge 0$ для всех нормирований v поля L, не принадлежащих множеству S. Множество обратимых элементов $\mathcal{U}_S$ кольца $\mathcal{O}_S$ называется *группой S-единиц поля L*.

В силу обобщенной теоремы Дирихле о единицах (см. [150], гл. IV, теорема 9) в случае, если группа $\mathcal{U}_S$ нетривиальна, она является прямым произведением мультипликативной группы K^* и свободной абелевой группы G ранга не более $|S| - 1$. Независимые образующие группы G называются *фундаментальными S-единицами*.

Отметим, что в случае, когда $K = \mathbb{F}_q$ — конечное поле из q элементов, группа $\mathcal{U}_S$ обязательно нетривиальна.

Положим $S_1 = \{v_{h_1}, \dots, v_{h_t}\} = S|_{K(x)}$ — множество ограничений конечных нормирований из S на поле $K(x)$, где $h_1, \dots, h_t \in K[x]$ — неприводимые многочлены. Следующее предложение характеризует S-целые элементы в поле L.

Предложение 2.3.3.1. *Любой элемент $\beta \in \mathcal{O}_S$ может быть единственным образом записан в виде*

$$\beta = \frac{\omega_1 + \omega_2\sqrt{f}}{h_1^{r_1} \cdots h_t^{r_t}}, \quad \text{где } \omega_1, \omega_2 \in K[x],\ h_j \nmid \gcd(\omega_1,\ \omega_2),\ r_j \in \mathbb{Z}. \tag{2.3.3.1}$$

При этом, если $r_j > 0$ и нормирование v_{h_j} имеет два продолжения на L, из которых одно не принадлежит S, то $h_j \nmid \omega_1$ и $h_j \nmid \omega_2$.

Доказательство. Аналогично доказательству предложения 2.2 из [130].

Любой элемент $\beta \in \mathcal{O}_S$ можно представить в виде (2.3.2.2). Предположим, что найдется нормирование $v_h \notin S_1$ такое, что $v_h(\omega_3) > 0$. Если нормирование v_h имеет два продолжения v_h^- и v_h^+ на L, то по предложению 2.3.2.1 либо $v_h^-\left(\omega_1 + \omega_2\sqrt{f}\right) = 0$, либо $v_h^+\left(\omega_1 + \omega_2\sqrt{f}\right) = 0$, но это противоречит условию $\alpha \in \mathcal{O}_S$. Если v_h имеет единственное продолжение $v_h^{L/K(x)}$ на L, то по предложению 2.3.2.1 имеем $v_h^{L/K(x)}(\omega_1 + \omega_2\sqrt{f}) \leq 1$, но $v_h^{L/K(x)}(\omega_3) \geq 2$, что снова противоречит условию $\alpha \in \mathcal{O}_S$. □

Отметим, что не любой элемент α вида (2.3.3.1) является S-целым. Например, если нормирование $v_h \in S_1$ имеет два продолжения v_h^- и v_h^+ на L и $v_h^+ \notin S$, то элемент $1/h$ не является S-целым.

Обозначим через $N = N_{L/K(x)}$ норменное отображение из L в $K(x)$. Для дальнейшего нам важно знать, какие значения может принимать норменное отображение на S-единицах.

Предложение 2.3.3.2. *Пусть $\alpha \in U_S$, тогда*

$$N(\alpha) = bh_1^{m_1} \cdots h_t^{m_t}, \quad \text{где } b \in K^*,\ m_i \in \mathbb{Z}. \tag{2.3.3.2}$$

Доказательство. Аналогично доказательству предложения 2.3 из [130].

Пусть α имеет вид (2.3.3.1) и существует нормирование $v_h \notin S_1$ такое, что $v_h(N(\alpha)) \neq 0$. Без ограничения общности можем считать, что $v_h(N(\alpha)) > 0$. Тогда в силу (2.3.2.6) имеем $v_h^-\left(\omega_1 + \omega_2\sqrt{f}\right) + v_h^-\left(\omega_1 - \omega_2\sqrt{f}\right) > 0$. По предложению 2.3.2.1 без ограничения общности можем считать, что $v_h^-\left(\omega_1 + \omega_2\sqrt{f}\right) > 0$. Так как $\alpha, 1/\alpha \in \mathcal{O}_S$ и $v_h^- \notin S$, то

$$v_h^-\left(\frac{1}{\alpha}\right) = v_h^-\left(\frac{\omega_1 - \omega_2\sqrt{f}}{N(\alpha)}\right) \geq 0,$$

откуда $v_h^-\left(\omega_1 - \omega_2\sqrt{f}\right) \geq v_h^-(N(\alpha)) = v_h(N(\alpha)) > 0$, следовательно, $v_h^- = v_h^+$. Но, в то же время,

$$v_h^-\left(\frac{1}{\alpha}\right) = v_h^-\left(\frac{1}{\omega_1 + \omega_2\sqrt{f}}\right) = -v_h^-\left(\omega_1 + \omega_2\sqrt{f}\right) < 0,$$

что приводит нас к противоречию. □

Как и в случае S-целых элементов, если элемент $\alpha \in L$ обладает свойством (2.3.3.2), то из этого не следует, что α является S-единицей. Например, если нормирование $v_h \in S_1$ имеет два продолжения на L и v_h^+ не принадлежит S, то $N(h) = h^2$, однако h не является S-единицей.

Если $\alpha = \omega_1 + \omega_2\sqrt{f} \in U_S$, то из предложения 2.3.3.2 следует, что

$$N(\alpha) = \omega_1^2 - \omega_2^2 f = b_1 h_1^{m_1} \cdots h_t^{m_t}, \quad \text{где } b_1 \in K^*,\ m_j \in \mathbb{Z},\ m_j \geq 0. \tag{2.3.3.3}$$

В следующем предложении по решению норменного уравнения (2.3.3.3) в многочленах $\omega_1, \omega_2 \in K[x]$, $\omega_2 \neq 0$, строится некоторая нетривиальная S-единица. Обозначим S_2 — множество таких нормирований $v \in S_1$ поля $K(x)$, имеющих два продолжения v^- и v^+ на поле

L, одно из которых, скажем v^+, не принадлежит множеству S. Обозначим S_3 — множество нормирований $v \in S_1$ поля $K(x)$, имеющих единственное продолжение на поле L, S_4 — множество нормирований $v \in S_1$ поля $K(x)$, имеющих два продолжения v^- и v^+, принадлежащих множеству S. Ясно, что $S_1 = S_2 \cup S_3 \cup S_4$. Обозначим $d_3 = \gcd\{\deg h : v_h \in S_3\}$, $d_4 = \gcd\{\deg h : v_h \in S_4\}$, $d = \gcd\{d_3, d_4\}$. Если оба множества S_3 и S_4 пустые, то положим $d = \infty$.

Предложение 2.3.3.3. *Пусть $\alpha = \omega_1 + \omega_2\sqrt{f} \in L$, где $\omega_1, \omega_2 \in K[x]$, $\omega_2 \neq 0$, и имеет место* (2.3.3.3). *Положим*

$$u = \alpha \cdot \prod_{v_h \in S_2,\ v_h^+(\alpha) > 0} h^{-r_j}. \tag{2.3.3.4}$$

Тогда справедливы следующие утверждения.

1. *Если $v_\infty \in S$ или $v_\infty^-, v_\infty^+ \in S$, то $u \in U_S$. В частности, если для всех $v_h \in S_2$ имеем $v_h^+(\alpha) = 0$, то α является S-единицей.*

2. *Если $v_\infty^- \in S$, $v_\infty^+ \notin S$, то при $v_\infty^+(u) \equiv 0 \pmod d$ существует S-единица вида* (2.3.3.1), *а при $v_\infty^+(u) \not\equiv 0 \pmod d$ S-единицы такого вида не существует.*

3. *Если $v_\infty \notin S$ или $v_\infty^-, v_\infty^+ \notin S$, то при $v_\infty(u) \equiv 0 \pmod{2d}$ или соответственно $v_\infty^-(u) = v_\infty^+(u) \equiv 0 \pmod d$ существует S-единица вида* (2.3.3.1), *а иначе S-единицы такого вида не существует.*

Доказательство. Аналогично доказательству предложения 2.4 из [130].

Докажем утверждение 1. Если $v_h \notin S_1$, то из (2.3.2.3) и (2.3.2.4) при учете (2.3.3.3) и предложения 2.3.2.1 имеем $v_h^-(\alpha) = v_h^+(\alpha) = 0$. Остается заметить, что для $v_h \notin S_3$ справедливо $v_h^+(\alpha) = 0$ в силу построения (2.3.3.4).

В утверждении 2. требуется построить такой элемент $\beta \in L$ вида (2.3.3.1), для которого кроме условий, которые мы проверили при доказательстве утверждения 1., дополнительно должно выполняться условие $v_\infty^+(\beta) = 0$. Значит, элемент β можно представить в виде $\beta = uH$, где $H \in K(x)$, H является $S_3 \cup S_4$-единицей поля $K(x)$. По определению числа d существует $S_3 \cup S_4$-единица $\gamma \in K(x)$ степени d, и степень любой $S_3 \cup S_4$-единицы кратна d, в том числе, если искомый элемент β существует, то для него $v_\infty^+(H) = v_\infty(H) \equiv 0 \pmod d$. Получается, что $v_\infty^+(u) \equiv 0 \pmod d$ является необходимым условием. Покажем, что это условие является достаточным. Положим $r = v_\infty^+(u)/d$, тогда можно взять $H = \gamma^{-r}$, и для $\beta = u\gamma^{-r}$ выполнено условие $v_\infty^+(\beta) = 0$.

Наконец, в утверждении 3. для искомой S-единицы β вида (2.3.3.1) должны быть выполнены условия $v_\infty^-(\beta) = v_\infty^+(\beta) = 0$. В силу рассуждений, проведенных при доказательстве утверждения 2., для каждого из нормирований v_∞^- и v_∞^+ соотношения $v_\infty^-(u) \equiv 0 \pmod d$ и

$v_\infty^+(u) \equiv 0 \pmod{d}$ являются необходимыми и достаточными соответственно для выполнения условий $v_\infty^-(\beta) = 0$ и $v_\infty^+(\beta) = 0$ по отдельности. Для того, чтобы условия $v_\infty^-(\beta) = 0$ и $v_\infty^+(\beta) = 0$ были выполнены одновременно, значения $r^- = v_\infty^-(u)/d$ и $r^+ = v_\infty^+(u)/d$ должны совпадать, то есть $v_\infty^-(u) = v_\infty^+(u)$. □

В предложении 2.3.3.3 условие (2.3.3.1) на вид искомой S-единицы является существенным, поскольку в поле L могут существовать другие S-единицы другого вида, даже, когда S-единиц вида (2.3.3.1) не существует. Также отметим, что в каждом из утверждений предложения 2.3.3.3 с точностью до умножения на константу из K^* может существовать несколько подходящих под условия S-единиц вида (2.3.3.1), в том числе из-за возможной неоднозначности выбора $S_3 \cup S_4$-единицы $\gamma \in K(x)$ степени d.

Следующее предложение уточняет предложение 2.3.3.3, в случаях, когда для данного $\alpha = \omega_1 + \omega_2\sqrt{f} \in L$, являющегося решением (2.3.3.3), S-единицы вида (2.3.3.1) не существует.

Предложение 2.3.3.4. *Пусть справедливы обозначения предложения 2.3.3.3, бесконечное нормирование поля $K(x)$ имеет два неэквивалентных продолжения $v_\infty^\pm$ на поле L и существует S_∞-единица u_∞ степени m.*

- *Если $v_\infty^- \in S$, $v_\infty^+ \notin S$, то при $v_\infty^+(u) \equiv 0 \pmod{\gcd(m,d)}$ существует S-единица вида $u \cdot H \cdot u_\infty^k$ для некоторого $k \in \mathbb{Z}$ и $H \in U_{S_3 \cup S_4} \subset K(x)$, а при $v_\infty^+(u) \not\equiv 0 \pmod{\gcd(m,d)}$ S-единицы такого вида не существует.*

- *Если $v_\infty^-, v_\infty^+ \notin S$, то при $v_\infty^+(u) - v_\infty^-(u) \equiv 0 \pmod{2m}$ и $v_\infty^+(u) + v_\infty^-(u) \equiv 0 \pmod{2d}$ существует S-единица вида $u \cdot H \cdot u_\infty^k$ для некоторого $k \in \mathbb{Z}$ и $H \in U_{S_3 \cup S_4} \subset K(x)$, а иначе S-единицы такого вида не существует.*

Доказательство. Аналогично доказательству предложения 2.4 из [130].

Пусть $v_\infty^- \in S$, $v_\infty^+ \notin S$ и $v_\infty^+(u) \equiv 0 \pmod{\gcd(m,d)}$. Пусть u_∞ — такая S_∞-единица, что $v_\infty^+(u_\infty) = m$. Пользуясь обозначениями, введенными при доказательстве предложения 2.3.3.3, рассмотрим $\beta = u \cdot \gamma^{-r} \cdot u_\infty^{-k}$, где r и k целочисленные решения уравнения $dr + mk = v_\infty^+(u)$. Тогда $v_\infty^+(\beta) = 0$, и β является S-единицей. В случае $v_\infty^+(u) \not\equiv 0 \pmod{\gcd(m,d)}$ уравнение $dr + mk = v_\infty^+(u)$ не имеет решений в целых числах r и k, поэтому S-единицы вида $u \cdot H \cdot u_\infty^k$ не существует.

Пусть $v_\infty^-, v_\infty^+ \notin S$. Для существования S-единицы вида $u \cdot H \cdot u_\infty^k$ необходимо и достаточно, чтобы система уравнений

$$\begin{cases} dr - mk = v_\infty^-(u), \\ dr + mk = v_\infty^+(u) \end{cases}$$

имела целочисленные решения r, k, что равносильно условиям $v_\infty^+(u) - v_\infty^-(u) \equiv 0 \pmod{2m}$ и $v_\infty^+(u) + v_\infty^-(u) \equiv 0 \pmod{2d}$. □

Для элемента $\alpha \in L$ назовем множество нормирований S поля L *минимальным*, если α является S-единицей поля L и для любого $\hat{S} \subset S$ элемент α не является $\hat{S}$-единицей поля L. Легко видеть, что для любого $\alpha \in L$ существует единственное минимальное множество $S = S_\alpha$, состоящее из конечного числа нормирований.

Следующее предложение 2.3.3.5 в некотором смысле является обратным к предложению 2.3.3.3, а именно в этом предложении по элементу $\alpha \in L$ указан способ, как построить минимальное множество нормирований S, для которого $\alpha \in U_S$.

Скажем, что нормирование v, имеющее два неэквивалентных продолжения v^- и v^+ на поле L, *согласовано* с элементом $\alpha \in L$ вида (2.3.3.1), если $v^+(\alpha) \leq v^-(\alpha)$. Нормирование v^- в этом случае также будем называть согласованным с элементом $\alpha \in L$.

Предложение 2.3.3.5. *Пусть элемент $\alpha \in L$ имеет вид (2.3.3.1) с нормой (2.3.3.2), и S — минимальное множество нормирований для элемента α, каждое из которых согласовано с α. Обозначим $q_j = v_{h_j}(\gcd(\omega_1, \omega_2))$ для $1 \leq j \leq t$ и $n = \max\bigl(\deg(\omega_1^2), \deg(\omega_2^2 f)\bigr)$. Тогда справедливы следующие утверждения*

1. *если для некоторого j, $1 \leq j \leq t$, $v^-_{h_j} = v^+_{h_j}$, то*
   - 1.1. $v^{L/K(x)}_{h_j}(\alpha) = m_j$;
   - 1.2. $v^{L/K(x)}_{h_j} \notin S$ *тогда и только тогда, когда* $m_j = 0$;
2. *если для некоторого j, $1 \leq j \leq t$, $v^-_{h_j} \neq v^+_{h_j}$, то*
   - 2.1. $v^-_{h_j}(\alpha) = m_j + r_j - q_j$, $v^+_{h_j}(\alpha) = q_j - r_j$;
   - 2.2. $v^-_{h_j} \notin S$ *тогда и только тогда, когда* $r_j + m_j = q_j$;
   - 2.3. $v^+_{h_j} \notin S$ *тогда и только тогда, когда* $r_j = q_j = 0$;
3. *если $v^-_\infty = v^+_\infty$, то*
   - 3.1. $v^{L/K(x)}_\infty(\alpha) = -\sum_{j=1}^t m_j \deg h_j$;
   - 3.2. $v^{L/K(x)}_\infty \notin S$ *тогда и только тогда, когда* $\sum_{j=1}^t m_j \deg h_j = 0$;
4. *если $v^-_\infty \neq v^+_\infty$, то*
   - 4.1. $v^-_\infty(\alpha) = n/2 - \sum_{j=1}^t (r_j + m_j) \deg h_j$;
   - 4.2. $v^+_\infty(\alpha) = \sum_{j=1}^t r_j \deg h_j - n/2$;
   - 4.3. $v^-_\infty \notin S$ *тогда и только тогда, когда* $n = 2\sum_{j=1}^t (r_j + m_j) \deg h_j$;
   - 4.4. $v^+_\infty \notin S$ *тогда и только тогда, когда* $n = 2\sum_{j=1}^t r_j \deg h_j$.

Доказательство. Пусть для некоторого j, $1 \le j \le t$, $v_{h_j}^- = v_{h_j}^+$, тогда в силу (2.3.2.5) имеем $v_{h_j}^{L/K(x)}(\alpha) = v_{h_j}^{L/K(x)}(\overline{\alpha}) = m_j$, откуда получаем первое утверждение.

Пусть для некоторого j, $1 \le j \le t$, $v_{h_j}^- \ne v_{h_j}^+$. Обозначим

$$v_{h_j}^- \left(\frac{\omega_1 + \omega_2\sqrt{f}}{\gcd(\omega_1, \omega_2)} \right) = s_j,$$

тогда $v_{h_j}^-(\alpha) = s_j + q_j - r_j$, $v_{h_j}^+(\alpha) = q_j - r_j$. Остается заметить, что в силу (2.3.3.2) выполнено соотношение $s_j + 2q_j = m_j + 2r_j$.

Пусть $v_\infty^- = v_\infty^+$, тогда

$$v_\infty^{L/K(x)}(\alpha) = 2\sum_{j=1}^{t} r_j \deg h_j - n = -\sum_{j=1}^{t} m_j \deg h_j,$$

откуда получаем третье утверждение.

Пусть $v_\infty^- \ne v_\infty^+$, тогда

$$v_\infty^- \left(\omega_1 + \omega_2\sqrt{f} \right) = n - \sum_{j=1}^{t} (2r_j + m_j) \deg h_j, \quad v_\infty^+ \left(\omega_1 + \omega_2\sqrt{f} \right) = -n,$$

откуда получается четвертое утверждение. □

2.3.4. Степень S-единицы

Пусть S — конечное множество неэквивалентных нормирований поля L такое, что $v_\infty \in S$, $S_1 = \{v_{h_1}, \dots, v_{h_t}\} = S|_{K(x)}$, $|S_1| = |S| - 1$. Пусть $\alpha \in U_S$, $\alpha = \omega_1 + \omega_2\sqrt{f}$, где $\omega_1, \omega_2 \in K[x]$, $\omega_2 \ne 0$, $\gcd(\omega_1,\ \omega_2) = 1$, $N(\alpha) = bh_1^{m_1} \dots h_t^{m_t}$, $m_i > 0$.

В этом параграфе будет дано определение степени S-единицы, где S — произвольное конечное множество нормирований поля L (дополнительно см. [17; 151]). По S-единице мы определим дивизор D, имеющий конечный порядок в группе классов дивизоров. В теореме 2.4.7.1 установлена связь между степенью S-единицы и порядком дивизора D.

Степенью S-единицы α называется число $\deg \alpha = \gcd\{v(\alpha) \mid v \in S\}$.

Данное определение степени S-единицы может быть использовано для произвольного множества нормирований S. Однако при наших условиях на множество S удобно использовать альтернативное определение степени S-единицы.

Предложение 2.3.4.1. *Справедливо равенство* $\deg \alpha = \gcd(m_1, \dots, m_t)$.

Доказательство. Если $v_{h_j} \in S_1$ имеет два продолжения $v_{h_j}^-$ и $v_{h_j}^+$, то выполнен п. 1 предложения 2.3.3.5. Если же $v_{h_j} \in S_1$ имеет единственное продолжение $v_{h_j}^- \in S$, то выполнен п. 3 предложения 2.3.3.5. Остается заметить, что $\gcd(m_1, \dots, m_t) \mid v_\infty(\alpha) = \sum m_j \cdot \deg h_j$. □

Отметим, что если $S = \{v_\infty, v_h^-\}$ и $\alpha = \omega_1 + \omega_2\sqrt{f}$ — S-единица, то $\deg \alpha = m$, где $N(\alpha) = bh^m$ (см. [96]).

Мы будем называть S-единицу *и простой*, если ее нельзя представить с точностью до постоянной в виде некоторой степени другой S-единицы. Ясно, что наибольший интерес представляют степени именно простых S-единиц.

2.3.5. S-единицы для двух нормирований

В этом параграфе доказан ряд свойств S-единиц для различных множеств S, состоящих из двух нормирований (см. [17; 130]).

1. Пусть бесконечное нормирование поля $K(x)$ имеет единственное продолжение $v_\infty = v_\infty^{L/K(x)}$ на поле L, и множество S состоит из двух элементов, причем $v_\infty \in S$. При этих предположениях единственным нетривиальным случаем является $S = S_\circ = \{v_\infty, v_h^-\}$, где нормирования $v_h^- \neq v_h^+$ в поле L.

Пусть существует нетривиальная $S_\circ$-единица $u_\circ \in U_\circ$ в поле L, тогда по предложению 2.3.3.1 $u_\circ = (\omega_1+\omega_2\sqrt{f})/h^r$, $r \geq 0$, и по предложению 2.3.3.2 $N(u_\circ) = bh^m$, где $b \in K^*$. Следовательно, $N(\omega_1 + \omega_2\sqrt{f}) = \omega_1^2 - \omega_2^2 f = bh^k$ для $k = 2r + m$ и $\gcd(\omega_1, \omega_2) \in K^*$. По предложению 2.3.3.5 имеем $v_\infty^{L/K(x)}(u_\circ) = -m \deg h$, а также, если $r > 0$, то $v_h^+(u_\circ) = v_h^+\left(\omega_1 + \omega_2\sqrt{f}\right) - r = 0$, $v_h^-(u_\circ) = -r$, следовательно, $k = r = -m$ и $u_\circ = \omega_1 - \omega_2\sqrt{f}$. Если же $r = 0$, то $k = r = -m$ и $u_\circ = \omega_1 + \omega_2\sqrt{f}$. Число m называется *степенью* единицы $u_\circ$.

Рассмотрим теперь обратную задачу — по решению норменного уравнения построить нетривиальную $S_\circ$-единицу. Пусть m — такое минимальное натуральное число, что норменное уравнение

$$\omega_1^2 - \omega_2^2 f = bh^m, \tag{2.3.5.1}$$

где $b \in K^*$, имеет решение в многочленах $\omega_1, \omega_2 \in K[x]$, $\omega_2 \neq 0$. Тогда по предложению 2.3.3.3 либо $\omega_1 + \omega_2\sqrt{f}$, либо $\omega_1 - \omega_2\sqrt{f}$ является фундаментальной $S_\circ$-единицей.

Таким образом, существует не более одной фундаментальной $S_\circ$-единицы α, которую можно искать в виде $\alpha = \omega_1 + \omega_2\sqrt{f}$, $\omega_1, \omega_2 \in K[x]$, $\omega_2 \neq 0$. Вопрос о существовании $S_\circ$-единиц подробно обсуждается в статье [130].

2. Пусть бесконечное нормирование поля $K(x)$ имеет два продолжения v_∞^- и v_∞^+ на поле L, и $S_\infty = \{v_\infty^-, v_\infty^+\}$. В этом случае нетривиальные S-единицы называют просто *единицами*. Группу единиц обозначим U_∞. Пусть существует нетривиальная единица $u_\infty \in U_\infty$ в поле L, тогда по предложению 2.3.3.1 $u_\infty = \omega_1 + \omega_2\sqrt{f}$, $\omega_1, \omega_2 \in K[x]$, а по предложению 2.3.3.2 имеем $N(u_\infty) = b$, где $b \in K^*$.

Обратно, если $\omega_1, \omega_2 \in K[x]$, $\omega_2 \neq 0$, есть решение норменного уравнения

$$\omega_1^2 - f\omega_2^2 = b,\ \omega_2 \neq 0,\ b \in K^*, \quad \deg(\omega_1^2) = \deg(\omega_2^2 f) = 2m, \tag{2.3.5.2}$$

то $u_\infty = u_\infty^\pm = \omega_1 \pm \omega_2\sqrt{f}$ — единица в поле L, причем, если число m минимальное, для которого существует решение (2.3.5.2), то u_∞ является фундаментальной единицей. Число m

называется *степенью* единицы u_∞.

Случай $S = S_\infty$ в проблеме поиска и построения S-единиц называют *классическим*, так как он фактически рассматривался еще в работах Абеля [127] и Чебышева [129]. В настоящее время этот случай рассматривается как модельный, и ему посвящено очень большое количество статей. Среди современных работ стоит отметить [52; 61; 62; 70; 71; 92; 118].

3. Рассмотрим нормирование v_h поля $K(x)$, имеющее два неэквивалентных продолжения v_h^+ и v_h^+ на поле L. Положим $S_h = \{v_h^-, v_h^+\}$ и U_h — группа S_h-единиц в поле L. Пусть существует нетривиальная S_h-единица $u_h \in U_h$, тогда по предложению 2.3.3.1 имеем

$$u_h = (\omega_1 + \omega_2\sqrt{f})/h^m, \quad m \geq 0,\ v_h(\omega_1) = v_h(\omega_2) = 0,\ \max\bigl(\deg(\omega_1^2, \omega_2^2 f\bigr) = 2m, \tag{2.3.5.3}$$

и по предложению 2.3.3.2 получаем $N(u_h) = b$, где $b \in K^*$. По предложению 2.3.3.5 без ограничения общности можем считать, что $v_h^-(u_h) = m$, $v_h^-(u_h) = -m$.

Обратно, если существуют $\omega_1, \omega_2 \in K[x]$, удовлетворяющие

$$\omega_1^2 - f\omega_2^2 = bh^{2m},\ v_h(\omega_2) = 0,\ b \in K^*, \quad \max\bigl(\deg(\omega_1^2),\ \deg(\omega_2^2 f)\bigr) = 2m, \tag{2.3.5.4}$$

то $u_h^\pm = h^{-m}(\omega_1 \pm \omega_2\sqrt{f}) \in U_h$ — нетривиальные S_h-единицы. При этом S_h-единица $u_h \in U_h$ является фундаментальной тогда и только тогда, когда $m \in \mathbb{N}$ — минимальное число, для которого (2.3.5.4) имеет решение в многочленах $\omega_1, \omega_2 \in K[h]$. Без ограничения общности мы можем считать, что $\operatorname{lc}(\omega_1) = 1$ в (2.3.5.3) и (2.3.5.4).

Степенью нетривиальной S_h-единицы $u_h \in U_h$, записанной в виде (2.3.5.3), называется число $\deg u_h = m \in \mathbb{N}$.

4. Докажем ряд утверждений, устанавливающих связь между S-единицами для множеств $S_\circ$, S_∞, S_h.

Предложение 2.3.5.1 ([17]). *1. Пусть $f \in K[x]$ свободный от квадратов многочлен, $\deg f = 2g+1$, $S_\circ = \{v_h^-, v_\infty\}$, $S_h = \{v_h^-, v_h^+\}$, где $v_h^- \neq v_h^+$ в поле L. Поле $L = K(x)(\sqrt{f})$ обладает фундаментальной $S_\circ$-единицей степени m тогда и только тогда, когда поле L обладает фундаментальной S_h-единицей степени m, если m нечетно, и степени $m/2$, если m четно.*

2. Пусть $f \in K[x]$ свободный от квадратов многочлен, $\deg f = 2g+2$, $F(X) = X^{2g+2}f(1/X)$, $\mathcal{L} = K(X)(\sqrt{F})$. Пусть $v_\infty^- \neq v_\infty^+$ в поле L и $v_h^- \neq v_h^+$ в поле $\mathcal{L}$, где $h = X$. Положим $\mathcal{S}_\infty = \{v_\infty^-, v_\infty^+\}$, $S_h = \{v_h^-, v_h^+\}$. Поле L обладает фундаментальной $\mathcal{S}_\infty$-единицей степени m тогда и только тогда, когда поле $\mathcal{L}$ обладает фундаментальной S_h-единицей степени m.

Доказательство. Доказательство первого утверждения следует из разрешимости норменного уравнения вида (2.3.5.1).

Доказательство второго утверждения получается путем отображения $\phi : L \to \mathcal{L}$, заданного заменой $\phi : x \to 1/X$, при котором справедливы соотношения (2.3.2.8) (подробнее см. [8]). □

Пусть $S_0 = \{v_h^-, v_\infty^-\}$, где v_∞^- — одно из двух продолжений нормирования v_∞ поля $K(x)$ на поле L, выбранное подходящим образом (при необходимости мы меняем обозначения v_∞^- и v_∞^- друг на друга). Положим $S_h = \{v_h^-,\ v_h^+\}$, $S_\infty = \{v_\infty^-, v_\infty^+\}$. Для соответствующих нетривиальных единиц поля L, при их существовании, будем использовать обозначения $u_0 \in U_0 = U(S_0)$, $u_h \in U_h = U(S_h)$, $u_\infty \in U_\infty = U(S_\infty)$. Обозначим $\deg U_0$, $\deg U_h$, $\deg U_\infty$ — степени соответствующих фундаментальных единиц.

Для $m, n \in \mathbb{Z}$ обозначим (m, n) и $[m, n]$ соответственно наибольший общий делитель и наименьшее общее кратное m и n.

Предложение 2.3.5.2 ([17]). *Пусть нормирования v_h и v_∞ поля $K(x)$ имеют по два продолжения v_h^-, v_h^+ и v_∞^-, v_∞^+ на поле $L = K(x)(\sqrt{f})$ и справедливо тождество*

$$\omega_1^2 - \omega_2^2 f = bh^m, \quad \text{где } \omega_1, \omega_2 \in K[x], \quad v_h(\omega_2) = 0, \quad b \in K^*. \tag{2.3.5.5}$$

Положим $u = \omega_1 + \omega_2\sqrt{f}$, $2m_1 = \max\big(\deg(\omega_1^2),\ \deg(f\omega_2^2)\big)$. Верны следующие утверждения:

1. если $m = 2m_1$, то $u_h = u \cdot h^{-m_1}$ является нетривиальной S_h-единицей степени m_1, при этом нетривиальные единицы u_0 и u_∞ существуют или не существуют одновременно;

2. если $m_1 < m < 2m_1$, то в поле L существование одной из нетривиальных единиц u_0, u_h, u_∞ влечет существование остальных двух единиц;

3. если $m = m_1$, то $u_0 = u$ является нетривиальной S_0-единицей степени m_1, при этом нетривиальные единицы u_h и u_∞ существуют или не существуют одновременно;

4. если $0 < m < m_1$, то в поле L существование одной из нетривиальных единиц u_0, u_h, u_∞ влечет существование остальных двух единиц;

5. если $m = 0$, то $u_\infty = u$ является нетривиальной S_∞-единицей степени m_1, при этом нетривиальные единицы u_0 и u_h существуют или не существуют одновременно.

Доказательство. 1. Если $m = 2m_1$, то элемент $u_h = u \cdot h^{-m_1}$ является нетривиальной S_h-единицей степени m_1.

Предположим, что в поле L существует S_0-единица u_0 степени m_0, причем без ограничения общности можем считать, что $v_h^-(u_h) = m_1$, $v_h^-(u_0) = m_0$. Пусть $d = (m_0, 2m_1)$, тогда $u_\infty = u_h^{m_0/d} u_0^{-2m_1/d} h^{m_0 m_1/d}$ является S_∞-единицей степени $m_0 m_1/d = [m_0, m_1]$.

Предположим, что в поле L существует S_∞-единица u_∞ степени m_2, причем без ограничения общности можем считать, что $v_h^-(u_h) = m_1$, $v_\infty^-(u_\infty) = m_2$. Пусть $d_1 = (m_1, m_2)$, тогда $u_0 = u_h^{m_2/d} u_\infty^{-m_1/d} h^{m_1 m_2/d}$ является S_∞-единицей степени $2m_1 m_2/d = 2[m_1, m_2]$.

2. Пусть $m_1 < m < 2m_1$. Предположим, что в поле L есть S_0-единица u_0 степени m_0, причем без ограничения общности за счет выбора в качестве S_0-единицы u_0 или u_0^{-1} можем считать, что $v_h^-(u_0) = m_0$. По предложениям 2.3.2.1 и 2.3.2.2 без ограничения общности за счет выбора обозначений $v_h^\pm$ и $v_\infty^\pm h$ имеем

$$v_h^-(u) = m, \quad v_h^+(u) = 0, \quad v_\infty^-(u) = m_1 - m, \quad v_\infty^+(u) = -m_1.$$

Тогда для $d = (m_0, m)$ имеем $u_\infty = u^{m_0/d} u_0^{-m/d}$ — S_∞-единица степени $m_0 m_1/d$.

Остальные случаи рассматриваются аналогично.

Предложение 2.3.5.2 доказано. □

В случае $\deg f = 2g + 1$ из существования решения норменного уравнения (2.3.5.5) следует существование S-единицы степени m, где $S = \{v_h^-, v_\infty\}$, а, значит, и существование S_h-единицы степени m или $m/2$ в зависимости от четности m.

5. Пусть нормирования v_h, v_q поля $K(x)$ имеют по два неэквивалентных продолжения на поле L. Положим $S = \{v_h^-, v_q^-\}$ и U_S — группа S-единиц в поле L. Пусть существует нетривиальная S-единица $\alpha \in U_S$, тогда по предложению 2.3.3.1

$$\alpha = \frac{\omega_1 + \omega_2\sqrt{f}}{h^r q^k}, \quad r, k \in \mathbb{Z}, \tag{2.3.5.6}$$

и по предложению 2.3.3.2 $N(\alpha) = b$, где $b \in K^*$. По предложению 2.3.3.5 без ограничения общности можем считать, что

$$v_h^-(\alpha) = -r, \quad v_h^+(\alpha) = 0, \quad v_q^-(\alpha) = -k, \quad v_q^+(\alpha) = 0,$$
$$v_\infty^-\left(\omega_1 + \omega_2\sqrt{f}\right) = v_\infty^-\left(\omega_1 + \omega_2\sqrt{f}\right) = -r\deg h - k\deg q.$$

Теперь рассмотрим обратную задачу. Предположим, что норменное уравнение

$$\omega_1^2 - \omega_2^2 f = b h^{2r} q^{2k}$$

имеет решение в многочленах $\omega_1, \omega_2 \in K[x]$ таких, что $\omega_2 \neq 0$, $\max\bigl(\deg(\omega_1^2),\ \deg(f\omega_2^2)\bigr) = r\deg h + k\deg q$. Тогда при правильном выборе обозначений $v_h^\pm$ и $v_\infty^\pm$ элемент α вида (2.3.5.6) является S-единицей в поле L.

2.4. Дивизоры

В этом разделе представлено краткое введение в теорию дивизоров в алгебраических функциональных полях. Более подробно с полными доказательствами см., например, [28; 132—134; 138]. Данная глава базируется на понятии плейса (см. параграф 2.3.1) и понятии нормирования в алгебраическом поле функций (см. параграф 2.3.2). Для более геометрической интерпретации теории дивизоров на алгебраических кривых отсылаем читателя, например, к [27].

2.4.1. Определение и основные свойства

Пусть L/K — алгебраическое поле функций от одной переменной с алгебраически замкнутым полем констант K.

Группой дивизоров $\mathrm{Div}(L)$ поля L/K называется свободная абелева группа, порожденная всеми плейсами L/K. Элементы группы $\mathrm{Div}(L)$ называются *дивизорами* поля L/K. Другими

словами, дивизоры — это формальные суммы вида

$$D = \sum_{P \in \mathbb{P}_L} n_P P, \qquad n_P \in \mathbb{Z},$$

причем только конечное число n_P отличны от нуля. *Носителем* дивизора D называется $\operatorname{Supp} D = \{P \in \mathbb{P}_L \mid n_P \neq 0\}$. Дивизор вида $D = P \in \mathbb{P}_L$ называется *простым дивизором*. Для плейса $Q \in \mathbb{P}_L$ и дивизора $D = \sum n_P P \in \operatorname{Div}(L)$ определим функцию $v_Q(D) = n_Q$, тогда

$$D = \sum_{P \in \operatorname{Supp} D} v_P(D)\, P.$$

В группе $\operatorname{Div}(L)$ можно ввести частичный порядок следующим образом: $D_1 \leq D_2$ тогда и только тогда, когда $v_P(D_1) \leq v_P(D_2)$ для любого $P \in \mathbb{P}_L$. Если $D \geq 0$, то дивизор D называется *эффективным*. *Степенью* дивизора D называется $\deg D = \sum v_P(D) \cdot \deg P$. Множество дивизоров степени ноль $\operatorname{Div}^0(L)$ образует подгруппу в $\operatorname{Div}(L)$.

Пусть $0 \neq \alpha \in L$. Обозначим Z и N соответственно множество нулей и полюсов α в $\mathbb{P}_L$. Определим

$$(\alpha)_\circ = \sum_{P \in Z} v_P(\alpha)\, P \quad \text{— дивизор нулей элемента } \alpha,$$

$$(\alpha)_\infty = \sum_{P \in N} v_P(\alpha)\, P \quad \text{— дивизор полюсов элемента } \alpha,$$

$$(\alpha) = (\alpha)_\circ - (\alpha)_\infty \quad \text{— главный дивизор элемента } \alpha.$$

Из (2.3.1.1) следует, что множество главных дивизоров

$$\operatorname{Princ}(L) = \{(\alpha) \mid 0 \neq \alpha \in L\}$$

образует подгруппу в $\operatorname{Div}^0(L)$ (см. теорему 2.2.3.2). Факторгруппа $\Delta^\circ(L) = \operatorname{Div}^0(L)/\operatorname{Princ}(L)$ называется *группой классов дивизоров* L/K. Класс дивизора $D \in \operatorname{Div}(L)$ в $\Delta^\circ(L)$ обозначается $[D]$. Два дивизора $D_1, D_2 \in \operatorname{Div}(L)$ называются *эквивалентными*, $D_1 \sim D_2$, если $[D_1] = [D_2]$, т. е. $D_1 = D_2 + (\alpha)$ для некоторого $\alpha \in L$, $\alpha \neq 0$.

2.4.2. Теорема Римана-Роха

Пространством Римана-Роха дивизора $D \in \operatorname{Div}(L)$ называется

$$\mathscr{L}(D) = \{\alpha \in L \mid (\alpha) \geq -D\} \cup \{0\}.$$

Для $D \in \operatorname{Div}(L)$ справедливы следующие утверждения

- $\alpha \in \mathscr{L}(D)$ тогда и только тогда, когда $v_P(\alpha) \geq -v_P(D)$ для всех $P \in \mathbb{P}_L$;
- $\mathscr{L}(D) \neq \{0\}$ тогда и только тогда, когда есть такой дивизор $\hat{D} \sim D$, что $\hat{D} \geq 0$ и $\mathscr{L}(D) = \mathscr{L}\left(\hat{D}\right)$;

- $\mathscr{L}(D)$ является линейным пространством над K.

Число $\ell(D) = \dim \mathscr{L}(D)$ называется *размерностью* дивизора D.

Для любого дивизора $D \in \mathrm{Div}(L)$ и рационального плейса $P \in \mathbb{P}_L$ справедливо неравенство $\ell(D+P) \leq \ell(D)+1$ и величина $\ell(D)$ конечна.

Пусть $P \in \mathbb{P}_L$ рациональный плейс и $\mathcal{O}_P$ его локальное кольцо (кольцо нормирования). Для алгебраически замкнутого поля K поле $\mathcal{O}_P/P$ канонически изоморфно K. Пусть h — униформизующая максимального кольца P. Тогда любой элемент $\alpha \in L$ может быть представлен в виде *степенного ряда*

$$\alpha = \sum_{j \geq m} a_j h^j, \quad a_j \in K, \quad a_m \neq 0.$$

Поле L/K является полем частных кольца $\mathcal{O}_P$ и может быть вложено в *поле формльных степенных рядов* $K((h))$. Ясно, что если $h \neq t \in P$ — другая униформизующая, то $K((t)) = K((h))$. Получается, что поле формальных степенных рядов зависит только от поля констант K и плейса P, поэтому обозначим его K_P.

Обозначим прямое произведение полей формальных степенных рядов

$$\mathcal{A}^* = \prod_{P \in \mathbb{P}_L} K_P.$$

Множество $\mathcal{A}^*$ является кольцом с операциями покомпонентного сложения и умножения. Скажем, что вектор $\xi \in \mathcal{A}^*$ имеет полюс в $P \in \mathbb{P}_L$, если для координаты $\xi_P \in K_P$ выполнено $m = m_P = v_P(\xi_P) < 0$. Подкольцо $\mathcal{A} \subset \mathcal{A}^*$ с конечным количеством полюсов называется *кольцом аделей*. Поле L естественным образом вкладывается в кольцо аделей $\mathcal{A}$.

Для дивизора $D \in \mathrm{Div}(L)$ определим множество $\mathcal{A}(D) \subset \mathcal{A}$ аделей ξ таких, что $v_P(\xi_P) \geq -v_P(D)$. Ясно, что $\mathcal{A}(D)$ является векторным K-подпространством $\mathcal{A}$. Множество $L \cap \mathcal{A}(D)$ можно отождествить с пространством Римана-Роха $\mathscr{L}(D)$ над полем K. Множество всех $\mathcal{A}(D)$ образует фундаментальную систему окрестностей в окрестности 0 в $\mathcal{A}$ и, следовательно, $\mathcal{A}$ становится топологическим кольцом (см. [152]).

Пусть $D_1, D_2 \in \mathrm{Div}(L)$. Тогда $\mathcal{A}(D_2) \subset \mathcal{A}(D_1)$ тогда и только тогда, когда $D_2 \leq D_1$. В этом случае

- $[\mathcal{A}(D_1) : \mathcal{A}(D_2)] = \deg D_1 - \deg D_2$;
- $[\mathcal{A}(D_1) : \mathcal{A}(D_2)] = [(\mathcal{A}(D_1) + L) : (\mathcal{A}(D_2) + L)] + [(\mathcal{A}(D_1) \cap L) : (\mathcal{A}(D_2) \cap L)]$.

Существует дивизор $D \in \mathrm{Div}(L)$ такой, что $\mathcal{A} = \mathcal{A}(D) + L$. Это означает, что элементы поля L/K образуют решетку в $\mathcal{A}$, и $\mathcal{A}(D)$ является фундаментальной областью для этой решетки.

Обозначим $\boldsymbol{i}(D) = [\mathcal{A} : \mathcal{A}(D) + L]$, тогда для любых дивизоров $D_1, D_2 \in \mathrm{Div}(L)$ имеем

$$\ell(D_1) - \deg D_1 - \boldsymbol{i}(D_1) = \ell(D_2) - \deg D_2 - \boldsymbol{i}(D_2).$$

Величина $\deg D - \ell(D)$ ограничена постоянной, зависящей только от поля L/K. Число

$$g = \max\{\deg D - \ell(D) + 1 \mid D \in \mathrm{Div}(L)\}$$

называется *родом* поля L/K. Таким образом, имеем $\ell(D) - \deg D - \boldsymbol{i}(D) = 1 - g$.

Теорема (Римана)**.** *Пусть поле функций L/K имеет род g. Тогда для всех дивизоров $D \in \mathrm{Div}(L)$*

$$\ell(D) \geq \deg D + 1 - g.$$

Для дивизора $D \in \mathrm{Div}(L)$ число $\boldsymbol{i}(D) = \ell(D) - \deg D + g - 1$ называется *индексом специальности*. Дивизор D называется *неспециальным*, если $\boldsymbol{i}(D) = 0$; в противном случае дивизор D называется *специальным*.

Дифференциалом ω поля L/K называется K-линейный функционал на $\mathcal{A}$, который обращается в ноль на некотором $\mathcal{A}(D)$ и на L/K (имеется ввиду образ L/K в $\mathcal{A}$). Если $\xi \in \mathcal{A}$ и $y \in L$, то положим $(y\omega)(\xi) = \omega(y\xi)$, причем функционал $y\omega$ обращается в ноль на $\mathcal{A}(D + (y))$.

Множество $\mathcal{A}(D)$ называется *параллелотопом*.

Для дифференциала ω существует максимальный параллелотоп $\mathcal{A}(D)$, на котором ω обращается в ноль. Множество дифференциалов образует одномерное K-пространство. Таким образом, если ω обращается в ноль на $\mathcal{A}(D)$, то $y\omega$ обращается в ноль на $\mathcal{A}(D + (y))$. Это означает, что множеству дифференциалов соответствует единственный класс эквивалентных дивизоров, называемый *канонический класс дивизоров*.

Теорема (Римана-Роха)**.** *Для произвольного дивизора $D \in \mathrm{Div}(L)$ имеем*

$$\ell(D) = \deg D + 1 - g + \ell(W - D),$$

где W — канонический дивизор (дивизор из канонического класса). Следовательно,

$$\boldsymbol{i}(D) = \ell(W - D).$$

Если W — канонический дивизор, то $\ell(W) = g$, $\deg W = 2g - 2$. Таким образом, если $\deg D \geq 2g - 2$, то $\boldsymbol{i}(D) = 0$.

Теорема (Формула Гурвица для рода)**.** *Пусть K — алгебраически замкнутое поле, L/K — поле функций. Пусть E/K есть конечное сепарабельное расширение поля L/K степени n. Положим g_L — род поля L/K и g_E — род поля E/K. Предположим, что для любого плейса $P \in \mathbb{P}_L$ и любого плейса $Q \in \mathbb{P}_E$, лежащего над P, индекс ветвления e_Q взаимно прост с характеристикой поля K. Тогда*

$$2g_E - 2 = n(2g_L - 2) + \sum_Q (e_Q - 1).$$

2.4.3. Неособые кривые и алгебраические поля функций

Пусть V — неособая проективная кривая над алгебраически замкнутым полем K и $L = K(V)$ — ее поле функций. Существует взаимно однозначное соответствие между K-точками $P \in V(K)$ и рациональными плейсами поля функций L/K, ставящее в соответствие точке P максимальный идеал $\mathcal{M}_P(V)$ локального кольца $\mathcal{O}_P(V)$. Это соответствие позволяет перенести определения и результаты полученные для алгебраических полей функций на алгебраические кривые (и обратно тоже). В качестве примеров приведем следующие понятия:

- *род* кривой V — это род поля функций $K(V)$;
- *дивизор* V — это формальная сумма $D = \sum_{P \in V} n_P P$, где $n_P \in \mathbb{Z}$ и только конечное количество n_P отличны от нуля; *степень* дивизора D равна $\deg D = \sum_{P \in V} n_P$; все дивизоры V образуют *группу дивизоров* $\mathrm{Div}(V)$; дивизоры степени ноль образуют подгруппу в $\mathrm{Div}(V)$, обозначаемую $\mathrm{Div}^0(V)$;
- *кратность* точки P рациональной функции $f \in K(V)$ есть $v_P(f)$, определяется через v_P — дискретное нормирование $K(V)$, соответствующее кольцу нормирования $\mathcal{O}_P(V)$;
- *главный дивизор* (f) рациональной функции $0 \neq f \in K(V)$ есть $(f) = \sum_{P \in V} v_P(f)\, P$; степень главного дивизора равна нулю;
- множество главных дивизоров $\mathrm{Princ}(V)$ образует подгруппу в $\mathrm{Div}^0(V)$; факторгруппа $\mathrm{Jac}(V) = \mathrm{Div}^0(V)/\mathrm{Princ}(V)$ называется *якобианом* V;
- для дивизора $D \in \mathrm{Div}(V)$ пространство $\mathcal{L}(D)$ определено также, как в случае функциональных полей; это конечно-мерное пространство над K, размерность которого можно определить с помощью теоремы Римана-Роха.

2.4.4. Кривые над не алгебраически замкнутыми полями

Пусть теперь K — совершенное поле и $\overline{K}$ — его замыкание. Рассмотрим проективную кривую $V \subseteq \mathbf{P}^n(\overline{K})$ определенную над K. Тогда поле $K(V)$ K-рациональных функций V является алгебраическим полем функций над K с одной переменной.

Дивизор $D = \sum_{P \in V} n_P P \in \mathrm{Div}(V)$ определен над K, если $D^\sigma = D$ для всех автоморфизмов $\sigma \in \mathcal{G}_{\overline{K}/K}$ (то есть $n_{P^\sigma} = n_P$ для всех $P \in V$). Дивизоры кривой V, определенные над K, образуют подгруппу $\mathrm{Div}_K(V) = \mathrm{Div}(V/K) \subseteq \mathrm{Div}(V)$. Для дивизора $D \in \mathrm{Div}_K(V)$ определено пространство $\mathscr{L}_K(D) = K(V) \cap \mathscr{L}(D)$. Это конечно-мерное K-векторное пространство, и его размерность над K равна размерности $\mathscr{L}_K(D)$ над $\overline{K}$, (см., например, [28], теорема 3.6.3(d)).

Эффективный дивизор $Q \in \mathrm{Div}_K(V)$ называется *простым дивизором* V/K, если Q не может быть представлен в виде суммы двух эффективных дивизоров $Q = Q_1 + Q_2$, $Q_1, Q_2 \in$

$\mathrm{Div}_K(V)$. Ясно, что $\mathrm{Div}_K(V)$ является свободной абелевой группой, порожденной простыми дивизорами. Простые дивизоры V/K соответствуют плейсам поля функций $K(V)/K$; в частности, K-рациональные точки V (как дивизоры степени один) соответствуют плейсам $K(V)/K$ степени один.

Есть еще один способ определить K-точки и K-рациональные функции и т.п. на многообразии, определенном над полем K, который опирается на действии группы Галуа $\mathcal{G}_{\overline{K}/K}$ на множествах $\mathbf{A}^n(\overline{K})$, $\mathbf{P}^n(\overline{K})$, $\overline{K}[X_1,\ldots,X_n]$, V, $\Gamma(V)$, $\overline{K}(V)$, и т.п. Для примера рассмотрим определенное над K проективное многообразие $V \subseteq \mathbf{P}^n(\overline{K})$, точку $P = (a_0 : \ldots : a_n) \in V$ и автоморфизм $\sigma \in \mathcal{G}_{\overline{K}/K}$; тогда $P^\sigma = (a_0^\sigma : \ldots : a_n^\sigma)$. Легко увидеть, что

$$V(K) = \{P \in V \mid P^\sigma = P \text{ для всех } \sigma \in \mathcal{G}_{\overline{K}/K}\},$$
$$K(V) = \{f \in \overline{K}(V) \mid f^\sigma = f \text{ для всех } \sigma \in \mathcal{G}_{\overline{K}/K}\}.$$

Произвольному плейсу $P \in \mathbb{P}_L$ поля L/K можно поставить в соответствие множество точек $V_P = \{Q \in V \mid \mathcal{M}_Q(V) \subseteq P\}$. Ясно, что для всех $\sigma \in \mathcal{G}_{\overline{K}/K}$ выполнено $\sigma(V_P) = V_P$ и $P = \bigcap\limits_{Q \in V_P} \mathcal{M}_Q(V)$. Обратно, для произвольной точки $Q \in V$ рассмотрим множество $V_Q(K) = \{\sigma(Q) \mid \sigma \in \mathcal{G}_{\overline{K}/K}\}$. Тогда множество функций $\{f \in \overline{K}(V) \mid f(Q) = 0 \text{ для всех } Q \in V_Q(K)\} \subseteq L/K$ является максимальным идеалом некоторого кольца нормирования $\mathcal{O}$ поля L/K и, следовательно, является плейсом P, причем $V_P = V_Q(K)$.

2.4.5. Приведенные дивизоры и представление Мамфорда

В этом параграфе используются обозначения §2.2.1 и §2.3.2. Подробнее о приведенных дивизорах и представлении Мамфорда см. [48; 97; 146]. Актуальные приложения теории дивизоров и представления Мамфорда к проблеме кручения в якобианах гиперэллиптических кривых см. в [11; 153—156].

Пусть K — поле, характеристики отличной от 2. Пусть $L = L/K = K(C)$ — алгебраическое поле функций гиперэллиптической кривой C, заданной уравнением $y^2 = f(x)$, где $f(x) \in K[x]$ — свободный от квадратов многочлен, $2g+1 \leq \deg f \leq 2g+2$. Пусть $\mathrm{Div}(L) = \mathrm{Div}(L/K) = \mathrm{Div}_K(C)$ — группа дивизоров поля L.

Сопряженным к плейсу $P = t \cdot \mathcal{O} \in \mathbb{P}_L$, $t \in L$, называется плейс $\iota P = \iota t \cdot \mathcal{O} \in \mathbb{P}_L$, Таким образом, гиперэллиптическая инволюция ι продолжается на группу дивизоров $\mathrm{Div}(L)$.

Наибольшим общим дивизором двух эффективных дивизоров $D_1, D_2 \in \mathrm{Div}(L)$, $D_1 = \sum_{P \in C} m_P P$ и $D_2 = \sum_{P \in C} n_P P$ называется эффективный дивизор

$$\mathrm{gcdiv}\,(D_1,\ D_2) = \sum_{P \in C} \min(m_P,\ n_P) P.$$

Для $\alpha, \beta \in L$ положим $\mathrm{gcdiv}\,(\alpha,\ \beta) = \mathrm{gcdiv}\,((\alpha)_\circ,\ (\beta)_\circ)$.

Лемма 2.4.5.1. *Пусть $\alpha, \beta \in L$, тогда*

1) $\operatorname{gcdiv}(\alpha,\ \beta) = \operatorname{gcdiv}(\alpha,\ \alpha+\beta)$;

2) $\iota \operatorname{gcdiv}(\alpha,\ \beta) = \operatorname{gcdiv}(\iota\alpha,\ \iota\beta)$.

Доказательство. Имеем

$$\operatorname{gcdiv}(\alpha,\ \beta) = \sum \min\bigl(v(\alpha), v(\beta)\bigr)\cdot v = \sum \min\bigl(v(\alpha), v(\alpha+\beta)\bigr)\cdot v = \operatorname{gcdiv}(\alpha,\ \alpha+\beta),$$
$$\iota \operatorname{gcdiv}(\alpha,\ \beta) = \sum \min\bigl(\iota v(\alpha), \iota v(\beta)\bigr)\cdot v = \sum \min\bigl(v(\iota\alpha), v(\iota\beta)\bigr)\cdot v = \operatorname{gcdiv}(\iota\alpha,\ \iota\beta).$$

□

В частности, для $U, V, W \in K[x]$, $\gcd(V,\ W) \in K^*$, из леммы 2.4.5.1 следует

$$2\operatorname{gcdiv}\left(V + W\sqrt{f},\ V - W\sqrt{f}\right) = \operatorname{gcdiv}(V,\ f),$$
$$\operatorname{gcdiv}\left(V + W\sqrt{f},\ U\right) = \iota \operatorname{gcdiv}\left(V - W\sqrt{f},\ U\right).$$

Лемма 2.4.5.2. *Элемент $\alpha \in L$ может быть записан в виде $\alpha = V + W\sqrt{f}$, $V, W \in K[x]$, тогда и только тогда, когда* $\operatorname{Supp}(\alpha)_\infty \subset \{\infty^-, \infty^+\}$.

Доказательство. Необходимость очевидна, докажем достаточность. Пусть дан элемент $\alpha = (V + W\sqrt{f})/U \in L$, где $U, V, W \in K[x]$, $\gcd(U,\ V,\ W) \in K^*$, и $\operatorname{Supp}(\alpha)_\infty \subset \{\infty^-, \infty^+\}$. Если $\deg U > 0$, то найдется нормирование $v \in \mathcal{V} \setminus \{v_\infty^-, v_\infty^+\}$ такое, что $v(U) > 0$ и $v(V + W\sqrt{f}) = 0$, поскольку иначе по лемме 2.4.5.1 имеем $\gcd(U,\ V,\ W) \in K[x] \setminus K$, что неверно по предположению. Следовательно, $v((\alpha)_\infty) > 0$, но это противоречит условию $\operatorname{Supp}(\alpha)_\infty \subset \{\infty^-, \infty^+\}$. □

В случае, когда элемент $\alpha \in L$ может быть записан в виде $\alpha = V + W\sqrt{f}$, $V, W \in K[x]$, будем писать $\alpha \in K[x][\sqrt{f}]$.

Эффективный дивизор $D \in \operatorname{Div}(L)$ называется *полуприведенным*, если $2(D \cap \iota D) \le (f)_{[2g+2]}$, где $(f)_{[2g+2]} = (f)_\circ$, если $\infty^- \ne \infty^+$, и $(f)_{[2g+2]} = (f)_\circ + \infty$, если $\infty^- = \infty^+ = \infty$. Полуприведенный дивизор $D \in \operatorname{Div}(L)$ называется *приведенным*, если $\deg D = g$.

Пусть K — алгебраически замкнутое поле характеристики, отличной от 2. Пусть $D \in \operatorname{Div}_0(L/K)$ и $B \in \operatorname{Div}(L/K)$, $\deg B = g$. По теореме Римана-Роха (см. §2.4.2)

$$\ell(D+B) = \ell(W - D - B) + \deg(D+B) + 1 - g.$$

Имеем $\ell(D+B) \ge 1$, поскольку $\deg(D+B) = g$ и $\ell(W - D - B) \ge 0$. Следовательно, существует функция $\alpha \in \mathscr{L}(D+B)$, $\alpha \ne 0$, такая, что $(\alpha) + D + B \ge 0$, и корректно определен эффективный дивизор $E = (\alpha) + D + B$, $\deg E = g$, то есть $D \in \operatorname{Div}_0(L/K)$. Получается, что при фиксированном дивизоре B для любого дивизора $D \in \operatorname{Div}_0(L/K)$ найдется *канонический представитель* $E - B$ в якобиане $J(L/K)$, $[E - B] \in J(L/K)$.

Пусть B — приведенный дивизор и дивизор $D \in \mathrm{Div}_0(L/K)$ такой, что $D = D_0 - D_\infty$ и эффективный дивизор $D_0 + \iota D_\infty + B$ является полуприведенным. Тогда найдется приведенный дивизор E такой, что $E - B$ — канонический представитель дивизора D в якобиане $J(L/K)$. В случае $\infty^- = \infty^+$ (что не является критическим ограничением) доказательство этого факта приведено в [97] или в гл. IIIa [48]. В общем случае набросок конструктивного доказательства приведен в §5.1.2.

Теорема 2.4.5.3. I. *Пусть* $D = \sum m_i P_i$ *— полуприведенный дивизор. Положим*

$$U(x) = \prod_i \prod_{Q_{ij} \in V_{P_i}} (x - x(Q_{ij}))^{m_i} \in K[x].$$

Существует единственный многочлен $V \in K[x]$*, удовлетворяющий условиям:*

1) $\deg V < \deg U$*;*

2) $V - y \in P_i$ *для всех номеров* i*, для которых* $m_i \neq 0$*;*

3) $U \mid V^2 - f$*.*

Тогда $D = \mathrm{gcdiv}\left((U),\ (V - y)\right)$*.*

II. *Пусть* $U, V \in K[x]$ *такие, что* $\deg V < \deg U$*. Если* $U \mid V^2 - f$*, то* $D = \mathrm{gcdiv}\left((U),\ (V - y)\right)$ *— полуприведенный дивизор.*

Доказательство. См., например, [97]. □

Представление полуприведенного дивизора D вида $D = \mathrm{gcdiv}\left((U),\ (V - y)\right)$ называется *представлением Мамфорда* (см. [48]). Другими словами, *представление Мамфорда полуприведенного дивизора* D называется пара многочленов (U, V) такая, что $D = \mathrm{gcdiv}\left((U),\ (V - y)\right)$. Иногда в качестве *представления Мамфорда* рассматривают тройку многочленов (U, V, U_1), где $U_1 = (V^2 - f)/U$.

В §§5.2-5.4 мы будем заново в частном порядке давать определение представления Мамфорда для каждого из рассматриваемых там случаев.

Следующая лемма в случае $\deg f = 2g + 1$ и $K = \mathbb{C}$ доказана в [48], шаг II §2 гл. IIIa, поэтому называется *леммой Мамфорда*. Мы докажем ее без дополнительных ограничений на степень многочлена f и поле K.

Лемма 2.4.5.4. *Если* $\alpha \in L$*,* $\alpha \neq 0$*, причем* $\deg(\alpha)_\circ \leq g$*, то* $\alpha \in K(x)$*.*

Доказательство. Пусть $\alpha = (V - W\sqrt{f})/U \in L$, где $U, V, W \in K[x]$ такие, что $\gcd(U,\ V,\ W) = 1$. Предположим, что $W \neq 0$ и $\deg(\alpha)_\infty = \deg(\alpha)_\circ \leq g$. Обозначим $N_\infty^- = -v_\infty^-\left(V - W\sqrt{f}\right)$ и $N_\infty^+ = -v_\infty^+\left(V - W\sqrt{f}\right)$. По предложению 2.3.2.2 имеем $\max\left(N_\infty^-, N_\infty^+\right) \geq \deg f/2 > g$. Распи-

шем подробно степень дивизора полюсов функции α:

$$\deg(\alpha)_\infty = 2\deg U - \deg \operatorname{gcdiv}\left(V - W\sqrt{f},\ U\right) +$$
$$+ \max\bigl(0, N_\infty^- - \deg U\bigr) + \max\bigl(0, N_\infty^+ - \deg U\bigr) \geq$$
$$\geq \max\bigl(\deg U, N_\infty^-\bigr) + \max\bigl(\deg U, N_\infty^+\bigr) - \deg U \geq \max\bigl(N_\infty^-, N_\infty^+\bigr),$$

что противоречит предположению $\deg(\alpha)_\infty \leq g$. □

2.4.6. Алгоритм Кантора для сложения двух приведенных дивизоров

Пусть $L = K(x)(\sqrt{f})$, $\deg f = 2g+1$. Сформулируем два алгоритма, представленных Кантором (см. [49]), которые позволяют по представлениям Мамфорда двух приведенных дивизоров $D_1, D_1 \in \mathrm{Div}_K^0(L)$ найти представление Мамфорда приведенного дивизора D такого, что $D \sim D_1 + D_2$. В этом параграфе, согласно статье [49], мы считаем, что все приведенные и полуприведенные дивизоры имеют вид $D = D_\circ - \deg D \cdot \infty$, где $D_\circ$ — эффективный дивизор.

Алгоритм 1. Алгоритм Кантора сложения дивизоров.

1: **Дано:** приведенные дивизоры $D_1, D_2 \in \mathrm{Div}_K^0(L)$, $D_1 = (U_1,\ V_1)$, $D_2 = (U_2,\ V_2)$.
2: Используя расширенный алгоритм Евклида, **вычислить** $d_1, e_1, e_2 \in K[x]$, где $d_1 = \gcd(U_1,\ U_2)$ и $d_1 = e_1U_1 + e_2U_2$;
3: используя расширенный алгоритм Евклида, **вычислить** $d, \omega_1, \omega_2 \in K[x]$, где $d = \gcd(d_1,\ V_1 + V_2)$ и $d_1 = \omega_1 d_1 + \omega_2(V_1 + V_2)$;
4: **вычислить** $\lambda_1 = \omega_1 e_1$, $\lambda_2 = \omega_1 e_2$, $\lambda_3 = \omega_2$, причем $d = \lambda_1 U_1 + \lambda_2 U_2 + \lambda_3(V_1 + V_2)$.
5: **вычислить**

$$U = \frac{U_1U_2}{d^2}, \qquad V \equiv \frac{\lambda_1U_1V_2 + \lambda_2U_2V_1 + \lambda_3(V_1V_2 + f)}{d} \pmod{U}.$$

6: **Вернуть:** полуприведенный дивизор $D \in \mathrm{Div}_K$, $D = (U,\ V)$, $D \sim D_1 + D_2$.

Алгоритм 2. Алгоритм редукции полуприведенных дивизоров.

1: **Дано:** полуприведенный дивизор $D \in \mathrm{Div}_K^0$, $D = (U,\ V)$.
2: **Вычислить**

$$U' = \frac{f - V^2}{U}, \qquad V' \equiv -V \pmod{U}'.$$

;
3: **если** $\deg U' > g$, **то** положить $U := U'$, $V := V'$ и перейти к шагу 2.;
4: **вычислить** $U' := \frac{U'}{c}$, где c — старший коэффициент U'.
5: **Вернуть:** полуприведенный дивизор $D \in \mathrm{Div}_K$, $D = (U,\ V)$, $D \sim D_1 + D_2$.

2.4.7. Дивизоры и S-единицы

Напомним, что *порядком класса дивизора* $[D]$ в группе классов дивизоров степени ноль $\Delta^\circ(L)$ называется минимальное натуральное число $m = \operatorname{Ord} \mathrm{D}$ такое, что дивизор mD эквивалентен дивизору некоторой функции $\beta \in L$. Если такого m не существует, то положим $\operatorname{Ord} \mathrm{D} = \infty$.

Понятие степени S-единицы в арифметике кольца S-целых элементов тесно связано с понятием порядка класса дивизора в группе классов дивизоров степени ноль. Эта связь указана в теореме 2.4.7.1, но пред тем, как ее сформулировать, мы должны для S-единицы дать следующее определение.

Дивизором кручения S-единицы α называется дивизор

$$D_\alpha = \frac{(\alpha)}{\deg \alpha}.$$

В §2.3.3 обсуждалось, что без ограничения общности можно рассматривать только множества S такие, что для любого $v \in S$ выполнено $v \neq \iota v$ и $\iota v \notin S$.

Пусть $L = K(x)(\sqrt{f})$, $\deg f = 2g+1$. Пусть $S = \{v^-_{h_1}, \dots, v^-_{h_t}, \infty\}$ и $\alpha \in U_S$. Обозначим $m_j = v^-_{h_j}(\alpha)$. Тогда дивизор кручения D_α мы можем записать в явном виде:

$$D_\alpha = \sum_{j=1}^{t} \frac{m_j}{d} (h_j)^-, \quad \text{где } d = \gcd(m_1, \dots, m_t). \tag{2.4.7.1}$$

Назовем набор $u_1, \dots, u_e$ некоторых S-единиц *независимым*, если из соотношения $u_1^{\lambda_1} \cdot \ldots \cdot u_e^{\lambda_e} \in K^*$ следует, что $\lambda_1 = \ldots = \lambda_e = 0$. Набор S-единиц $u_1, \dots, u_e$ называется *полным*, если для любого $\alpha \in U_S$ найдутся $\lambda_1, \dots, \lambda_e \in \mathbb{Z}$ и $b \in K^*$ такие, что $\alpha = b u_1^{\lambda_1} \cdot \ldots \cdot u_e^{\lambda_e}$. Полный набор независимых S-единиц $u_1, \dots, u_e$ называется *базисом* группы U_S или *системой фундаментальных* S-единиц. В случае, когда базис состоит из одного элемента u_1, то есть группа U_S изоморфна $K^* \times \mathbb{Z}$, S-единицу u_1 будем называть *фундаментальной*.

Теорема 2.4.7.1. *Пусть $u_1, \dots, u_e$ — базис группы S-единиц U_S и элемент $\alpha \in U_S$ имеет вид*

$$\alpha = b u_1^{\lambda_1} \cdot \ldots \cdot u_e^{\lambda_e}, \qquad \text{где} \quad \lambda_j \in \mathbb{Z}, \quad b \in K^*.$$

Тогда порядок дивизора кручения D_α выражается следующей формулой

$$\operatorname{Ord} \mathrm{D}_\alpha = \frac{\deg \alpha}{\gcd(\lambda_1, \dots, \lambda_e)}. \tag{2.4.7.2}$$

Доказательство. Обозначим $d = \gcd(\lambda_1, \dots, \lambda_e)$ Без ограничения общности можем считать, что $d = 1$, поскольку в противном случае вместо α можно рассмотреть $\hat{\alpha} = \alpha^{1/d}$.

Итак, при условии $d = 1$ имеем $\deg \alpha \cdot D_\alpha = (\alpha)$, и, следовательно, $\operatorname{Ord} \mathrm{D}_\alpha \leq \deg \alpha$. Пусть $\operatorname{Ord} \mathrm{D}_\alpha \cdot D_\alpha = (\beta)$ для некоторой функции $\beta \in L$. Исходя из вида дивизора функции β получаем, что $v(\beta) = 0$ для всех для всех нормирований v, не принадлежащих S, поэтому

β является S-единицей, а значит имеет вид $\beta = b_1 u_1^{\gamma_1} \cdot \ldots \cdot u_e^{\gamma_e}$. Пусть $\deg \alpha = \text{Ord } \mathrm{D}_\alpha \cdot q + z$, $0 \le z < \text{Ord } \mathrm{D}_\alpha$. Тогда $z \cdot D_\alpha = (\alpha) - q \cdot (\beta) = \left(\frac{\alpha}{\beta^q}\right)$, а в силу минимальности Ord D_α получаем $z = 0$ и $u = b_2 \beta^q$. Из единственности разложения

$$bu_1^{\lambda_1} \cdot \ldots \cdot u_e^{\lambda_e} = \alpha = b_2 \beta^q = b_3 u_1^{q\gamma_1} \cdot \ldots \cdot u_e^{q\gamma_e}$$

заключаем, что $\lambda_j = q\gamma_j$, $j = 1, \ldots, e$. Учитывая, что $\gcd(\lambda_1, \ldots, \lambda_e) = 1$, имеем $q = 1$, следовательно, $\alpha = b_4 \beta$, Ord $\mathrm{D}_\alpha = \deg \alpha$. □

В качестве следствия из теоремы 2.4.7.1 отметим, что для фундаментальной S-единицы α справедливо равенство Ord $\mathrm{D}_\alpha = \deg \alpha$.

В статье [130] для множества нормирований S приведено индуктивное построение системы фундаментальных S-единиц $\varepsilon_1, \ldots, \varepsilon_t$ над конечным полем $\mathbb{F}_q$. Существенным моментом в этом построении является наличие фундаментальной S_i'-единицы δ_i для каждого i, $1 \le i \le t$, $S_i' = \{v_\infty, v_i^-\}$. В случае произвольного поля (например, поля характеристики 0) на это полагаться уже нельзя.

Глава 3. Функциональные непрерывные дроби

Эта глава посвящена исследованию функциональных непрерывных дробей и их свойств таких, как периодичность и квазипериодичность (§3.1.6, §3.1.7, §3.2.1, §3.2.3), свойство наилучшего приближения (§3.1.8), связь с уравнениями типа Пелля (§3.1.8, §3.2.1, §3.2.2) и с нетривиальными единицами и S-единицами гиперэллиптического поля (§3.2.1, §3.3.3). Также в этой главе рассматриваются вопросы о строении функциональной непрерывной дроби: симметрии периодов и квазипериодов (§3.1.6, §3.1.7, §3.2.5), оценки на длины предпериодов, квазипериодов и периодов (§3.1.2, §§3.3.2-3.3.4). Основные результаты и утверждения снабжены показательными примерами и контрпримерами (§3.2.4, §3.2.5, §3.3.4). Исследования ведутся как элементарным методом, так и с помощью анализа дивизоров объектов, связанных с функциональными непрерывными дробями. Отдельное внимание заслуживают вычислительные приложения функциональных непрерывных дробей. Для поиска точек конечного порядка в якобиане гиперэллиптической кривой стандартной техникой является использование алгоритма Кантора (§2.4.6) и его обобщений (см., например, [139]). В §3.2.4 для этой задачи предложены эффективные алгоритмы, основанные на применении функциональных непрерывных дробей (см. также §3.1.4 и [66]).

Отдельно отметим раздел 3.3, в котором получены оценки сверху на длины периодов и квазипериодов функциональных непрерывных дробей произвольных элементов гиперэллиптического поля (см. теоремы 3.3.2.3, 3.3.2.4 и следствие 3.3.2.4). В теореме 3.3.3.3 и следствии 3.3.3.5 найдены точные оценки на длину периода и длину квазипериода непрерывной дроби для "ключевых" элементов вида $\sqrt{f}/x^s$ гиперэллиптического поля $L = K(x)(\sqrt{f})$, определенного над полем K алгебраических чисел.

Найденные оценки являются точными как в случае, когда гиперэллиптическое поле задается многочленом четной степени, так и в случае, когда гиперэллиптическое поле задается многочленом нечетной степени. Особенность четного случая заключается в том, что длина квазипериода может быть в несколько раз больше степени фундаментальной S-единицы (см. соответствующие примеры в §3.3.4). В связи с этим неожиданным свойством, в §3.3.6 доказано, что в каждом гиперэллиптическом поле, обладающим периодическими элементами, найдется такой элемент, длина периода которого больше любого наперед заданного числа. В §3.3.5 для гиперэллиптического поля L, определенного над полем K алгебраических чи-

сел, доказана теорема 3.3.5.1 о конечности множества таких дискриминантов D, что найдется элемент $\alpha \in L$ с дискриминантом D, обладающий квазипериодическим разложением в непрерывную дробь. В §3.3.7 найденные результаты проиллюстрированы на случае, когда базовое поле K является квадратичным расширением поля $\mathbb{Q}$.

Результаты Главы 3 опубликованы в статьях [3; 10; 13], [14; 17; 19; 20].

3.1. Понятие функциональной непрерывной дроби и основные свойства

В этом разделе изложена теория функциональных непрерывных дробей, связанных с нормированиями первой степени. Мы вводим понятие функциональной непрерывной дроби для элементов гиперэллиптических полей и рассматриваем их основные свойства. Разложение функции в функциональную непрерывную дроби носит локальный характер, поскольку зависит от выбранного нормирования (или с геометрической точки зрения — строится в выбранной точке кривой). В некотором смысле можно установить аналогию между разложением функции в непрерывную дробь и разложением в степенной ряд. И то и другое понятие помогают в изучении локальных свойств функции или объектов, связанных с этой функцией. Так, например, применение теории функциональных непрерывных дробей к проблеме кручения в якобиане гиперэллиптической кривой дает ответ о порядке точки кручения в якобиане, но не дает описание подгруппы кручения целиком.

Среди базовых свойств функциональных непрерывных дробей можно выделить следующие: свойство сходимости по выбранному нормированию, свойство наилучшего приближения, свойство периодичности или квазипериодичности (см. [62—64; 92; 118; 157], [65—67],[61; 68—70; 113; 114]). В частности, благодаря этим свойствам удается установить глубокую связь между проблемой решения функциональных уравнений типа Пелля, проблемой существования фундаментальных единиц и S-единиц в гиперэллиптических полях, проблемой кручения в якобианах гиперэллиптических кривых [17; 92]. За счет универсальной арифметической структуры теория функциональных непрерывных дробей позволяет получить не только теоретические результаты в указанных проблемах, но и сформулировать новые вычислительные подходы. Эффективные алгоритмы построения непрерывных дробей (см. [62; 66]), могут быть использованы в теории кодирования (см., например, [158]), в теоретико-числовых вопросах разложения на простые множители (см., например, [159; 160]), для построения новых криптографических систем или для исследования стойкости криптосистем на эллиптических кривых и в якобианах гиперэллиптических кривых (см., например, [97; 101—103; 161; 162]).

Теория функциональных непрерывных дробей в гиперэллиптических полях строится для произвольного поля констант K, характеристики отличной от 2. Условие на характеристику важно, чтобы гиперэллиптические кривые могли быть заданы афинными уравнениями вида

$y^2 = f(x)$, где $f \in K[x]$ (см. §2.2).

Пусть $h \in K[x]$, $\deg h = 1$. В §3.1.1 введено понятие функциональной непрерывной дроби, построенной по нормированию первой степени v_h в поле формальных степенных рядов $K((h))$. В §3.1.2 понятие функциональной непрерывной дроби перенесено на гиперэллиптическое поле L, устанавлены алгебраические соотношения между полными и неполными частными непрерывных дробей. В §3.1.4 найдены формулы, позволяющие рекуррентно восстанавливать полные и неполные частные непрерывных дробей, производя только алгебраические операции с многочленами. В §3.1.5 дано определение приведенных элементов относительно рассматриваемого нормирования и доказывается ряд свойств приведенных элементов. Эти свойства в §3.1.6 позволяют определить длину предпериода квазипериодической непрерывной дроби. В §3.1.7 найдены достаточные условия на вид квадратичной иррациональности α, позволяющие утверждать, что непрерывная дробь α является не только квазипериодической, но и периодической. В статье [130] доказано, что в случае $\deg h = 1$ с точностью до умножения на константу наилучшие приближения и только они являются подходящими дробями. В §3.1.8 сформулированы общие свойства наилучших приближений и доказана теорема о достаточных условиях наилучшего приближения, являющегося решением норменного уравнения. Эта теорема позволяет сформулировать эквивалентные условия наличия решения норменного уравнения, связанного с данным элементом α гиперэллиптического поля L и наличия нетривиальных S-единиц поля L, а также сделать вывод о квазипериодичности непрерывной дроби элемента α.

Кроме непрерывных дробей, построенных в полях степенных рядов в $K((1/X))$ или $K((h))$ (соответственно по бесконечному нормированию или по конечному линейному нормированию), в главе 5 рассмотрены “экзотические” варианты непрерывных дробей. Так в разделе 5.3 рассматривается теория функциональных непрерывных дробей, построенных по двум несопряженным нормированиям первой степени (дополнительно см. [7]). В разделе 5.4 рассматривается теория функциональных непрерывных дробей, построенных по конечному нормированию второй степени (дополнительно см. [11] и [16]).

Результаты этого раздела опубликованы в статьях [19; 20; 157].

3.1.1. Разложение в непрерывную дробь

В этом параграфе используются обозначения, введенные в §2.3.2. Основная цель — ввести понятие функциональной непрерывной дроби и доказать простейшие свойства.

Пусть K — произвольное поле, $\operatorname{Char} K \neq 2$ и $h \in K[x]$. Элемент $\alpha \in \overline{K(x)}_h$ имеет разложение в формальный степенной ряд вида (2.3.2.1), с коэффициентами в $\Sigma = \{R \in K[x] : \deg R < \deg h\}$. Тем самым можно считать, что $\overline{K(x)}_h = \Sigma((h))$ — множество формальных

степенных рядов вида (2.3.2.1) (в случае $\deg h = 1$ имеем $\Sigma = K$ и $\overline{K(x)}_h = K((h)))$. Значит

$$\alpha = \sum_{j=-r}^{\infty} \sigma_j h^j, \quad \sigma_j \in \Sigma,$$

причем мы допускаем, что начиная с некоторого момента все σ_j могут быть равны 0. Введем обозначение

$$[\alpha]_h = \begin{cases} \sum\limits_{j=-r}^{0} \sigma_j h^j, & \text{если } r \geq 0, \\ 0, & \text{если } r < 0. \end{cases}$$

Положим $\alpha_0 = \alpha$, $a_0 = [\alpha_0]_h$. Если $\alpha_0 - a_0 \neq 0$, то положим

$$\alpha_1 = \frac{1}{\alpha - a_0} \in \overline{K(x)}_h, \quad a_1 = [\alpha_1]_h .$$

Далее по индукции определяем *неполные частные* a_j и *полные частные* α_j: если $\alpha_{j-1} - a_{j-1} \neq 0$, то

$$\alpha_j = \frac{1}{\alpha_{j-1} - a_{j-1}} \in \overline{K(x)}, \quad a_j = [\alpha_j]_h .$$

В результате получаем *непрерывную дробь*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}. \tag{3.1.1.1}$$

Непрерывная дробь называется *конечной*, если найдется номер n, для которого $\alpha_n = [\alpha_n]_h$, и в этом случае построение непрерывной дроби завершается. В противном случае непрерывная дробь называется *бесконечной*.

При $K = \mathbb{F}_q$ следующее предложение доказано в [130].

Предложение 3.1.1.1. *Непрерывная дробь вида* (3.1.1.1) *элемента* $\alpha \in \overline{K(x)}_h$ *конечна тогда и только тогда, когда* $\alpha \in K(x)$.

Доказательство. Если непрерывная дробь конечна, то, очевидно, $\alpha \in K(x)$.

Пусть $\alpha \in K(x)$, тогда можно записать $\alpha = \mu/\omega$, $\mu, \omega \in \Sigma[h]$, $\gcd(\mu, \omega) \in K^*$. Можем считать, что $v_h(\mu) = 0$, так как в противном случае $a_0 = [\alpha] = 0$, и вместо α будем рассматривать $\frac{1}{\alpha}$. Более того, можем считать, что $v_h(\omega) > 0$, так как в противном случае вместо α будем рассматривать $\frac{1}{\alpha - a_0}$, где $a_0 = [\alpha]_h$.

Положим $M_0 = \max(\deg \mu, \deg \omega)$. По построению $a_0 = \xi/h^\nu \in \Sigma[h^{-1}]$, где $\nu = v_h(\omega) > 0$, $\xi \in \Sigma[h]$, $\nu \deg h \leq \deg \xi \leq (\nu+1)\deg h - 1$, причем справедливо соотношение

$$\xi \frac{\omega}{h^\nu} \equiv \mu \pmod{h^{\nu+1}}.$$

Опять по построению непрерывной дроби

$$\alpha_1 = \frac{\mu_1}{\omega_1}, \quad \text{где } \mu_1 = \omega h^{-\nu},\ \omega_1 = (\mu - \xi\omega h^{-\nu})h^{-\nu},$$

причем $\mu_1, \omega_1 \in \Sigma[h]$, $\gcd(\mu_1, \omega_1) \in K^*$, $v_h(\mu_1) = 0$, $v_h(\omega_1) > 0$. Имеем $\deg \mu_1 = \deg \omega - \nu \deg h$, $\deg \omega_1 \leq \max(\deg \mu, \deg \omega + \deg h - 1) - \nu \deg h$, причем строгое неравенство возможно только в случае $\deg \mu = \deg \omega + \deg h - 1$. Положим $M_1 = \max(\deg \mu_1, \deg \omega_1)$, тогда $M_1 \leq M_0 - (\nu - 1)\deg h - 1 < M_0$. Следовательно, количество шагов построения непрерывной дроби конечно. □

Будем использовать стандартную сокращенную запись $[a_0; a_1, a_2, \ldots]$ для непрерывной дроби (3.1.1.1). По построению, $\alpha_j = [a_j; a_{j+1}, \ldots]$. Для конечной непрерывной дроби будем писать $[a_0; a_1, a_2, \ldots, a_n]$.

Продолжая обозначения, введенные в доказательстве предложения 3.1.1.1, для $\alpha = \mu/\omega$, $v_h(\mu) = 0$, положим $\alpha_j = \mu_j/\omega_j$, $\nu_j = v_h(\omega_j) = -v_h(\alpha_j) = -v_h(a_j)$ для $j \in \mathbb{N}$. Тогда $\max(\deg \mu, \deg \omega) \leq \sum_{j=0}^{n} \big((\nu_j - 1)\deg h + 1\big)$, а в случае $\deg h = 1$, получаем $\max(\deg \mu, \deg \omega) \leq \sum_{j=0}^{n} \nu_j$. Следовательно, можно утверждать , что в случае $\deg h = 1$ число шагов n построения непрерывной дроби рациональной функции $\alpha = \mu/\omega$ не превосходит $\max(\deg \mu, \deg \omega)$.

Определим по индукции *континуанты* $p_j, q_j \in K(x)$. Положим $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$ и

$$p_j = a_j p_{j-1} + p_{j-2}, \quad q_j = a_j q_{j-1} + q_{j-2}, \quad j \geq 0. \tag{3.1.1.2}$$

Тогда $p_j/q_j = [a_0; a_1, a_2, \ldots, a_j]$ при $j \geq 0$.

Предложение 3.1.1.2. *Для $j \geq -1$ справедливы соотношения*

$$q_j p_{j-1} - p_j q_{j-1} = (-1)^j, \tag{3.1.1.3}$$

$$q_j \alpha - p_j = \frac{(-1)^j}{q_j \alpha_{j+1} + q_{j-1}}, \tag{3.1.1.4}$$

$$\alpha = \frac{p_j \alpha_{j+1} + p_{j-1}}{q_j \alpha_{j+1} + q_{j-1}}. \tag{3.1.1.5}$$

Доказательство. См., например, [115]. □

Далее предполагаем, что $h \in K[x]$ — неприводимый над полем K многочлен.

Дробь p_j/q_j назовем j-й *подходящей дробью* к α, а величины $p_j = p_j(a_0, a_1, \ldots, a_j)$ и $q_j = q_j(a_1, \ldots, a_j)$ — *континуантами*. По построению, $v_h(a_j) = v_h(\alpha_j) < 0$ для $j \geq 1$. Из (3.1.1.2) по индукции легко получить соотношения

$$v_h(q_j) = v_h(a_j) + v_h(q_{j-1}) = \sum_{i=1}^{j} v_h(a_i), \tag{3.1.1.6}$$

$$v_h(p_j) = v_h(a_j) + v_h(p_{j-1}) = \sum_{i=0}^{j} v_h(a_i). \tag{3.1.1.7}$$

Из (3.1.1.4) получаем

$$v_h(q_j \alpha - p_j) = -v_h(q_{j+1}) = -v_h(a_{j+1}) - v_h(q_j) > -v_h(q_j), \tag{3.1.1.8}$$

или, что эквивалентно,

$$v_h\left(\alpha - \frac{p_j}{q_j}\right) = -v_h\left(q_{j+1}\right) - v_h\left(q_j\right) > -2v_h\left(q_j\right). \tag{3.1.1.9}$$

Предложение 3.1.1.3. *Для $\alpha \in \overline{K(x)}_h \setminus K(x)$ имеем $\lim\limits_{j\to\infty} p_j/q_j = \alpha$, т. е. подходящие дроби сходятся к α (имеется ввиду сходимость по нормированию v_h).*

Доказательство. Из (3.1.1.9) имеем $\lim_{j\to\infty} v_h\left(\alpha - p_j/q_j\right) = +\infty$, откуда следует утверждение предложения. □

Предложение 3.1.1.4. *При $j \geq 0$ справедливы соотношения*

$$\frac{p_j}{q_j} = [a_0; a_1, \ldots, a_j], \tag{3.1.1.10}$$

$$\alpha = [a_0; a_1, \ldots, a_j, \alpha_{j+1}], \tag{3.1.1.11}$$

$$\alpha_j = [a_j; a_{j+1}, \ldots], \tag{3.1.1.12}$$

$$\frac{q_j}{q_{j-1}} = [a_j; a_{j-1}, \ldots, a_1], \tag{3.1.1.13}$$

$$\frac{p_j}{p_{j-1}} = [a_j; a_{j-1}, \ldots, a_0]. \tag{3.1.1.14}$$

Доказательство. Соотношения (3.1.1.10)-(3.1.1.14) могут быть проверены по индукции. Покажем шаг индукции, например, для (3.1.1.13):

$$\frac{q_j}{q_{j-1}} = \frac{a_j q_{j-1} + q_{j-2}}{q_{j-1}} = a_j + \frac{1}{q_{j-1}/q_{j-2}}.$$

□

Стандартным образом, как и в случае поля вещественных чисел, можно показать, что если непрерывная дробь $[a_0, a_1, \ldots]$ для некоторого $\alpha \in \overline{K(x)}_h$ является периодической, то α — квадратичная иррациональность. В случае, когда поле K бесконечно, обратное утверждение верно не всегда (см. пример в [61] для нормирования v_∞). Однако, в случае конечного поля $K = \mathbb{F}_q$ и $\deg h = 1$ справедливо утверждение: если $\alpha \in \overline{\mathbb{F}_q(x)}_h = \mathbb{F}_q((h))$ — квадратичная иррациональность, то непрерывная дробь для α периодична (см. [130]).

Свойства периодичности и квазипериодичности непрерывных дробей будут детально рассматриваться в следующих параграфах.

3.1.2. Свойства полных частных непрерывной дроби

В этом параграфе мы продолжаем изучать свойства непрерывных дробей и связанных с ними объектов. В частности, мы докажем справедливость представления (3.1.2.4), где A_j, B_j определены в (3.1.2.2). Для дальнейших приложений важно показать, что величины A_j, B_j являются многочленами ограниченной степени.

Пусть $f(x) \in K[x]$, свободный от квадратов многочлен, $2g+1 \leq \deg f \leq 2g+2$, $g \in \mathbb{N}$. Пусть $h \in K[x]$, нормирование v_h поля $K(x)$ имеет два продолжения v_h^- и v_h^+ на поле $L = K(x)(\sqrt{f})$. Как было указано в §2.3.2, два продолжения нормирования соответствуют двум вложениям поля L в поле формальных степенных рядов $\overline{K(x)}_h$. Вложение поля L в поле $\overline{K(x)}_h$ позволяет рассматривать разложение элементов $\alpha \in L$ в непрерывную дробь, причем так как вложений два, то формально и разложений тоже два.

Скажем, что непрерывная дробь $[a_0; a_1, a_2, \ldots]$ элемента $\alpha \in L \subset \overline{K(x)}_h$ соответствует нормированию v_h^-, если $a_j = [\alpha_j]_h$ так, что $v_h(a_j) \leq 0$, если $v_h^-(\alpha_j) \leq 0$, $a_j = 0$, если $v_h^-(\alpha_j) > 0$, и $v_h^-(\alpha_j - a_j) > 0$ для всех $j \in \mathbb{N}$. Положим $S_h = \{v_h^-,\ v_h^+\}$, а в случае $\deg f = 2g+1$ еще дополнительно $S_\circ = \{v_\infty,\ v_h^-\}$.

Пусть α является корнем многочлена

$$H(Z) = \lambda_2 Z^2 + 2\lambda_1 Z + \lambda_0, \qquad \text{где} \quad \lambda_0, \lambda_1, \lambda_2 \in K[x], \quad \gcd(\lambda_0,\ \lambda_1,\ \lambda_2) \in K^*. \tag{3.1.2.1}$$

Положим $\overline{\alpha}$ — *сопряженный* к α элемент (т. е. второй корень квадратного трехчлена (3.1.2.1)), $d = \lambda_1^2 - \lambda_2\lambda_0$ — сокращенный дискриминант многочлена (3.1.2.1). Будем предполагать, что d/f является полным квадратом в кольце $K[x]$, т. е. $\alpha \in L$. Положим $v_h(\lambda_i) = l_i$, $i = 1, 2, 3$, причем в случае $\lambda_1 = 0$ считаем $l_1 = +\infty$.

Лемма 3.1.2.1. *Пусть* $\alpha = (-\lambda_1 + \sqrt{d})/\lambda_2$ *и* $v_h^-(\alpha) \geq v_h^-(\overline{\alpha})$. *Тогда возможен один из следующих случаев*

- *при* $2l_1 \leq l_0 + l_2$ *имеем* $v_h^-(\alpha) = l_0 - l_1$ *и* $v_h^-(\overline{\alpha}) = l_1 - l_2$;
- *при* $2l_1 > l_0 + l_2$ *имеем* $v_h^-(\alpha) = v_h^-(\overline{\alpha}) = (l_0 - l_2)/2$, *причем* $l_0 = 0$ *или* $l_2 = 0$.

Доказательство. Рассмотрим несколько случаев.

1. Пусть $2l_1 \leq l_0 + l_2$, тогда

$$l_1 = v_h^-\left(-\lambda_1 - \sqrt{d}\right) \leq v_h^-\left(-\lambda_1 + \sqrt{d}\right),$$

поскольку в противном случае, если $v_h^-\left(-\lambda_1 - \sqrt{d}\right) > l_1$ и $v_h^-\left(-\lambda_1 + \sqrt{d}\right) > l_1$, то $v_h(\lambda_1) > l_1$, что противоречит нашим обозначениям. Имеем

$$l_1 + v_h^-\left(-\lambda_1 + \sqrt{d}\right) = v_h^-\left(-\lambda_1 - \sqrt{d}\right) + v_h^-\left(-\lambda_1 + \sqrt{d}\right) = v_h(\lambda_0\lambda_2) = l_0 + l_2.$$

Следовательно, $v_h^-(\alpha) = l_0 - l_1$ и $v_h^-(\overline{\alpha}) = l_1 - l_2$.

2. Пусть $2l_1 > l_0 + l_2$, тогда в силу (3.1.2.1) либо $l_0 = 0$ и l_2 четно, либо $l_2 = 0$ и l_0 четно.

Предположим, что $l_0 = 0$, $l_2 = 2t$, тогда

$$t = v_h^-\left(-\lambda_1 - \sqrt{d}\right) \leq v_h^-\left(-\lambda_1 + \sqrt{d}\right),$$

поскольку в противном случае, если $v_h^-\left(-\lambda_1 - \sqrt{d}\right) > t$ и $v_h^-\left(-\lambda_1 + \sqrt{d}\right) > t$, то $t = v_h\left(\sqrt{d}\right) >$

t, что невозможно. Имеем

$$t + v_h^-\left(-\lambda_1 + \sqrt{d}\right) = v_h^-\left(-\lambda_1 - \sqrt{d}\right) + v_h^-\left(-\lambda_1 + \sqrt{d}\right) = v_h\left(\lambda_0\lambda_2\right) = 2t.$$

Следовательно, $v_h^-(\alpha) = v_h^-(\overline{\alpha}) = -t$.

Предположим, что $l_2 = 0$, $l_0 = 2t$, тогда

$$t = v_h^-\left(-\lambda_1 - \sqrt{d}\right) \le v_h^-\left(-\lambda_1 + \sqrt{d}\right),$$

поскольку в противном случае, если $v_h^-\left(-\lambda_1 - \sqrt{d}\right) > t$ и $v_h^-\left(-\lambda_1 + \sqrt{d}\right) > t$, то $t = v_h\left(\sqrt{d}\right) > t$, что невозможно. Имеем

$$t + v_h^-\left(-\lambda_1 + \sqrt{d}\right) = v_h^-\left(-\lambda_1 - \sqrt{d}\right) + v_h^-\left(-\lambda_1 + \sqrt{d}\right) = v_h\left(\lambda_0\lambda_2\right) = 2t.$$

Следовательно, $v_h^-(\alpha) = v_h^-(\overline{\alpha}) = t$. □

Пусть $[a_0; a_1, \ldots]$ — разложение α в непрерывную дробь, соответствующее нормированию v_h^-. Пусть $H(X,Y) = \lambda_2 X^2 + 2\lambda_1 XY + \lambda_0 Y^2$. При $j \ge -1$ обозначим

$$A_j = (-1)^{j+1} H(p_j, q_j), \qquad B_j = (-1)^j(\lambda_2 p_{j-1}p_j + 2\lambda_1 p_{j-1}q_j + \lambda_0 q_{j-1}q_j). \tag{3.1.2.2}$$

Выпишем явно A_j и $B_j - \lambda_1$ при $j = -1$ и $j = 0$:

$$A_{-1} = \lambda_2, \quad B_{-1} - \lambda_1 = -\lambda_1, \quad A_0 = -(\lambda_2 a_0^2 + 2\lambda_1 a_0 + \lambda_0), \quad B_0 - \lambda_1 = \lambda_2 a_0 + \lambda_1. \tag{3.1.2.3}$$

Предложение 3.1.2.2. *При $j \ge -1$ справедливо тождество*

$$\alpha_{j+1} = \frac{B_j + \lambda_2\alpha}{A_j}, \tag{3.1.2.4}$$

Доказательство. По определению мы имеем $\alpha_0 = \alpha$. Далее, из (3.1.1.5) получаем

$$\alpha_{j+1} = -\frac{p_{j-1} - \alpha q_{j-1}}{p_j - \alpha q_j} = -\frac{(p_{j-1} - \alpha q_{j-1})(p_j - \overline{\alpha} q_j)}{(p_j - \alpha q_j)(p_j - \overline{\alpha} q_j)},$$

тогда с обозначениями (3.1.2.2) имеем

$$\alpha_{j+1} = \frac{(-1)^j\lambda_2\big(p_j p_{j-1} - (\alpha + \overline{\alpha})q_j p_{j-1} + \alpha\overline{\alpha} q_j q_{j-1} + \alpha(q_j p_{j-1} - p_j q_{j-1})\big)}{A_j},$$

откуда, учитывая (3.1.1.3), получаем (3.1.2.4). □

В статье [130] для $K = \mathbb{F}_q$ в случае $\deg h = 1$ доказано, что начиная с некоторого номера j величины A_j и B_j являются многочленами. Нам требуется более общее утверждение.

Предложение 3.1.2.3. *При $j \ge -1$ величины A_j и B_j являются многочленами, т. е. $A_j, B_j \in K[x]$.*

Доказательство. Без ограничения общности мы можем предполагать, что

$$\alpha = \frac{-\lambda_1 + \sqrt{d}}{\lambda_2}, \quad d = \lambda_1^2 - \lambda_0\lambda_2, \quad \lambda_0, \lambda_1, \lambda_2 \in K[x]. \tag{3.1.2.5}$$

При $j=-1$ имеем $A_{-1}=\lambda_2$, $B_{-1}=0$, поэтому утверждение очевидно. При $j=0$, учитывая (3.1.2.3), имеем

$$v_h(A_0)=v_h\left(\frac{d-(\lambda_1+a_0\lambda_2)^2}{\lambda_2}\right)=v_h\left(\lambda_2(a_0-\overline{\alpha})(\alpha-a_0)\right)=$$
$$=v_h^-\left(a_0\lambda_2+\lambda_1+\sqrt{d}\right)+v_h(\alpha-a_0).$$

Имеем по построению $v_h^-(\alpha-a_0)>0$, а также $v_h^-\left(a_0\lambda_2+\lambda_1+\sqrt{d}\right)\geq 0$, поскольку нормирование каждого слагаемого неотрицательное. Из равенства $\alpha(\lambda_2\alpha+2\lambda_1)=-\lambda_0$ следует, что $v_h^-(\lambda_2\alpha)\geq 0$, поэтому $v_h(a_0)+v_h(\lambda_2)\geq 0$, значит $v_h(B_0)\geq 0$.

Пусть теперь $j\geq 1$. По построению (3.1.1.2) и (3.1.2.2) $A_j,B_j\in K(x)$ — рациональные функции, причем их знаменатели могут иметь только вид ch^n для некоторых $n\in\mathbb{Z}$, $c\in K^*$. Для того, чтобы $A_j,B_j\in K[x]$, достаточно доказать, что $v_h(A_j)\geq 0$, $v_h(B_j)\geq 0$.

Положим

$$H(X,Y)=\lambda_2X^2+2\lambda_1XY+\lambda_0Y^2, \tag{3.1.2.6}$$

тогда

$$H(X,Y)=Y^2\cdot H(X/Y)=\lambda_2(X-\alpha Y)(X-\overline{\alpha}Y).$$

Учитывая (3.1.1.8), находим

$$v_h(A_j)=v_h^-\left(\lambda_2(p_j-\alpha q_j)(p_j-\overline{\alpha}q_j)\right)=v_h(\lambda_2)-v_h(a_{j+1})+v_h^-\left(\frac{p_j}{q_j}-\overline{\alpha}\right). \tag{3.1.2.7}$$

Если $v_h^-\left(\sqrt{d}/\lambda_2\right)\leq 0$, то

$$v_h^-\left(\frac{p_j}{q_j}-\alpha\right)>0\geq v_h^-(\alpha-\overline{\alpha})=v_h^-\left(\frac{2\sqrt{d}}{\lambda_2}\right)=\frac{1}{2}v_h(d)-v_h(\lambda_2).$$

Тогда

$$v_h^-\left(\frac{p_j}{q_j}-\overline{\alpha}\right)=v_h^-\left(\frac{p_j}{q_j}-\alpha+\alpha-\overline{\alpha}\right)=v_h^-(\alpha-\overline{\alpha}).$$

Таким образом, из (3.1.2.7) имеем $v_h(A_j)=\frac{1}{2}v_h(d)-v_h(a_{j+1})>0$.

Если $v_h^-\left(\sqrt{d}/\lambda_2\right)>0$, то, учитывая, что по построению

$$0<v_h^-\left(\frac{p_j}{q_j}-\alpha\right)=v_h^-\left(\frac{p_j}{q_j}+\frac{\lambda_1}{\lambda_2}-\frac{\sqrt{d}}{\lambda_2}\right),$$

имеем $v_h^-\left(\frac{p_j}{q_j}+\frac{\lambda_1}{\lambda_2}\right)>0$. Тогда

$$v_h^-\left(\frac{p_j}{q_j}-\overline{\alpha}\right)\geq\min\left(v_h\left(\frac{p_j}{q_j}+\frac{\lambda_1}{\lambda_2}\right),\ v_h^-\left(\frac{\sqrt{d}}{\lambda_2}\right)\right)>0.$$

Снова, из (3.1.2.7) имеем $v_h(A_j)>v_h^-(\lambda_2)-v_h(a_{j+1})>0$.

Найдем нижнюю оценку для $v_h(B_j)$. Из (3.1.2.4) получаем $B_j=A_j\alpha_{j+1}-\lambda_2\alpha$. Мы уже

видели, что $v_h(\lambda_2\alpha) \geq 0$. Из оценок нормирования $v_h^-(A_j)$ имеем $v_h^-(A_j\alpha_{j+1}) = v_h(A_j a_{j+1}) \geq 0$. Значит, $v_h(B_j) \geq \min\{v_h^-(A_j\alpha_{j+1}),\ v_h^-(\lambda_2\alpha)\} \geq 0$. □

Предложение 3.1.2.4. *1. При $j \geq -1$ справедливо соотношение*

$$v_h(A_j) \geq \min\left\{\frac{1}{2}v_h(d) - v_h(a_{j+1}),\ v_h(\lambda_2) - 2\sum_{i=1}^{j+1} v_h(a_i)\right\}, \tag{3.1.2.8}$$

причем, если минимум достигается на одной из величин, то в (3.1.2.8) выполнено равенство.

2. При $j \geq 0$ справедливы следующие утверждения:

- *если $v_h(A_{j-1}) = v_h(d)/2 - v_h(a_j)$, то $v_h(A_j) = v_h(d)/2 - v_h(a_{j+1})$;*
- *если $v_h(A_j) = v_h(\lambda_2) - 2\sum_{i=1}^{j+1} v_h(a_i)$, то $v_h(A_{j-1}) = v_h(\lambda_2) - 2\sum_{i=1}^{j} v_h(a_i)$.*

Доказательство. В доказательстве предложения 3.1.2.3 была полечена формула (3.1.2.7). Используя (3.1.1.4), оценим

$$v_h^-(p_j - q_j\overline{\alpha}) = v_h^-(q_j(\alpha - \overline{\alpha}) + (p_j - q_j\alpha)) \geq \min\left\{v_h(q_j) + v_h^-\left(\frac{\sqrt{d}}{\lambda_2}\right),\ -v_h(q_{j+1})\right\},$$

откуда и получается соотношение (3.1.2.8), а также остальные утверждения предложения 3.1.2.4. □

Замечание 3.1.2.5. *Если выполнены условия*

$$0 = v_h(\lambda_0) < v_h(\lambda_2) < v_h(\lambda_1), \tag{3.1.2.9}$$

то $v_h^-\left(\sqrt{d}/\lambda_2\right) = -v_h(\lambda_2)/2 < 0$, поэтому в данном случае имеем

$$v_h(A_j) = \frac{1}{2}v_h(d) - v_h(a_{j+1}), \quad j \geq -1. \tag{3.1.2.10}$$

Предложение 3.1.2.6. *Пусть $\gamma = \deg h - 1$, тогда при $j \geq -1$ имеем*

$$\deg A_j \leq \max((2j+2)\gamma + \deg\lambda_2,\ (2j+1)\gamma + \deg\lambda_1,\ 2j\gamma + \deg\lambda_0),$$
$$\deg B_j \leq \max((2j+1)\gamma + \deg\lambda_2,\ 2j\gamma + \deg\lambda_1,\ (2j-1)\gamma + \deg\lambda_0).$$

В случае $\deg h = 1$ степени многочленов A_j, B_j не превосходят $\Lambda = \max(\deg\lambda_0,\ \deg\lambda_1,\ \deg\lambda_2)$.

Доказательство. Заметим, что по построению $v_\infty(a_j) \geq -\gamma$, следовательно, из (3.1.1.2) имеем

$$v_\infty(p_j) \geq -(j+1)\gamma, \quad v_\infty(q_j) \geq -j\gamma.$$

Теперь требуемые неравенства получаются из (3.1.2.2). □

Замечание 3.1.2.7. *В частности, в случае* $\deg h = 1$, *который будет далее в этой главе предметом основного внимания, из предложения 3.1.2.6 получаем*

$$\deg A_j, \deg B_j \leq \max\left(\deg \lambda_0,\ \deg \lambda_1,\ \deg \lambda_2\right).$$

С учетом представления (3.1.2.4) получаем

$$-v_h\left(a_j\right) \leq v_h\left(A_j\right) \leq \max\left(\deg \lambda_0,\ \deg \lambda_1,\ \deg \lambda_2\right).$$

3.1.3. Связь непрерывных дробей, построенных по нормированиям первой степени

Пусть K — произвольное поле характеристики отличной от 2, а h и X — трансцендентные элементы. В этом параграфе мы рассмотрим связь непрерывных дробей, построенных в полях формальных степенных рядов $K((h))$ и $K((1/X))$ (см. [8]). В дальнейшем будем использовать аргументы h, X для многочленов $f(h)$, $F(X)$, чтобы при необходимости использовать эту связь.

Напомним, что в поле рациональных функций $K(h)$ конечное нормирование v_h для элемента $\alpha \in K(h)$ определяется следующим образом: $v_h(\alpha) = m \in \mathbb{Z}$, где $\alpha = h^m \cdot p/q$, $p, q \in K[x]$, $h \nmid p$, $h \nmid q$. Бесконечное нормирование v_∞ элемента $\beta \in K(X)$ определяется как $v_\infty(\beta) = \deg\omega - \deg\tau$, где $\beta = \tau/\omega$, $\tau, \omega \in K[X]$. Нормирования v_h и v_∞ естественным образом продолжаются соответственно на поля формальных степенных рядов $K((h))$ и $K((1/X))$, где

$$K((x)) = \left\{ \sum_{j=s}^{\infty} c_j h^j \;\middle|\; c_j \in K,\ s \in \mathbb{Z},\ c_s \in K^* \right\},$$

$$K((1/X)) = \left\{ \sum_{j=s}^{\infty} c_j \left(\frac{1}{X}\right)^j \;\middle|\; c_j \in K,\ s \in \mathbb{Z},\ c_s \in K^* \right\}.$$

Тогда для элементов

$$\alpha = \sum_{j=s}^{\infty} c_j x^j \in K((h)), \qquad \beta = \sum_{j=s}^{\infty} c_j \left(\frac{1}{X}\right)^j \in K((1/X))$$

имеем $v_h(\alpha) = v_\infty(\beta) = s$. Определим

$$[\alpha]_h = \begin{cases} \sum_{j=s}^{0} c_j x^j, & s \leq 0, \\ 0, & s > 0, \end{cases} \qquad [\beta]_\infty = \begin{cases} \sum_{j=s}^{0} c_j \left(\frac{1}{X}\right)^j, & s \leq 0, \\ 0, & s > 0. \end{cases}$$

Непрерывные дроби в полях $K((h))$ и $K((1/X))$ строятся стандартным рекуррентным обра-

зом:

$$\alpha_0 = \alpha, \quad a_j = [\alpha_j]_h, \quad \alpha_{j+1} = \frac{1}{\alpha_j - a_j}, \quad j \in \mathbb{N}_0,$$
$$\beta_0 = \beta, \quad b_j = [\beta_j]_\infty, \quad \beta_{j+1} = \frac{1}{\beta_j - b_j}, \quad j \in \mathbb{N}_0,$$

причем рекуррентный процесс по $j \in \mathbb{N}_0$ продолжается пока $\alpha_j \neq a_j$ и $\beta_j \neq b_j$ соответственно. Для самих конечных или бесконечных непрерывных дробей будем использовать стандартные обозначения

$$[a_0; a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}, \quad [b_0; b_1, b_2, \ldots] = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cdots}}.$$

Непрерывные дроби, построенные в поле $K((1/X))$, называют *классическими*, поскольку история их рассмотрения восходит к классическим работам Абеля и Чебышева. Отображение $\phi : h \to 1/X$ продолжается естественным образом $\phi : K((h)) \to K((1/X))$, причем $\phi(\alpha) = \beta$, $\phi([\alpha]_h) = [\beta]_\infty$. Поэтому $\phi(\alpha_j) = \beta_j$, $\phi(a_j) = b_j$ и для формальных непрерывных дробей справедливо соотношение

$$\phi\big([a_0; a_1, a_2, \ldots]\big) = [b_0; b_1, b_2, \ldots].$$

В текущей главе основное внимание уделяется функциональным непрерывным дробям, построенным по конечному (линейному) нормированию в поле формальных степенных рядов $K((h))$. Однако, указанная выша связь позволяет нам использовать и транслировать результаты полученные в классическом случае для непрерывных дробей в $K((1/X))$ (см., например, [8; 13; 17; 92; 130]).

Рассмотрим свободный от квадратов многочлен $f \in K[h]$ со свободным членом $f(0) = \gamma^2$, являющимся полным квадратом в K^*, тогда $\pm\sqrt{f} \in K((h))$ и поле $L = K(h)(\sqrt{f})$ вкладывается двумя неэквивалентными способами в поле формальных степенных рядов $K((h))$. Мы фиксируем одно из вложений, например, соответствующее $v_h\left(\sqrt{f(h)} - \gamma\right) > 0$, где под выражением $\sqrt{f(h)} - \gamma$ мы подразумеваем соответствующий образ в $K((h))$. Тогда нормирование поля L, индуцированное из нормирования v_x поля $K((h))$ и зафиксированного вложения, обозначим v_h^-.

Аналогичным образом для свободного от квадратов многочлена $F \in K[X]$ четной степени со старшим коэффициентом, являющимся полным квадратом в K^*, поле $\mathcal{L} = K(X)(\sqrt{F})$ можно двумя способами вложить в поле формальных степенных рядов $K((1/X))$. Если положить $g = [(\deg f - 1)/2]$ и $F(X) = X^{2g+2} f(1/X) \in K[X]$, то мы фиксируем то вложение, для которого $v_\infty\left(\phi(\sqrt{f(h)} - \gamma)\right) > 0$. Индуцированное нормирование поля $\mathcal{L}$ из нормирования v_∞ поля $K((1/X))$ и зафиксированного вложения обозначим v_∞^-. Тогда $\phi(\sqrt{f}/h^{g+1}) = \sqrt{F}$, и непрерывные дроби элементов полей L и $\mathcal{L}$, построенные соответственно в полях $K((h))$ и $K((1/X))$, переводятся друг в друга с помощью отображений ϕ и ϕ^{-1}. Так, например, для

непрерывной дроби элемента $\sqrt{f}/h^{g+1} = [a_0; a_1, a_2, \ldots]$, построенной в поле $K((h))$, справедливо равенство

$$\phi\big([a_0; a_1, a_2, \ldots]\big) = \big[\phi(a_0); \phi(a_1), \phi(a_2), \ldots\big] = \sqrt{F},$$

где $\big[\phi(a_0); \phi(a_1), \phi(a_2), \ldots\big]$ — непрерывная дробь элемента $\sqrt{F}$, построенная в поле $K((1/X))$.

Сохраняя обозначения, введенные выше, рассмотрим элемент $\alpha \in L = K(h)(\sqrt{f})$, являющийся корнем квадратного уравнения (3.1.2.1) с сокращенным дискриминантом d для некоторых $\lambda_0, \lambda_1, \lambda_2 \in K[h]$. Положим $r = \max\big(\deg \lambda_0, \deg \lambda_1, \deg \lambda_2\big)$, $\Lambda_i(X) = X^r \lambda_i(1/X)$, $i = 0, 1, 2$, $D = \Lambda_1^2 - \Lambda_0\Lambda_2$, тогда $\Lambda_i, D \in K[X]$ и $\deg_X \Lambda_i = r - v_h(\lambda_i)$, $\deg_X D = 2r - v_h(d) = 2r - 2s_0$, $(\Lambda_0, \Lambda_1, \Lambda_2) \in K^*$, где $v_h(d) = 2s_0$ четно, поскольку нормирование v_h поля $K(h)$ имеет два продолжения на поле L.

Элемент $\beta = \phi(\alpha) \in \mathcal{L}$ является корнем квадратного уравнения

$$\Lambda_2 Z^2 + 2\Lambda_1 Z + \Lambda_1 = 0 \tag{3.1.3.1}$$

с сокращенным дискриминантом D. Разложения элементов α и β в непрерывные дроби соответственно в полях $K((h))$ и $K((1/X))$ переводятся друг в друга с помощью ϕ и ϕ^{-1}. В частности, у этих разложений будут одинаковые такие характеристики как длина предпериода, длина квазипериода и длина периода.

Предложение 3.1.3.1. *Пусть элемент $\beta \in \mathcal{L}$ является корнем квадратного уравнения (3.1.3.1) с коэффициентами $\Lambda_0, \Lambda_1, \Lambda_2 \in K$ такими, что*

$$(\Lambda_0, \Lambda_1, \Lambda_2) \in K^*, \quad r = \max\big(\deg \Lambda_0, \deg \Lambda_1, \deg \Lambda_2\big).$$

Пусть непрерывная дробь β, построенная в поле $K((1/X))$, имеет вид $[b_0; b_1, \ldots]$. Тогда $\deg b_j \le r$

Доказательство. Пусть $\beta = \phi(\alpha)$ и $\alpha = [a_0; a_1, \ldots]$ и $\beta = [b_0; b_1, \ldots]$. Тогда $a_j \in K[h^{-1}]$, $b_j \in K[X]$ и $b_j = \phi(a_j)$. Обозначим $\tilde{A}_j = X^r A_j(1/X)$, $\tilde{B}_j = X^r B_j(1/X)$, где величины A_j, B_j определены в (3.1.2.2). Тогда в силу предложения 3.1.2.3 и предложения 3.1.2.6 получаем, что $\tilde{A}_j, \tilde{B}_j \in K[X]$ и $\deg_X \tilde{A}_j, \deg_X \tilde{B}_j \le r$. Имеем

$$\beta_j = \frac{\tilde{B}_j + \Lambda_2\beta}{\tilde{A}_j},$$

откуда с учетом $\deg_X \tilde{A}_j = r - v_h(A_j)$ получаем $\deg_X b_j = v_h(A_j) \le \deg_h A_j \le r$. Предложение 3.1.3.1 доказано. □

3.1.4. Рекуррентные формулы

В этом параграфе и далее используются обозначения, введенные в §3.1.2. Нашей текущей задачей является доказательство рекуррентных формул и тождеств, связывающих величины a_j, p_j, q_j, A_j, B_j. С помощью полученных соотношений можно получить эффективный

алгоритм построения непрерывной дроби, использующий только сложение, умножения многочленов и на каждом шаге одно деление с остатком многочленов ограниченной степени (см. [62]).

Предложение 3.1.4.1. *При $j \geq 0$ справедливы тождества*

$$B_j + B_{j-1} - a_j A_{j-1} = 2\lambda_1, \tag{3.1.4.1}$$

$$(B_j - \lambda_1)^2 + A_j A_{j-1} = d. \tag{3.1.4.2}$$

Доказательство. По построению непрерывной дроби $[a_0, a_1, \ldots]$ для остатков α_j справедливо соотношение

$$\alpha_j = a_j + \frac{1}{\alpha_{j+1}}. \tag{3.1.4.3}$$

Подставим вместо α_j и α_{j+1} в (3.1.4.3) выражение (3.1.2.4) и приведем к общему знаменателю

$$A_j A_{j-1} = (B_j + \lambda_2\alpha)(B_{j-1} - a_j A_{j-1} + \lambda_2\alpha), \tag{3.1.4.4}$$

раскрывая скобки, имеем

$$A_j A_{j-1} = B_j B_{j-1} - a_j A_{j-1} B_j + \lambda_2\alpha(B_j + B_{j-1} - a_j A_{j-1}) + \lambda_2^2\alpha^2. \tag{3.1.4.5}$$

Подставим выражения для корней $H(X)$

$$\alpha,\ \overline{\alpha} = \frac{-\lambda_1 \pm \sqrt{d}}{\lambda_2}, \qquad d = \lambda_1^2 - \lambda_0\lambda_2, \tag{3.1.4.6}$$

в равенство (3.1.4.5) и приравняем коэффициенты при $\sqrt{d}$, тогда получим рекуррентное соотношение (3.1.4.1) для B_j. Подставим выражение (3.1.4.1) во вторую скобку (3.1.4.4) и воспользуемся тождеством $\lambda_2\alpha^2 + 2\lambda_1\alpha + \lambda_0 = 0$, тогда

$$B_j^2 - 2\lambda_1 B_j + A_j A_{j-1} + \lambda_0\lambda_2 = 0, \tag{3.1.4.7}$$

откуда следует (3.1.4.2). □

Напомним, что *инволюцией* $\iota : L \to L$ называется автоморфизм поля L, заданный следующим образом:

$$\iota(\omega_1 + \omega_2\sqrt{f}) = \omega_1 - \omega_2\sqrt{f}, \quad \omega_1,\ \omega_2 \in K(x).$$

Предложение 3.1.4.2. *При $j \geq 0$ элементы α_{j+1} и $\iota\alpha_{j+1} = \overline{\alpha_{j+1}}$ поля L являются корнями квадратного уравнения*

$$A_j X^2 - 2(B_j - \lambda_1)X - A_{j-1} = 0 \tag{3.1.4.8}$$

с дискриминантом (3.1.4.2). При $j \geq 0$ справедливо тождество

$$\alpha_{j+1} = -\frac{A_{j-1}}{B_j + \lambda_2\overline{\alpha}}. \tag{3.1.4.9}$$

Доказательство. В силу (3.1.2.4) и теоремы Виета для корней квадратного уравнения имеем соотношения

$$\alpha_{j+1} = \frac{B_j + \lambda_2\alpha}{A_j}, \qquad \overline{\alpha_{j+1}} = \frac{B_j + \lambda_2\overline{\alpha}}{A_j},$$
$$\alpha_{j+1} + \overline{\alpha_{j+1}} = \frac{2B_j - 2\lambda_1}{A_j}, \qquad \alpha_{j+1}\cdot\overline{\alpha_{j+1}} = \frac{B_j^2 - 2\lambda_1 B_j + \lambda_0\lambda_2}{A_j^2} = -\frac{A_{j-1}}{A_j}.$$

Отсюда снова по теореме Виета заключаем, что α_{j+1} и $\overline{\alpha_{j+1}}$ являются корнями уравнения (3.1.4.8). Из (3.1.4.7) и (3.1.4.2) имеем рекуррентные соотношения на A_j

$$A_j = \frac{2\lambda_1 B_j - B_j^2 - \lambda_0\lambda_2}{A_{j-1}} = \frac{d - (B_j - \lambda_1)^2}{A_{j-1}}. \tag{3.1.4.10}$$

Подставляя (3.1.4.10) в (3.1.2.4), получаем еще одно выражение для α_{j+1}

$$\alpha_{j+1} = \frac{A_{j-1}(B_j + \lambda_2\alpha)}{d - (B_j - \lambda_1)^2} = -\frac{A_{j-1}}{B_j + \lambda_2\overline{\alpha}}. \tag{3.1.4.11}$$

□

Для всех $j \geq 0$ положим $s_j = -v_h(a_j)$, $t_j = -v_h(q_j)$. По построению непрерывной дроби имеем $s_j \geq 1$, $t_j = \sum\limits_{i=1}^{j} s_i$, $v_h(p_j) = -t_j - s_0$. Предположим, что корни многочлена $H(X)$, определенного в (3.1.2.1), принадлежат полю $L = K(x)(\sqrt{f})$, тогда $\sqrt{d/f} \in K[x]$, причем $v_h(d)$ четно, поскольку $v_h(f) = 0$. Обозначим $t = \frac{1}{2}v_h(d) \geq 0$.

Предложение 3.1.4.3. *При $j \geq 0$ справедливы соотношения*

$$v_h(A_j) = t + s_{j+1} \geq 1, \qquad v_h(B_j - \lambda_1) = t. \tag{3.1.4.12}$$

Коэффициенты $B_{j,i} \in \Sigma$ разложения многочлена B_j по h удовлетворяют соотношениям

$$B_{j,i} - \frac{\lambda_{1,i}}{2} = \pm d_{i-t}, \quad i = 0, 1, \ldots, t + s_j + s_{j+1} - 1, \tag{3.1.4.13}$$

где $\lambda_{1,i} \in \Sigma$ — коэффициенты разложения многочлена λ_1 по h и

$$\sqrt{d} = \sum_{i=0}^{\infty} d_{i-t}h^i, \quad \textit{причем } d_i = 0, \ \textit{при } -t \leq i < 0.$$

Доказательство. Соотношения (3.1.4.12) при $j = 0$ проверяются непосредственно, а при $j \geq 1$ следуют из (3.1.2.10) и (3.1.4.2).

Из (3.1.4.11) получаем

$$B_j - \lambda_1 \mp \sqrt{d} = B_j + \lambda_2\overline{\alpha} = -\frac{A_{j-1}}{\alpha_{j+1}}, \tag{3.1.4.14}$$

где знак перед $\sqrt{d}$ выбирается в зависимости от выбора знака для α и $\overline{\alpha}$ в (3.1.4.6) (всюду верхний знак или всюду нижний). Сравнивая коэффициенты в (3.1.4.14) при первых степенях h вплоть до степени $t + s_j + s_{j+1} - 1$, получаем соотношения (3.1.4.13). Соотношения (3.1.4.13) также могут быть получены из формулы (3.1.4.2). □

Предложение 3.1.4.4. *Пусть* $h \in K[x]$, $\deg h = 1$, *и многочлен* $\omega \in K[x]$,

$$\omega = c_0 + c_1 h + \ldots + c_n h^n, \quad c_i \in K,\ c_0 \neq 0,\ c_n \neq 0,$$

имеет разложение в формальный степенной ряд

$$\sqrt{\omega} = \sum_{i=0}^{\infty} \omega_i h^i, \quad \omega_i \in K,$$

причем $\omega_{s_0+1} = \ldots = \omega_{s_0+\delta} = 0$ *и* $\omega_{s_0+\delta+1} \neq 0$ *для некоторых* $s_0, \delta \in \mathbb{N}$. *Тогда* $\delta < \max(s_0,\ n - s_0)$.

Доказательство. Положим $c_i = 0$ при $i > n$, тогда для коэффициентов c_i и ω_i справедливы соотношения

$$c_i = \sum_{r=0}^{i} \omega_r \omega_{i-r}.$$

Предположим, что $\delta \geq \max(s_0,\ n - s_0)$, то есть $\delta + s_0 + 1 > \max(2s_0,\ n)$. Коэффициент $c_{\delta+s_0+1}$ удовлетворяет соотношению:

$$0 = c_{\delta+s_0+1} = \sum_{r=0}^{\delta+s_0+1} \omega_r \omega_{i-r} = 2\omega_0 \omega_{\delta+s_0+1}.$$

Поскольку по условию $\omega_{\delta+s_0+1} \neq 0$ и $\omega_0 = \sqrt{c_0} \neq 0$, то мы пришли к противоречию. □

Следующий пример показывает, что верхняя оценка для δ в предложении 3.1.4.4 достигается.

Пример 3.1.4.5. *Рассмотрим многочлен* $\omega \in K[x]$ *следующего вида*

$$\omega = c^2 + bx^n, \quad c \neq 0,\ b \neq 0$$

и его разложение в $K((x))$*:*

$$\sqrt{\omega} = \sum_{i=0}^{\infty} \omega_i x^i, \quad \omega_i \in K.$$

Тогда $\omega_0 = c$, $\omega_r = 0$ *для любого* $r \in \mathbb{N}$, $r \not\equiv 0 \pmod{n}$ *и* $\omega_n = \frac{b}{2c}$. *При* $r = nl$, $l \geq 2$ *имеем рекуррентные соотношения*

$$\omega_{nl} = -\frac{1}{2c} \sum_{i=1}^{l-1} \omega_{ni} \omega_{n(l-i)} = -\frac{n_l \omega_n^l}{(2c)^{l-1}} = -\frac{n_l b^l}{(2c)^{2l-1}}, \quad n_l \in \mathbb{N},$$

которые легко установить по индукции. Таким образом, если $s_0 = 0$ *или* $s_0 = n$, *то* $\delta = n - 1 = \max(s_0,\ n - s_0) - 1$.

Предложение 3.1.4.6. *Последовательность многочленов* A_j *удовлетворяет рекуррентному соотношению*

$$A_j = A_{j-2} + a_j(B_{j-1} - B_j). \tag{3.1.4.15}$$

Доказательство. Запишем (3.1.4.2) для двух последовательных номеров $j-1$ и j, а затем вычтем их:

$$0 = (B_j - \lambda_1)^2 - (B_{j-1} - \lambda_1)^2 + A_j A_{j-1} - A_{j-1}A_{j-2},$$

$$(B_j + B_{j-1} - 2\lambda_1)(B_j - B_{j-1}) = A_{j-1}(A_{j-2} - A_j),$$

и, подставив в первую скобку выражение (3.1.4.1), получим (3.1.4.15). □

Предложение 3.1.4.7. *Неполные частные a_j непрерывной дроби $[a_0, a_1, a_2, \ldots]$ квадратичной иррациональности α удовлетворяют квадратному уравнению*

$$A_{j-1}X^2 - 2(B_{j-1} - \lambda_1)X + A_j - A_{j-2} = 0, \tag{3.1.4.16}$$

причем корни этого уравнения имеют вид

$$a_j = \frac{B_{j-1} + B_j - 2\lambda_1}{A_{j-1}}, \qquad a'_j = \frac{B_{j-1} - B_j}{A_{j-1}}. \tag{3.1.4.17}$$

Доказательство. Подставим выражение (3.1.4.1) в (3.1.4.15), тогда получим аналог соотношения (3.1.4.8), а именно,

$$A_{j-1}a_j^2 - 2(B_{j-1} - \lambda_1)a_j + A_j - A_{j-2} = 0$$

с сокращенным дискриминантом

$$(B_{j-1} - \lambda_1)^2 - A_{j-1}(A_j - A_{j-2}) = d - A_{j-1}A_j = (B_j - \lambda_1)^2,$$

причем корни имеют вид (3.1.4.17). □

Предложение 3.1.4.8. *При $j \geq 1$ справедливы тождества*

$$\frac{p_j}{q_j} = \frac{B_j - 2\lambda_1}{\lambda_2} + \frac{A_j}{\lambda_2} \cdot \frac{q_{j-1}}{q_j}, \tag{3.1.4.18}$$

$$-\lambda_0 \cdot \frac{q_j}{p_j} = B_j + A_j \cdot \frac{p_{j-1}}{p_j}, \tag{3.1.4.19}$$

$$\lambda_2 \cdot \frac{p_{j-1}}{q_j} = A_{j-1} \cdot \frac{q_j}{q_{j-1}} - B_j. \tag{3.1.4.20}$$

Доказательство. Без ограничения общности мы предполагаем, что α имеет вид (3.1.2.5). Из формулы (3.1.1.5) выразим α_{j+1}, и, учитывая (3.1.4.6), имеем

$$\alpha_{j+1} = -\frac{\alpha q_{j-1} - p_{j-1}}{\alpha q_j - p_j} = -\frac{(\sqrt{d} - \lambda_1)q_{j-1} - \lambda_2 p_{j-1}}{(\sqrt{d} - \lambda_1)q_j - \lambda_2 p_j}. \tag{3.1.4.21}$$

Подставим это выражение в (3.1.2.4) и приведем к общему знаменателю

$$(B_j - \lambda_1 + \sqrt{d})((\sqrt{d} - \lambda_1)q_j - \lambda_2 p_j) = -A_j((\sqrt{d} - \lambda_1)q_{j-1} - \lambda_2 p_{j-1}),$$

раскрываем скобки и, приравнивая коэффициенты при $\sqrt{d}$ и все остальные, имеем искомые тождества (3.1.4.18)-(3.1.4.19). □

Предложение 3.1.4.9. *Положим*

$$\theta_{j+1} = \alpha_1 \alpha_2 \dots \alpha_{j+1}. \tag{3.1.4.22}$$

тогда при $j \geq 0$ *справедливо тождество*

$$\theta_{j+1} = \frac{(-1)^j}{\alpha q_j - p_j}. \tag{3.1.4.23}$$

Доказательство. По индукции с использованием первой части (3.1.4.21). □

3.1.5. Приведенные элементы

Элемент $\beta \in L$ называется *приведенным* относительно нормирования v_h^-, если $v_h^-(\beta) < 0$ и $v_h^-\left(\overline{\beta}\right) > 0$.

Предложение 3.1.5.1. *Элемент* $\alpha + a_0$ *является приведенным тогда и только тогда, когда* $v_h(\lambda_0) < v_h(\lambda_2) < v_h(\lambda_1)$.

Доказательство. По построению непрерывной дроби $v_h^-(\alpha - a_0) > 0$. Пусть $\alpha + a_0$ — приведенный элемент, тогда $v_h^-(\alpha + a_0) < 0$, $v_h^-(\overline{\alpha} + a_0) > 0$. Следовательно, по теореме Виета

$$v_h\left(\frac{\lambda_1}{\lambda_2}\right) = v_h\left((\alpha - a_0) + (\overline{\alpha} + a_0)\right) \geq \min\left(v_h^-(\alpha - a_0),\ v_h^-(\overline{\alpha} + a_0)\right) > 0, \tag{3.1.5.1}$$

откуда $v_h(\lambda_2) < v_h(\lambda_1)$. Без ограничения общности можем считать, что $\alpha = \frac{-\lambda_1 + \sqrt{d}}{\lambda_2}$. Поскольку $v_h^-(\alpha + a_0) < 0$, то

$$v_h(a_0) = v_h^-(\alpha) = v_h^-\left(\frac{-\lambda_1 + \sqrt{d}}{\lambda_2}\right) < 0, \tag{3.1.5.2}$$

но из неравенства (3.1.5.1) следует, что

$$v_h(a_0) = v_h^-\left(\frac{\sqrt{d}}{\lambda_2}\right) < 0, \tag{3.1.5.3}$$

поэтому,

$$v_h\left(\lambda_1^2 - \lambda_2 \lambda_0\right) = v_h(d) < 2v_h(\lambda_2), \tag{3.1.5.4}$$

значит $v_h(\lambda_0) < v_h(\lambda_2)$.

Обратно, если $v_h(\lambda_0) < v_h(\lambda_2) < v_h(\lambda_1)$, то справедливы неравенства (3.1.5.2), (3.1.5.3) и (3.1.5.4), и по построению непрерывной дроби $v_h^-(\alpha - a_0) > 0$, следовательно, $v_h^-(\alpha + a_0) < 0$. Далее запишем

$$v_h^-(\overline{\alpha} + a_0) = v_h^-\left((a_0 - \alpha) - \frac{2\lambda_1}{\lambda_2}\right) \geq \min\left(v_h^-(\alpha - a_0),\ v_h\left(\frac{2\lambda_1}{\lambda_2}\right)\right) > 0,$$

что и требовалось доказать. □

Предложение 3.1.5.2. *Справедливы следующие утверждения:*

- *при $j \geq 0$ элементы α_{j+1} являются приведенными тогда и только тогда, когда $v_h(d)/2 < v_h(\lambda_2) - 2v_h(q_j)$;*

- *один из элементов α_0 или $\overline{\alpha_0}$ приведенный тогда и только тогда, когда $v_h(\lambda_2) > 0$ и $[\lambda_1/\lambda_2]_h^- = \left[\sqrt{d}/\lambda_2\right]_h^-$ или $[\lambda_1/\lambda_2]_h^- = -\left[\sqrt{d}/\lambda_2\right]_h^-$.*

Доказательство. Элементы α_{j+1} и $\overline{\alpha}_{j+1}$ являются корнями уравнения (3.1.4.8), поэтому по теореме Виета

$$\alpha_{j+1} \cdot \overline{\alpha}_{j+1} = -\frac{A_{j-1}}{A_j}. \tag{3.1.5.5}$$

Если $v_h(d)/2 \leq v_h(\lambda_2) - v_h(q_j) - v_h(q_{j+1})$, то по предложению 3.1.2.4 имеем

$$v_h^-(\overline{\alpha}_{j+1}) = v_h(A_{j-1}) - \frac{1}{2}v_h(d) = \min\left\{-v_h(a_j),\ v_h(\lambda_2) - 2v_h(q_j) - \frac{1}{2}v_h(d)\right\}.$$

Таким образом, $v_h^-(\overline{\alpha}_{j+1}) > 0$ при $j \geq 1$ тогда и только тогда, когда $v_h(d)/2 < v_h(\lambda_2) - 2v_h(q_j)$.

Если же $v_h(d)/2 > v_h(\lambda_2) - v_h(q_j) - v_h(q_{j+1})$, то снова по предложению 3.1.2.4 имеем

$$v_h^-(\overline{\alpha}_{j+1}) = v_h(A_{j-1}) - v_h(A_j) - v_h(a_{j+1}) = v_h(a_{j+1}) < 0,$$

т. е. элемент α_{j+1} не является приведенным.

При $j = 0$ из (3.1.5.5) имеем

$$v_h^-(\overline{\alpha}_1) = \max\left\{v_h(a_1),\ v_h(\lambda_2) - \frac{1}{2}v_h(d)\right\},$$

а при $j = -1$ утверждение очевидно. □

Замечание 3.1.5.3. *Из предложения 3.1.5.2 очевидно следует, что если элемент α_j приведенный, то элемент α_{j+1} также приведенный.*

Замечание 3.1.5.4. *Заметим, что $v_h(q_j) \leq 0$ и при росте j величина $|v_h(q_j)|$ растет. Следовательно, по предложению 3.1.5.2 для элемента α с бесконечной непрерывной дробью всегда найдется номер n, начиная с которого все элементы α_j, $j \geq n$, являются приведенными.*

Замечание 3.1.5.5. *Если $0 = v_h(\lambda_0) < v_h(\lambda_2) < v_h(\lambda_1)$, то $v_h(d) = v_h(\lambda_2)$, поэтому из предложений 3.1.5.1 и 3.1.5.2 следует, что элементы $\alpha + a_0$, α_j, $j \geq 1$, являются приведенными. В этом случае непрерывную дробь элемента $\alpha + a_0$ назовем* чисто приведенной.

Предложение 3.1.5.6. *Если элемент α_j приведенный, то справедливо тождество*

$$\left[\frac{1}{\overline{\alpha}_{j+1}}\right] = -a_j. \tag{3.1.5.6}$$

Если непрерывная дробь элемента $\alpha_0 + a_0$ чисто приведена, то (3.1.5.6) справедливо для $j \geq 1$ и $\left[\overline{\alpha}_1^{-1}\right] = -2a_0$.

Доказательство. Справедливы тождества

$$\frac{1}{\alpha_{j+1}} = \alpha_j - a_j, \qquad \frac{1}{\overline{\alpha}_{j+1}} = \overline{\alpha}_j - a_j. \tag{3.1.5.7}$$

Так как α_j приведенный, то $v_h^-(\overline{\alpha}_j) > 0$, следовательно, выполнено (3.1.5.6). □

3.1.6. Свойства квазипериодических непрерывных дробей

Напомним, что непрерывная дробь элемента α называется *квазипериодической*, если найдутся $m \in \mathbb{N}_0$, $\tau \in \mathbb{N}$ и $b \in K^*$ такие, что $\alpha_{m+\tau} = b\alpha_m$. Наименьшее такое τ называется *длиной квазипериода*. Если соотношение $\alpha_{m+\tau} = b\alpha_m$ выполнено при $m = 0$, то непрерывная дробь называется *чисто квазипериодической*. Минимальное значение m называется *длиной предпериода*.

Предложение 3.1.6.1. *Пусть непрерывная дробь α квазипериодическая. Непрерывная дробь $\tilde{\alpha} = a_0 + \alpha$ чисто квазипериодическая тогда и только тогда, когда $0 = v_h(\lambda_0) < v_h(\lambda_2) < v_h(\lambda_1)$.*

Доказательство. Так как разложение в непрерывную дробь элемента α квазипериодическое, то существуют такие минимальные целые числа $m \geq 1$ и $\tau \geq 1$, что

$$\alpha_{m+\tau} = b\alpha_m, \qquad b \in K^*, \tag{3.1.6.1}$$

или $\alpha_\tau = b(\alpha_0 + a_0)$, если непрерывная дробь $\tilde{\alpha}$ чисто квазипериодическая.

Докажем необходимость. По предложению 3.1.5.2 элемент $\tilde{\alpha} = \alpha + a_0$ является чисто приведенным. Следовательно, по предложению 3.1.5.1 имеем условия $0 = v_h(\lambda_0) < v_h(\lambda_2) < v_h(\lambda_1)$.

Докажем достаточность. Из (3.1.1.12) имеем

$$[a_{m+\tau}, a_{m+\tau+1}, \ldots] = b[a_m; a_{m+1}, \ldots] = [ba_m, b^{-1}a_{m+1}, \ldots], \tag{3.1.6.2}$$

что равносильно $a_{m+\tau+j} = b^{(-1)^j} a_{m+j}$ для $j = 0, 1, 2, \ldots$.

Из равенства (3.1.6.1) следует, что $\overline{\alpha}_{m+\tau} = b\overline{\alpha}_m$. По замечанию 3.1.5.5 непрерывная дробь элемента $\tilde{\alpha} = a_0 + \alpha$ чисто приведена, следовательно, по предложению 3.1.5.6 при $m \geq 2$ получаем $a_{m+\tau-1} = b^{-1}a_{m-1}$. Значит,

$$[a_{m+\tau-1}, a_{m+\tau}, \ldots] = [b^{-1}a_{m-1}, ba_m, b^{-1}a_{m+1}, \ldots] = b^{-1}[a_{m-1}, a_m, \ldots],$$

откуда $\alpha_{m+\tau-1} = b^{-1}\alpha_{m-1}$, что противоречит минимальности m в (3.1.6.1). При $m = 1$ мы также получаем противоречие с единственным отличием в том, что по предложению 3.1.5.6 будет справедливо равенство $a_\tau = b^{-1} \cdot 2a_0$. □

Замечание 3.1.6.2. *Из предложения 3.1.6.1 и замечания 3.1.5.3 следует, что если непрерывная дробь α квазипериодическая и α_m — первое приведенное полное частное непрерывной*

дроби, то квазипериод начинается с α_m *и* $[a_0; a_1, \ldots, a_{m-1}]$ *— предпериод. В этом случае говорят, что длина предпериода равна* m*.*

В следующем предложении дается ответ на вопрос, какой может быть длина предпериода.

Предложение 3.1.6.3. *Пусть непрерывная дробь* α *квазипериодическая с предпериодом* $[a_0; a_1, \ldots, a_{m-1}]$ *длины* m*. Возможен один из четырех случаев:*

1. *если* $v_h^-(\alpha) < 0$ *и* $v_h^-(\overline{\alpha}) > 0$ *(то есть элемент* α *приведенный), то* $m = 0$*, то есть непрерывная дробь* α *чисто квазипериодическая;*
2. *если* $v_h^-(\alpha - \overline{\alpha}) < 0$ *и* $v_h^-(\overline{\alpha}) \leq 0$*, то* $m = 1$*;*
3. *если* $v_h^-(\alpha - \overline{\alpha}) = 0$*, то* $m = 2$*;*
4. *если* $v_h^-(\alpha - \overline{\alpha}) > 0$*, то* $m \geq 2$*.*

Доказательство. Пункт 1 следует из замечания 3.1.6.2.

Предположим выполнены условия пункта 2: $v_h^-(\alpha - \overline{\alpha}) < 0$ и $v_h^-(\overline{\alpha}) \leq 0$. Элемент α не является приведенным, поэтому длина предпериода не меньше 1. По построению непрерывной дроби $v_h^-(\alpha - a_0) > 0$, откуда $v_h^-(\alpha_1) = -v_h^-(\alpha - a_0) < 0$. С другой стороны, так как $v_h^-(\alpha - \overline{\alpha}) < 0$, то

$$v_h^-(\overline{\alpha}_1) = -v_h^-(\overline{\alpha} - a_0) = -v_h^-((\overline{\alpha} - \alpha) + (\alpha - a_0)) > 0.$$

Следовательно, элемент α_1 приведенный, и, значит, длина предпериода равна 1.

Предположим выполнены условия пункта 3: $v_h^-(\alpha - \overline{\alpha}) = 0$. Элемент α не является приведенным, поэтому длина предпериода не меньше 1. По построению непрерывной дроби $v_h^-(\alpha - a_0) > 0$, откуда $v_h^-(\alpha_1) = -v_h^-(\alpha - a_0) < 0$. С другой стороны, так как $v_h^-(\alpha - \overline{\alpha}) = 0$, то

$$v_h^-(\overline{\alpha} - a_0) = v_h^-((\overline{\alpha} - \alpha) + (\alpha - a_0)) \geq 0.$$

Значит,

$$v_h^-(\alpha_1 - \overline{\alpha}_1) = v_h^-(\overline{\alpha} - \alpha) - v_h^-(\alpha - a_0) - v_h^-(\overline{\alpha} - a_0) < v_h^-(\overline{\alpha} - \alpha) = 0.$$

Следовательно, элемент α_1 не является приведенным, но по пункту 2 длина предпериода непрерывной дроби α_1 равна 1, следовательно, длина предпериода непрерывной дроби α равна 2.

Предположим выполнены условия пункта 4: $v_h^-(\alpha - \overline{\alpha}) > 0$. Элемент α не является приведенным, поэтому длина предпериода не меньше 1. По построению непрерывной дроби $v_h^-(\alpha - a_0) > 0$, откуда $v_h^-(\alpha_1) = -v_h^-(\alpha - a_0) < 0$. С другой стороны, так как $v_h^-(\alpha - \overline{\alpha}) > 0$, то

$$v_h^-(\overline{\alpha} - a_0) = v_h^-((\overline{\alpha} - \alpha) + (\alpha - a_0)) > 0.$$

Значит,

$$v_h^-(\alpha_1-\overline{\alpha}_1)=v_h^-(\overline{\alpha}-\alpha)-v_h^-(\alpha-a_0)-v_h^-(\overline{\alpha}-a_0)<v_h^-(\overline{\alpha}-\alpha)<v_h^-(\overline{\alpha}-\alpha).$$

Если $v_h^-(\alpha_1-\overline{\alpha}_1)<0$, то по пункту 2 длина предпериода непрерывной дроби α_1 равна 1, следовательно, длина предпериода непрерывной дроби α равна 2. Если $v_h^-(\alpha_1-\overline{\alpha}_1)=0$, то по пункту 3 длина предпериода непрерывной дроби α_1 равна 2, следовательно, длина предпериода непрерывной дроби α равна 3. Если $v_h^-(\alpha_1-\overline{\alpha}_1)>0$, то длина предпериода непрерывной дроби α не менее 3. □

Если $\alpha_n=c\alpha_0$, то можно записать

$$\alpha_0=[a_0,a_1,\ldots,a_{n-1},c\cdot a_0,c^{-1}a_1,\ldots,c^{(-1)^{n-1}}a_{n-1},c^{(-1)^n+1}\cdot a_0,c^{(-1)^{n+1}-1}a_1,\ldots],$$

т. е.

$$\alpha_0=[a_0,a_1,\ldots,a_{n-1},c\cdot[a_0;a_1,\ldots,a_{n-1},c\cdot[a_0;a_1,\ldots,a_{n-1},c\cdot[a_0;a_1,\ldots]]]].$$

В этом случае более кратко мы будем писать $\alpha_0=[\overline{a_0,a_1,\ldots,a_{n-1}}^{c}]$.

Предложение 3.1.6.4. *Пусть непрерывная дробь α квазипериодическая с квазипериодом $[\overline{a_m,a_{m+1},\ldots,a_{m+\tau-1}}^{c}]$. Тогда сопряженный элемент $\overline{\alpha}$ также квазипериодический с квазипериодом $-c[\overline{a_{m+\tau-1},a_{m+\tau-2},\ldots,a_m}^{c^{-1}}]$. Если непрерывная дробь α чисто квазипериодическая, то непрерывная дробь $\overline{\alpha}^{-1}$ также чисто квазипериодическая.*

Доказательство. Рассуждения проводятся также, как в [118]. Предположим, что $\alpha_{m+\tau}=c\alpha_m$. Обозначим $\beta_j=-\frac{1}{\overline{\alpha_j}}$, тогда по построению

$$\alpha_{j+1}=\frac{1}{\alpha_j-a_j},\quad \overline{\alpha_{j+1}}=\frac{1}{\overline{\alpha_j}-a_j},\quad \beta_j=\frac{1}{\beta_{j+1}-a_j},$$

причем по предложению (3.1.5.6) при $j\geq m$ имеем $[\beta_{j+1}]_h^-=a_j$. Следовательно,

$$\beta_{m+\tau}=[a_{m+\tau-1};a_{m+\tau-2},\ldots,a_m,\beta_m],\quad \beta_m=-\frac{1}{\overline{\alpha_m}}=-\frac{c}{\overline{\alpha_{m+\tau}}}=c\beta_{m+\tau},$$

т. е.

$$\beta_{m+\tau}=[\overline{a_{m+\tau-1};a_{m+\tau-2},\ldots,a_m}^{c^{-1}}],$$

$$\beta_m=[\overline{c\cdot a_{m+\tau-1};c^{-1}\cdot a_{m+\tau-2},\ldots,c^{(-1)^{m+\tau-1}}\cdot 2a_0}^{c^{-1+(-1)^{m+\tau-1}}}].$$

Отсюда следует, что непрерывная дробь элемента $-1/\overline{\alpha_m}$ чисто квазипериодическая, а разложение элемента $\overline{\alpha_m}$ в непрерывную дробь имеет вид

$$\overline{\alpha_m}=[0;-c[\overline{a_{m+\tau-1};a_{m+\tau-2},\ldots,a_m}^{c^{-1}}]].$$

Предложение 3.1.6.4 доказано. □

3.1.7. О периодичности квазипериодических непрерывных дробей

В этом параграфе рассмотрим некоторые условия, при которых квазипериодические элементы гиперэллиптического поля являются также периодическими или чисто периодическими. Далее в §3.2.3 будет доказано, что для элементов вида $\sqrt{f}/x^s$, $s \in \mathbb{Z}$, условие квазипериодичности влечет условие периодичности. Дополнительно о периодичности квазипериодических элементов см. [3; 13; 118; 140—142].

Предложение 3.1.7.1. *Пусть $\lambda_1 = 0$, $\alpha \in L$ является корнем многочлена (3.1.2.1) и непрерывная дробь элемента $\tilde{\alpha} = a_0 + \alpha$ чисто квазипериодическая с длиной квазипериода n, т. е. выполнено $\alpha_n = c\tilde{\alpha}$ с минимальным $n \in \mathbb{N}$ и некоторой постоянной $c \in K^*$. Тогда*

- *при $n = 2k$ возможно только $c = 1$, т. е. непрерывная дробь элемента $\tilde{\alpha}$ чисто периодическая с длиной периода $n = 2k$, причем*

$$\tilde{\alpha} = [\overline{2a_0; a_1, \ldots, a_{k-1},\ a_k, a_{k-1}, \ldots, a_1}]; \tag{3.1.7.1}$$

- *при $n = 2k+1$ и $c = 1$ непрерывная дробь элемента $\tilde{\alpha}$ чисто периодическая с длиной периода $n = 2k+1$, причем*

$$\tilde{\alpha} = [\overline{2a_0; a_1, \ldots, a_{k-1},\ a_k,\ a_k, a_{k-1} \ldots, a_1}]; \tag{3.1.7.2}$$

- *при $n = 2k+1$ и $c \neq 1$ непрерывная дробь элемента $\tilde{\alpha}$ чисто периодическая с длиной периода $2n = 4k+2$, причем*

$$\tilde{\alpha} = [\overline{2a_0; a_1, \ldots, a_{n-1}}^{\,c}] =$$
$$= \left[\overline{2a_0; a_1, \ldots, a_k,\ c^{(-1)^k}a_k, \ldots, c^{-1}a_1, 2ca_0, c^{-1}a_1, \ldots, c^{(-1)^k}a_k,\ a_k \ldots, a_1}\right]. \tag{3.1.7.3}$$

Доказательство. Если $c = 1$, то по определению получаем, что непрерывная дробь элемента $\tilde{\alpha}$ чисто периодическая с длиной периода n.

Предположим, что $c \neq 1$. Пусть разложение в непрерывную дробь элемента α имеет вид $[a_0; a_1, a_2, \ldots]$, тогда $[\tilde{\alpha}]_h^- = 2a_0$ и непрерывную дробь $\tilde{\alpha}$ можно записать $\tilde{\alpha} = [2a_0, a_1, \ldots, a_{n-1}, c\tilde{\alpha}]$, где $c\tilde{\alpha} = [2ca_0, c^{-1}a_1, \ldots, c^{(-1)^{n-1}}a_{n-1}, c^{(-1)^n}c\tilde{\alpha}]$. Отсюда получаем, что $\alpha_{2n} = c^{(-1)^n}c\tilde{\alpha}$. Если $n = 2k+1$, то $\alpha_{2n} = \tilde{\alpha}$, поэтому непрерывная дробь элемента $\tilde{\alpha}$ чисто периодическая с длиной периода $2n$.

Из соотношения (3.1.4.18) при $j = n-1$ имеем

$$\frac{p_{n-1}}{q_{n-1}} = \frac{B_{n-1} - 2\lambda_1}{\lambda_2} + \frac{A_{n-1}}{\lambda_2} \cdot \frac{q_{n-2}}{q_{n-1}}. \tag{3.1.7.4}$$

В силу (3.1.1.10) и (3.1.1.13) получаем

$$a_0+\cfrac{1}{a_1+\cfrac{1}{\cfrac{\dots}{a_{n-2}+\cfrac{1}{a_{n-1}}}}}=\frac{B_{n-1}-2\lambda_1}{\lambda_2}+\cfrac{1}{ca_{n-1}+\cfrac{1}{\cfrac{\dots}{c^{(-1)^{n-1}}a_2+\cfrac{1}{c^{(-1)^n}a_1}}}}, \tag{3.1.7.5}$$

Из $\alpha_n=c\tilde{\alpha}=c(a_0+\alpha)$ следует, что

$$cA_{n-1}=A_{-1}=\lambda_2,\quad B_{n-1}=a_0\lambda_2. \tag{3.1.7.6}$$

Используя условие $\lambda_1=0$, из (3.1.7.5) и единственности разложения в непрерывную дробь, неполные частной которой удовлетворяют условиям $v_h(a_j)<0$ для $j\geq 1$, имеем

$$a_{n-i}=c^{(-1)^i}a_i,\ i=1,\dots,n-1. \tag{3.1.7.7}$$

Если $n=2k+1$, то из (3.1.7.7) следует (3.1.7.3). Если $n=2k$, то из (3.1.7.7) при $i=k$ заключаем $a_k=c^{(-1)^k}a_k$, откуда $c=1$, что противоречит предположению $c\neq 1$. □

В доказательстве предложения 3.1.7.1 мы воспользовались условием $\lambda_1=0$ только для доказательства периодичности в случае четного квазипериода и для описания вида периода (3.1.7.1)-(3.1.7.3), поэтому справедливо следующее предложение.

Предложение 3.1.7.2. *Пусть непрерывная дробь $\alpha\in L$ квазипериодическая $\alpha_{m+\tau}=c\alpha_m$, $c\in K^*$, и длина квазипериода τ нечетна. Тогда непрерывная дробь α периодическая, причем длина периода равна τ, если $c=1$, и равна 2τ, если $c\neq 1$.*

Отметим, что при $\lambda_1\neq 0$ и четной длине квазипериода непрерывная дробь может быть как периодической, так и непериодической. В примере 3.2.3.5 приведен элемент $\alpha\in L$, разложение в непрерывную дробь которого квазипериодическое, но не периодическое.

Теорема 3.1.7.3. *Пусть $\alpha\in L$ является корнем уравнения (3.1.2.1) и непрерывная дробь α квазипериодична. Непрерывная дробь $\alpha_0=\alpha+a_0$ чисто периодична тогда и только тогда, когда $v_h(\lambda_2)>0$ и $\lambda_1=0$, то есть α имеет вид $\alpha=r\sqrt{f}$, где $r\in K(x)$, $v_h(r)<0$.*

Доказательство. Достаточность доказана в предложении 3.1.7.1. Докажем необходимость. По предложению 3.1.6.1 имеем $0=v_h(\lambda_0)<v_h(\lambda_2)<v_h(\lambda_1)$. Остается заметить, что из условий $\alpha_0=\alpha_n$, (3.1.7.5) и (3.1.7.6) при $c=1$ следует, что $\lambda_1=0$. □

Теорема 3.1.7.4. *Пусть $\alpha_0\in L\setminus K(x)$ имеет вид*

$$\alpha_0=\frac{B+\sqrt{d}}{A},\quad d=t^2f,\ t\in K[x],\quad (A,\ B,\ t)=1,\quad A=U\cdot h^s,\ v_h(A)=s>0,$$

и непрерывная дробь α_0 квазипериодична. Тогда следующие условия эквивалентны:

1. *Непрерывная дробь α_0 или $\overline{\alpha_0}$ чисто периодична;*

2. $B/A = \pm\left[\sqrt{d}/A\right]_h^-$;

3. $U \mid f, \quad A \mid B^2 - d, \quad \deg B \le \deg A.$

Доказательство. $1 \Rightarrow 2$. Домножив B на -1 в случае необходимости, мы можем считать, что непрерывная дробь α_0 чисто периодична. По теореме 3.1.7.3 элемент α_0 можно представить в виде $\alpha_0 = \alpha + a_0$, причем $a_0 = [\alpha]_h^-$ и элемент α имеет вид $\alpha = r\sqrt{f}$, где $r \in K(x)$, $v_h(r) < 0$. Отсюда сразу следует требуемое утверждение.

$2 \Rightarrow 1$. Снова домножив B на -1 в случае необходимости, мы можем считать, что по предложению 3.1.5.2 элемент α_0 приведенный и удовлетворяет уравнению

$$(\alpha_0 - a)^2 - 2\left(\frac{B}{A} - a\right)(\alpha_0 - a) + \left(\left(\frac{B}{A} - a\right)^2 - \frac{d}{A^2}\right) = 0, \quad \text{где} \quad a = \frac{1}{2}\left[\frac{B + \sqrt{d}}{A}\right]_h^-.$$

Обозначим $\lambda_2 = A^2$, $\lambda_1 = B - aA$, $\lambda_0 = (B - aA)^2 - d$, тогда $v_h(\lambda_2) > 0$, $\lambda_1 = 0$, $v_h(\lambda_0) = 0$, следовательно, можно применить теорему 3.1.7.3 и получить то, что требуется.

$1, 2 \Rightarrow 3$. В силу чистой периодичности и (3.1.2.4) для $\alpha = \sqrt{d}/A$, $a_0 = [\alpha]_h^- = B/a$, имеем $\lambda_1 = 0$ и $\alpha_0 = \alpha_n = (B_{n-1} + \sqrt{d})/A_{n-1}$, то есть $A = A_{n-1}$, $B = B_{n-1}$. Тогда из (3.1.4.1) получаем, что $A \mid B^2 - d$. Так как знаменатель $[\alpha]_h^-$ имеет вид bh^m, $b \in K^*$, $m \in \mathbb{N}$, то $U \mid B$. В силу $(A,\ B,\ t) = 1$ имеем $(U,\ t) = 1$, и из условия $A \mid B^2 - t^2 f$ выводим $U \mid f$. Наконец, из-за того, что $v_\infty(a_0) \ge 0$, следует неравенство $\deg B \le \deg A$.

$3 \Rightarrow 2$. Запишем $B = U \cdot B_1$, $f = U \cdot f_1$, где $B_1, f_1 \in K[x]$, $\deg B_1 \le s$. Тогда условие $A \mid B^2 - d$ влечет $U \cdot B_1^2 \equiv t^2 \cdot f_1 \pmod{h^s}$. Последнее сравнение с ограничением $\deg B_1 \le s$ равносильно $B_1/h^s = \pm\left[t\sqrt{f_1/U}\right]_h^-$, то есть $B/A = \pm\left[\sqrt{d}/A\right]_h^-$, что и требовалось доказать. □

Следствие 3.1.7.5. *Если непрерывная дробь $\sqrt{f}$ квазипериодическая, то она периодическая только если выполнено одно из эквивалентных условий*

$$1.\ \frac{a_2}{2} = \frac{B_1}{A_1} = \left[\frac{\sqrt{f}}{A_1}\right]_h^-, \quad 2.\ B_2 = B_1 = a_1(f - \gamma^2) - \gamma, \quad 3.\ A_2 = A_0 = f - \gamma^2,$$

где γ — младший коэффициент в разложении $\sqrt{f} \in K((h))$.

Доказательство. По предложению 3.1.5.2 квазипериод начинается с $\alpha_2 = (B_1 + \sqrt{f})/A_1$, то есть непрерывная дробь α_2 чисто квазипериодическая. Далее остается применить теорему 3.1.7.4. Условия 2 и 3 следуют из (3.1.4.1) и (3.1.4.15) соответственно. □

Предложение 3.1.7.6. *Пусть $\alpha \in L$ имеет квазипериодическое разложение в непрерывную дробь с длиной квазипериода τ и длиной предпериода m, и $\alpha_{m+\tau} = c\alpha_m$. Если выполнено одно из эквивалентных условий*

$$1.\ \frac{B_{m-1} - \lambda_1}{A_{m-1}} = \frac{a_m}{2}, \quad 2.\ B_{m-1} = B_m, \quad 3.\ A_{m-2} = A_m,$$

то

$$\left[\frac{B_{m-1}-\lambda_1}{A_{m-1}}\right]_h^- = \frac{B_{m-1}-\lambda_1}{A_{m-1}} = \left[\frac{\sqrt{d}}{A_{m-1}}\right]_h^- = \frac{a_m}{2} = \frac{[\alpha_m]_h^-}{2}$$

и непрерывная дробь α периодическая, причем период имеет вид

$$[\overline{a_m, a_{m+1}, \ldots, a_{m+k-1},\ a_{m+k}, a_{m+k-1}, \ldots, a_{m+1}}], \tag{3.1.7.8}$$

если длина квазипериода $\tau = 2k$, и

$$\left[\overline{a_m; a_{m+1}, \ldots, a_{m+k},\ c^{(-1)^k}a_{m+k}, \ldots, c^{-1}a_{m+1},\ ca_m, c^{-1}a_{m+1}, \ldots, c^{(-1)^k}a_{m+k},\ a_{m+k}\ldots, a_{m+1}}\right], \tag{3.1.7.9}$$

если длина квазипериода $\tau = 2k+1$ и $c \neq 1$.

Доказательство. По предложению 3.1.4.2 имеем

$$\alpha_m + \overline{\alpha_m} = 2\frac{B_{m-1}-\lambda_1}{A_{m-1}}. \tag{3.1.7.10}$$

Из предложения 3.1.6.4 следует, что

$$\alpha_m = [\overline{a_m, a_{m+1}, \ldots, a_{m+\tau-1}}^c], \quad \overline{\alpha_m}^{-1} = -c[\overline{a_{m+\tau-1}, a_{m+\tau-2}, \ldots, a_m}^{c^{-1}}]. \tag{3.1.7.11}$$

С использованием (3.1.4.1) и (3.1.4.15) мы видим, что все три условия в предложении эквивалентны тому, что

$$\frac{B_{m-1}-\lambda_1}{A_{m-1}} = \frac{a_m}{2}. \tag{3.1.7.12}$$

Подставим (3.1.7.11) и (3.1.7.12) в (3.1.7.10), учитывая приведенность α_m и единственность разложения в непрерывную дробь, имеем

$$a_{m+j} = c^{(-1)^{j+1}}a_{m+\tau-j}, \quad j = 1, \ldots, \tau-1, \tag{3.1.7.13}$$

откуда и получается утверждение предложения 3.1.7.6. □

3.1.8. Наилучшее приближение

Для числовых непрерывных дробей подходящие дроби и только они дают наилучшее приближение рациональными числами с ограниченными знаменателями (см., например, [163—165]). Цель этого параграфа — исследовать, справедливо ли аналогичное утверждение для функциональных непрерывных дробей. Нам понадобятся некоторые утверждения из [130], которые мы напомним без доказательств.

Для $p, q \in K[x]$ положим

$$\varphi_h\left(\frac{p}{q}\right) = r - v_h(q), \quad \text{где} \quad r = \max\left(\left[\frac{\deg p}{\deg h}\right], \left[\frac{\deg q}{\deg h}\right]\right). \tag{3.1.8.1}$$

Несократимая дробь $p/q \in K(x)$ является *наилучшим приближением* к $\beta \in \overline{K(x)}$, если для любой другой несократимой дроби $u/w \in K(x)$, $u/w \neq p/q$, такой, что $\varphi_h(u/w) \leq \varphi_h(p/q)$,

справедливо неравенство

$$v_h\left(\beta-\frac{p}{q}\right)>v_h\left(\beta-\frac{u}{w}\right).$$

Положим $s=v_h(p)$, $t=v_h(q)$ и запишем представление p/q в $\Sigma(h^{-1})$:

$$\frac{p}{q}=\frac{p_sh^{s-r}+p_{s+1}h^{s+1-r}+\ldots+p_r}{q_th^{t-r}+q_{t+1}h^{t+1-r}+\ldots+q_r},$$

где $p_j,q_j\in\Sigma$. В такой записи $\varphi_h(p/q)=r-t$ — максимальная степень по h^{-1} знаменателя.

Теорема 3.1.8.1. *Пусть $\beta\in\overline{K(x)}$ и $p/q\in K(x)$.*

1. *Пусть $\deg h=1$. Дробь p/q является наилучшим приближением к β тогда и только тогда, когда $v_h(\beta-p/q)>2\varphi_h(p/q)$;*

2. *Пусть $\deg h>1$. Если $v_h(\beta-p/q)>2\varphi_h(p/q)+1$, то дробь p/q является наилучшим приближением к β. Если дробь p/q является наилучшим приближением к β, то $v_h(\beta-p/q)>2\varphi_h(p/q)$.*

Доказательство. См. теорему 5.4 из [130]. □

Предложение 3.1.8.2. *Пусть дроби $p/q,\ u/w\in K(x)$ являются наилучшими приближениями к $\beta\in\overline{K(x)}$ и $\varphi_h(p/q)=\varphi_h(u/w)$. Тогда найдется такая константа $b\in K^*$, что $p=bu$, $q=bw$.*

Доказательство. См. предложение 5.5 из [130]. □

Теорема 3.1.8.3. *Пусть $\deg h=1$. Справедливы следующие утверждения:*

1. *j-я подходящая дробь p_j/q_j к β является наилучшим приближением к β;*

2. *если дробь u/w является наилучшим приближением к β, то найдется такая подходящая дробь p_j/q_j к β и такая константа $b\in K^*$, что $u=bp_j$, $w=bq_j$.*

Доказательство. См. теорему 5.6 из [130]. □

Следующая теорема в случае $\deg h=1$ дает достаточные условия наилучшего приближения, являющегося решением норменного уравнения.

Теорема 3.1.8.4. *Пусть $\deg h=1$. Пусть $\alpha\in L$ является корнем $H(X)$, как в (3.1.2.1), причем коэффициенты $\lambda_0,\lambda_1,\lambda_2$ удовлетворяют соотношениям:*

$$0=v_h(\lambda_0)<v_h(\lambda_2)<v_h(\lambda_1), \tag{3.1.8.2}$$

$$2(\deg\lambda_2-\deg\lambda_0)<v_h(\lambda_2), \tag{3.1.8.3}$$

$$\deg\lambda_2-\deg\lambda_0<2(\deg\lambda_2-\deg\lambda_1). \tag{3.1.8.4}$$

Пусть при некоторых $m \in \mathbb{N}$ и $b \in K^*$ норменное уравнение

$$N_{L/K(x)}(\omega_1 - \alpha\omega_2) = bh^m \tag{3.1.8.5}$$

имеет решение в многочленах $\omega_1, \omega_2 \in K[x]$, $v_h(\omega_1) = 0$. Тогда ω_1/ω_2 является наилучшим приближением к α и, следовательно, $\omega_1/\omega_2 = p_n/q_n$ для некоторой подходящей дроби p_n/q_n к α.

Доказательство. Из условий (3.1.8.2), $v_h(f) = 0$ и замечания 3.1.2.5 имеем $v_h(\lambda_2) = 2s_0$ для некоторого $s_0 \in \mathbb{N}$. Так как $v_h^-(\alpha) = -s_0$, то $v_h(\omega_2) = s_0$, $v_h(\omega_1) = 0$. Для того, чтобы дробь ω_1/ω_2 являлась наилучшим приближением к α, необходимо, чтобы было выполнение неравенство

$$m - s_0 = v_h^-\left(\alpha - \frac{\omega_1}{\omega_2}\right) > 2\varphi_h\left(\frac{\omega_1}{\omega_2}\right) = 2\max(\deg\omega_1,\ \deg\omega_2) - 2v_h(\omega_2). \tag{3.1.8.6}$$

Далее мы получим оценку на значение m с помощью сравнения нормирований у слагаемых норменного уравнения (3.1.8.5).

Используя выражение (3.1.2.6), запишем явно норменное уравнение (3.1.8.5)

$$N_{L/K(x)}(\omega_1 - \alpha\omega_2) = \frac{H(\omega_1,\omega_2)}{\lambda_2} = \left(\omega_1 + \omega_2\frac{\lambda_1}{\lambda_2}\right)^2 - \left(\frac{\omega_2}{\lambda_2}\right)^2 d = \tag{3.1.8.7}$$

$$= \omega_1^2 + 2\frac{\lambda_1}{\lambda_2}\omega_1\omega_2 + \left(\frac{\lambda_1}{\lambda_2}\omega_2\right)^2 - \left(\left(\frac{\lambda_1}{\lambda_2}\omega_2\right)^2 - \frac{\lambda_0}{\lambda_2}\omega_2^2\right) = bh^m. \tag{3.1.8.8}$$

В силу (3.1.8.4) имеем

$$-v_\infty\left(\left(\frac{\lambda_1}{\lambda_2}\omega_2\right)^2\right) < -v_\infty\left(\frac{\lambda_0}{\lambda_2}\omega_2^2\right).$$

Рассмотрим два случая:

$$-v_\infty(\omega_1) \le -v_\infty\left(\frac{\lambda_1}{\lambda_2}\omega_2\right), \quad -v_\infty(\omega_1) > -v_\infty\left(\frac{\lambda_1}{\lambda_2}\omega_2\right).$$

Пусть

$$-v_\infty(\omega_1) \le -v_\infty\left(\frac{\lambda_1}{\lambda_2}\omega_2\right), \tag{3.1.8.9}$$

тогда из (3.1.8.8) имеем $m = -v_\infty\left(\frac{\lambda_0}{\lambda_2}\omega_2^2\right)$. Таким образом, для того, чтобы было справедливо неравенство (3.1.8.6), нам необходимо показать, что

$$\deg\lambda_0 - \deg\lambda_2 + s_0 > 2\max(\deg\omega_1 - \deg\omega_2,\ 0). \tag{3.1.8.10}$$

Если $\deg\omega_2 \le \deg\omega_1$, то по предположению (3.1.8.9) имеем

$$0 \le \deg\omega_1 - \deg\omega_2 \le \deg\lambda_1 - \deg\lambda_2,$$

откуда с использованием (3.1.8.4) получаем

$$0 \le 2(\deg\omega_1 - \deg\omega_2) \le 2(\deg\lambda_1 - \deg\lambda_2) < \deg\lambda_0 - \deg\lambda_2 < \deg\lambda_0 - \deg\lambda_2 + s_0,$$

что и требовалось показать в (3.1.8.10). Если же $\deg\omega_2 > \deg\omega_1$, то (3.1.8.10) следует из неравенств (3.1.8.3).

Пусть

$$-v_\infty(\omega_1) > -v_\infty\left(\frac{\lambda_1}{\lambda_2}\omega_2\right),$$

тогда $m = -\max(2\deg\omega_1,\ 2\deg\omega_2 + \deg\lambda_0 - \deg\lambda_2)$, т. е. необходимо показать, что

$$\max\bigl(2(\deg\omega_1 - \deg\omega_2),\ \deg\lambda_0 - \deg\lambda_2\bigr) + s_0 > 2\max(\deg\omega_1 - \deg\omega_2,\ 0).$$

Из неравенств (3.1.8.3) и (3.1.8.4) это очевидно.

Теперь, учитывая неравенство (3.1.8.6), по теореме 3.1.8.3 найдется подходящая дробь $\frac{p_n}{q_n}$ к α такая, что $\frac{p_n}{q_n} = \frac{\omega_1}{\omega_2}$. □

Следующие примеры показывают, что ни от одного из условий (3.1.8.3) и (3.1.8.4) в теореме 3.1.8.4 избавиться нельзя.

Пример 3.1.8.5. *Пусть α является корнем уравнения $h^2fX^2-1=0$, где $h\in K[x]$, $\deg h = 1$, $f = 1 - bh^m$, $b\in K^*$, m — нечетное положительное число. Здесь $\lambda_2 = h^2f$, $\lambda_1 = 0$, $\lambda_0 = -1$, $d = h^2f$ и справедливы неравенства $0 = v_h(\lambda_0) < v_h(\lambda_2) = 2 < v_h(\lambda_1) = \infty$, $s_0 = 1$. Пусть $\omega_1 = 1$, $\omega_2 = hf$. Тогда пара $\omega_1,\omega_2 \in K[x]$, $v_h(\omega_1) = 0$, является решением норменного уравнения*

$$\omega_1^2 - \frac{1}{h^2f}\omega_2^2 = bh^m.$$

Отметим, что выполнены все условия теоремы 3.1.8.4 кроме (3.1.8.3), и при этом ω_1/ω_2 не является наилучшим приближением к α, поскольку не выполнено неравенство

$$m + s_0 > 2\max(\deg\omega_1,\ \deg\omega_2), \tag{3.1.8.11}$$

а, следовательно, не выполнено и (3.1.8.6).

Пример 3.1.8.6. *Пусть $\deg h = 1$ и*

$$\lambda_0 = h^{4k}\mu^2 + bh^m - 1, \quad \lambda_1 = h^{3k}\mu, \quad \lambda_2 = h^{2k},$$

где $b\in K^*$, $m,k\in\mathbb{N}$, m нечетно, $\mu\in K[x]$, $\deg\mu \geq (m-3k)/2$, $v_h(\mu) = 0$. Пусть α является корнем уравнения $\lambda_2X^2 + 2\lambda_1X + \lambda_0 = 0$ с дискриминантом $d = \lambda_1^2 - \lambda_0\lambda_2 = h^{2k}(1-bh^m)$, $\sqrt{d}\in L$, $s_0 = k$. Тогда пара $\omega_1 = 1 - h^{2k}\mu$, $\omega_2 = h^k$ является решением уравнения $N_{L/K(x)}(\omega_1 - \alpha\omega_2) = bh^m$, что может быть непосредственно проверено с использованием (3.1.8.7). Однако ω_1/ω_2 не является наилучшим приближением к α, поскольку не выполнено неравенство (3.1.8.11). Отметим, что в этом примере выполнены все условия теоремы 3.1.8.4 за исключением условия (3.1.8.4).

Пример 3.1.8.7. *Пусть $\deg h = 1$ и α является корнем уравнения $h^{2k}X^2 - f = 0$, где многочлен $f\in K[x]$ нечетной степени, $v_h(f) = 0$, $\sqrt{f}\in L$, $k\in\mathbb{N}$, $0 < k < \deg f$. Пусть*

пара многочленов $\omega_1, \omega_2 \in K[x]$, $v_h(\omega_1) = 0$, *дает решение уравнения* $N_{L/K(x)}(\omega_1 - \alpha\omega_2) = bh^m$ *при некоторых* $m \in \mathbb{N}$ *и* $b \in K^*$. *Тогда по теореме 3.1.8.4 дробь* $\frac{\omega_1}{\omega_2}$ *является наилучшим приближением к* $\alpha = \sqrt{f}/h^k$ *и, следовательно,* $\frac{\omega_1}{\omega_2} = \frac{p_n}{q_n}$ *для некоторой подходящей дроби* $\frac{p_n}{q_n}$ *к* α.

Положим $S = \{v_h, v_\infty\}$, если бесконечное нормирование v_∞ поля $K(x)$ имеет единственное продолжение на $L = K(x)(\sqrt{f})$, и $S = \{v_h, v_\infty^-, v_\infty^+\}$ иначе.

Теорема 3.1.8.8. *Пусть* $\deg h = 1$ *и* $\alpha \in L$ *является корнем* $H(X)$, *как в* (3.1.2.1), *с дискриминантом* $d = \omega^2 f$, *причем коэффициенты* $\lambda_0, \lambda_1, \lambda_2$ *удовлетворяют соотношениям* (3.1.8.2)-(3.1.8.4) *и* $v_h(\lambda_2) = 2s_0$. *Тогда для* $m, n \in \mathbb{N}$ *и* $\omega_1, \omega_2, \mu_1, \mu_2 \in K[x]$, $v_h(\omega_1) = 0$, *следующие условия эквивалентны:*

1. m — *наименьшее число, для которого существует решение норменного уравнения* (3.1.8.5), *где* $b \in K^*$. *В этом случае* ω_1/ω_2 *является наилучшим приближением к* α, $\omega_1/\omega_2 = p_{n-1}/q_{n-1}$.

2. n — *наименьшее число, для которого многочлен* A_{n-1}, *определенный в* (3.1.2.2), *имеет вид* $A_{n-1} = b_0\lambda_2 h^{s_n - s_0}$, $b_0 \in K^*$, $s_n \in \mathbb{N}$. *В этом случае* $v_h(A_{n-1}) = m + 2v_h^-(\theta_{n-1})$, *где величина* θ_{n-1} *определена в* (3.1.4.22).

3. $\xi = \omega_1 - \omega_2\alpha$ *является* S*-единицей степени* m, *причем* m — *минимальная степень среди* S*-единиц вида* $z_1 - z_2\alpha$, *где* $z_1, z_2 \in K[x]$, $v_h(z_1) = 0$. *В этом случае* $\lambda_2 \mid \gcd(\lambda_1, \omega) \cdot \omega_2$.

4. *Существует* S*-единица* $\xi = \mu_1 + \mu_2\sqrt{f}$ *такая, что* $\omega \mid \gcd(\lambda_1, \lambda_2) \cdot \mu_2$ *и* $v_h(\mu_1) = 0$, *причем* $\deg \xi = m$ — *минимальная степень среди* S*-единиц такого вида.*

Если выполнен пункт 4, $\omega \mid \mu_2 \cdot h^{s_0}$ *и*

$$|2(\deg \mu_1 - \deg \mu_2) - \deg f| \geq |\deg \lambda_0 - \deg \lambda_2|, \tag{3.1.8.12}$$

то непрерывная дробь α *квазипериодическая.*

Доказательство. Пусть норменное уравнение (3.1.8.5) имеет решение $\omega_1, \omega_2 \in K[x]$, $v_h(\omega_1) = 0$, $b \in K^*$. Тогда по теореме 3.1.8.4 ω_1/ω_2 является наилучшим приближением к α и, следовательно, $\omega_1/\omega_2 = p_{n-1}/q_{n-1}$ для некоторой подходящей дроби p_{n-1}/q_{n-1} к α. Определим $H(X, Y)$ как в (3.1.2.6), тогда (3.1.8.5) равносильно

$$H(\omega_1, \omega_2) = b\lambda_2 h^m.$$

Обозначим $t_n = \sum_{j=1}^n s_j$, где $s_j = -v_h(a_j)$, тогда из (3.1.1.6)-(3.1.1.8) и предложения 3.1.4.9 имеем

$$p_{n-1} = c\frac{\omega_1}{h^{t_{n-1}+s_0}}, \quad q_{n-1} = c\frac{\omega_2}{h^{t_{n-1}+s_0}}, \quad c \in K^*, \quad v_h(\theta_{n-1}) = -t_{n-1}. \tag{3.1.8.13}$$

Следовательно, по определению (3.1.2.2) многочлена A_{n-1} получаем

$$A_{n-1} = (-1)^n H(p_{n-1}, q_{n-1}) = \frac{(-1)^n c^2}{h^{2t_{n-1}+2s_0}} H(\omega_1, \omega_2) = b_0 \lambda_2 h^{m-2t_{n-1}-2s_0}. \tag{3.1.8.14}$$

С другой стороны замечание 3.1.2.5 влечет $v_h(\lambda_2) = 2s_0$ и $v_h(A_{n-1}) = s_0 + s_n$, откуда $m = v_h(A_{n-1}) - 2v_h^-(\theta_{n-1})$. Таким образом, доказано, что из пункта 1 следует пункт 2. Приведенные рассуждения можно провести в обратную сторону, восстановив многочлены ω_1, ω_2 из (3.1.8.13). При этом будет справедливы равенства (3.1.8.14), а следовательно, многочлены ω_1, ω_2 являются решением норменного уравнения (3.1.8.5). Условия минимальности n и m дополняют друг друга. Эквивалентность пунктов 1 и 2 доказана.

Пусть выполнен пункт 1 и $\xi = \omega_1 - \omega_2\alpha$. Поскольку $\xi \cdot \overline{\xi} = bh^m$, то для некоторого $r \in \mathbb{Z}$ можно записать

$$\xi = \frac{\mu_1 + \mu_2\sqrt{f}}{h^r}, \quad \mu_1, \mu_2 \in K[x], \quad v_h(\mu_1) = 0.$$

Так как $\xi = \omega_1 - \omega_2\alpha = c^{-1}h^{t_{n-1}+s_0}(p_{n-1} - q_{n-1}\alpha)$, то из (3.1.1.8) имеем $v_h^-(\xi) = s_0 + t_{n-1} + t_n = m$, следовательно, $v_h^+(\xi) = 0$, $r = 0$ и ξ является S-единицей. Считая, что α имеет вид (3.1.2.5), получаем

$$\xi = \mu_1 + \mu_2\sqrt{f} = \omega_1 - \alpha\omega_2 = \omega_1 + \frac{\lambda_1\omega_2}{\lambda_2} - \frac{\omega\omega_2}{\lambda_2}\sqrt{f}.$$

Значит,

$$\mu_1 = \omega_1 + \frac{\lambda_1\omega_2}{\lambda_2}, \quad \mu_2 = -\frac{\omega\omega_2}{\lambda_2}, \quad \text{и} \quad \omega_1 = \mu_1 + \frac{\lambda_1\mu_2}{\omega}, \quad \omega_2 = -\frac{\lambda_2\mu_2}{\omega}. \tag{3.1.8.15}$$

Остается только заметить, что если существует S-единица вида, как в пункте 3 или пункте 4, но меньшей степени, чем m, то данная S-единица даст решение норменного уравнения (3.1.8.5) с меньшим значением m, что противоречит условию пункта 1. Эквивалентность пунктов 1, 3 и 4 доказана.

Пусть выполнены условия пункта 4, $\omega \mid \mu_2 \cdot h^{s_0}$ и справедливо неравенство (3.1.8.12). Если $r_0 = \max(\deg\lambda_0, \deg\lambda_2)$, то неравенство (3.1.8.12) эквивалентно неравенству

$$\max(\deg\mu_1 - \deg\mu_2, \deg\mu_2 - \deg\mu_1 + \deg f) \geq r_0 - \deg\omega,$$

которое эквивалентно $\deg\tilde{\mu}_1 - \deg\tilde{\mu}_2 \geq r_0 - s_0$, где многочлены $\tilde{\mu}_1, \tilde{\mu}_2 \in K[x]$ такие, что $\tilde{\mu}_1 - \tilde{\mu}_2\sqrt{d_0} = \xi$ или $\tilde{\mu}_1 - \tilde{\mu}_2\sqrt{d_0} = \xi^2$, $d_0 = d \cdot h^{-2s_0}$. Таким образом, справедливо условие 2 теоремы 3.2.1.1, что влечет квазипериодичность непрерывной дроби α. □

Следующий пример показывает, что существуют элементы $\alpha \in L$, для которых выполнены все условия теоремы 3.1.8.8, включая эквивалентные пункты 1 - 4, однако разложение α в непрерывную дробь не квазипериодическое. В частности, наличие нетривиального решения норменного уравнения (3.1.8.5), вообще говоря, не влечет квазипериодичность непрерывной дроби элемента α.

Пример 3.1.8.9. *Пусть α является корнем уравнения*

$$h^2(1-h)^3X^2 - (h^{2g} + h^{2g-1} + \ldots + h + 1) = 0,$$

где $h \in K[x]$, $\deg h = 1$, $g > 2$. Тогда имеем

$$f = 1 - h^{2g+1}, \quad Q = 1 - h, \quad d = h^2Q^2f, \quad \omega = hQ, \quad s_0 = 1,$$
$$\lambda_2 = h^2Q^3, \quad \lambda_1 = 0, \quad \lambda_0 = \frac{f}{Q}.$$

Существует решение норменного уравнения

$$\omega_1^2 - \frac{f}{h^2Q^4}\omega_2^2 = h^{2g+1}, \quad \omega_1 = 1,\ \omega_2 = hQ^2.$$

Этому решению соответствует S-единица $\mu_1+\mu_2\sqrt{f} = 1-\sqrt{f}$, где значения $\mu_1 = 1$, $\mu_2 = -1$ вычислены по формулам (3.1.8.15). Так как $Q \mid f$, то для любой S-единицы $\tilde{\mu}_1 - \tilde{\mu}_2\sqrt{f}$ имеем $v_Q(\tilde{\mu}_2) = v_Q(\mu_2) = 0$.

Выполнены все условия теоремы 3.1.8.4, поэтому ω_1/ω_2 является наилучшим приближением к $\alpha = \sqrt{f}h^{-1}Q^{-2}$. Также выполнены условия теоремы 3.1.8.8, включая эквивалентные пункты 1 - 4, в поле $L = K(x)(\sqrt{f})$ существует нетривиальная S-единица $1 - \sqrt{f}$. Так как из пункта 4 теоремы 3.1.8.8 имеем $\mu_2 = -1$, то при приведенных условиях непрерывная дробь элемента α не квазипериодическая, так как не существует S-единицы $\tilde{\mu}_1 - \tilde{\mu}_2\sqrt{f}$ такой, что $\omega \mid \tilde{\mu}_2 \cdot h^{s_0}$.

Пусть $\deg h = 1$ и $S = \{v_\infty, v_h^-\}$.

Предложение 3.1.8.10. *Пусть $\alpha \in L$ является корнем многочлена $H(X)$, как в (3.1.2.1), с дискриминантом $d = \lambda_1^2 - \lambda_2\lambda_0 = \omega^2 f$, причем $\lambda_2,\ \lambda_1,\ \lambda_0$ удовлетворяют условиям (3.1.8.2)-(3.1.8.4), $v_h(\lambda_2) = 2s_0$. В поле L существует такая фундаментальная S-единица $u = \theta_1 + \theta_2\sqrt{f}$, что $\theta_1, \theta_2 \in K[x]$, $v_h(\theta_1) = 0$, $\lambda_2 \mid h^{s_0}\omega\theta_2$, тогда и только тогда, когда существует минимальное целое $n \geq 2$ такое, что $A_n = b_0\lambda_2h^{m_0}$ для некоторых $m_0 \in \mathbb{Z}$ и $b_0 \in K^*$.*

Доказательство. Пусть в поле L есть фундаментальная S-единица $u = \theta_1 + \theta_2\sqrt{f}$ такая, что $\lambda_2 \mid h^{s_0}\omega\theta_2$. Тогда найдутся такие многочлены $\omega_1, \omega_2 \in K[x]$, $v_h(\omega_1) = 0$, что $\theta_1 + \sqrt{f}\theta_2 = \omega_1 - \alpha\omega_2$, и норменное уравнение имеет вид $H(\omega_1, \omega_2) = b\lambda_2h^m$. Используя теорему 3.1.8.4 и деля норменное уравнение на $h^{2t_{n-1}+2s_0}$, получаем $A_n = (-1)^{n+1}H(p_n,\ q_n)$, где $m_0 = 2 - 2t_{n-1} - 2s_0$.

Доказательство обратного утверждения тривиально. □

3.2. О квазипериодичности и периодичности функциональных непрерывных дробей

Для числовых непрерывных дробей хорошо известна теорема Эйлера-Лагранжа, согласно которой квадратичные иррациональности и только они имеют периодическое разложение в непрерывную дробь (см., например, [163—165]). Из теоремы Эйлера-Лагранжа следует, что уравнение Пелля вида $x^2 - dy^2 = 1$ имеет нетривиальные решения в целых числах (x, y) для любого целого неотрицательного свободного от квадратов $d \geq 2$. Нетривиальными называются решения (x, y), для которых $y \neq 0$. "Базисное" решение $(x, y) = (p, q)$ уравнения Пелля может быть построено с помощью подходящей дроби $p/q = p_n/q_n$ к $\sqrt{d}$, причем непрерывная дробь $\sqrt{d}$ имеет вид $[a_0; \overline{a_1, \ldots, a_n, 2a_0}]$. Далее, по базисному решению восстанавливается бесконечная серия решений с помощью возведения в целую степень единицы $p + q\sqrt{d}$ кольца целых элементов поля $\mathbb{Q}(\sqrt{d})$.

В *функциональном случае* вместо целого d рассматривается свободный от квадратов многочлен $f(x)$, определенный над некоторым полем K; вместо уравнения Пелля $x^2 - dy^2 = 1$ рассматривается *функциональное уравнение типа Пелля* $\omega_1^2 - \omega_2^2 f = bh^m$, решение которого ищется в виде набора $(\omega_1, \omega_2, b, m)$, где $\omega_1, \omega_2 \in K[x]$, $b \in K^*$, $m \in \mathbb{N}$. В этом разделе $h \in K[x]$ многочлен первой степени, который без ограничения общности можно считать совпадающим с x. В дальнейшем в следующих главах будут рассмотрены функциональные непрерывные дроби обобщенного типа, построенные с помощью неприводимого над K многочлена h второй степени и с помощью двух линейных многочленов (см. главу 5). Таким образом, вместо кольца $\mathbb{Z}$ в функциональном случае рассматривается кольцо $K[x]$, вместо поля $\mathbb{Q}(\sqrt{d})$ — поле $K(x)(\sqrt{f})$. В разделе 3.1 было показано, как может быть определена функциональная непрерывная дробь, а также доказаны простейшие свойства, связанные с полными и неполными частными.

Интересно, что теорема Эйлера-Лагранжа о числовых непрерывных дробях не имеет полного аналога в функциональном случае, поскольку оказывается, что не только не все функциональные квадратичные иррациональности имеют периодическое разложение в непрерывную дробь, а более того, существуют поля $K(x)(\sqrt{f})$, в которых ни один элемент не имеет периодического разложения в непрерывную дробь. Однако, все же некоторую аналогию провести можно, а именно наличие периодических непрерывных дробей оказывается напрямую связано с разрешимостью функционального уравнения типа Пелля. В случае наличия решений, "базисное" решение может быть построено аналогично числовому случаю с помощью подходящих дробей. "Базисному" решению соответствует *фундаментальная S-единица*, с помощью которой восстанавливаются все решения функционального уравнения типа Пелля. В работе [52] рассмотрена аналогия с теоремой Эйлера-Лагранжа для функциональных непрерывных

дробей с другой стороны. А именно, в этой работе доказано, что для любой функциональной квадратичной иррациональности последовательность степеней неполных частных непрерывной дроби, построенной в поле $K((1/x))$, всегда периодическая.

Текущая глава посвящена исследованию функционального аналога теоремы Эйлера-Лагранжа и сопутствующим утверждениям о периодичности и квазипериодичности непрерывных дробей в функциональном случае.

В §3.2.1 доказан функциональный аналог теоремы Эйлера-Лагранжа о периодичности (квазипериодичности) непрерывных дробей квадратичных иррациональностей. В теореме 3.2.1.1 сформулирован критерий квазипериодичности непрерывных дробей, построенных в поле $K((h))$, $\deg h = 1$, для квадратичных иррациональностей гиперэллиптического поля L (теорема 3.2.1.1). Для непрерывных дробей, построенных в $K((1/x))$ аналогичный критерий был получен в [118]. В теореме 3.2.1.3 найден промежуток значений $s \in \mathbb{Z}$, для которых квадратичные иррациональности α и $h^s\alpha$ одновременно квазипериодические.

В §3.2.2 доказаны технические предложения 3.2.2.2 и 3.2.2.1.

В §3.2.3 в теореме 3.2.3.3 доказано, что для ключевых элементов вида $\sqrt{f}/h^s$, $s \in \mathbb{Z}$, условие квазипериодичности непрерывной дроби влечет ее периодичность. Впервые этот факт был доказан в статьях [141; 166] с некоторыми ограничениями, и в полной общности доказан в [142]. В предложении 3.2.3.4 доказан уточненный критерий периодичности для "ключевых" элементов.

В §3.2.4 обсуждается алгоритм поиска квазипериодических непрерывных дробей, а также приведены примеры непрерывных дробей, найденные с помощью приведенного алгоритма.

В §3.2.5 строится пример непрерывной дроби с несимметричным периодом, причем этот период не может быть приведен к симметричному виду циклическими сдвигами. Ранее нам не встречались в литературе примеры таких непрерывных дробей для элементов гиперэллиптического поля L.

Результаты этого раздела опубликованы в [14; 17; 19].

3.2.1. Критерий квазипериодичности непрерывных дробей

В этом параграфе используются обозначения и результаты §2.3.5. Основные утверждения этого параграфа представлены в статьях [17; 19].

Пусть $h \in K[x]$, $\deg h = 1$.Тогда $K[x] = K[h]$, $K(x) = K(h)$. Там, где это уместно, обозначения будем вести от элемента h так, что $f = f(h) \in K[h]$ и $L = K(h)(\sqrt{f})$. Без ограничения общности в этом разделе можно считать $h = x$. Далее в главе 5 введение элемента h, отличного от x, будет существенно.

Пусть α является корнем многочлена

$$H(X) = \lambda_2 X^2 + 2\lambda_1 X + \lambda_0, \quad \text{где } \lambda_0, \lambda_1, \lambda_2 \in K[h], \quad (\lambda_0,\ \lambda_1,\ \lambda_2) \in K^*. \tag{3.2.1.1}$$

Величину $d = \lambda_1^2 - \lambda_2\lambda_0$ будем называть сокращенным дискриминантом многочлена (3.2.1.1) или просто *дискриминантом*. Будем предполагать, что d/f является полным квадратом в поле $K(h)$, т. е. $d = \omega^2 f$, $\omega \in K[h]$ и $\alpha \in L = K(h)(\sqrt{f})$. Пусть $\alpha = [a_0; a_1, \ldots]$ — разложение α в непрерывную дробь, соответствующее нормированию v_h^-.

Положим $\overline{\alpha}$ — второй корень уравнения (3.2.1.1). Элемент $\overline{\alpha}$ будем называть *сопряженным* к α с помощью *инволюции* $\iota : L \to L$, меняющий $\sqrt{f}$ на $-\sqrt{f}$.

Центральным утверждением этого параграфа является следующий критерий квазипериодичности непрерывной дроби произвольной квадратичной иррациональности α, построенной в поле формальных степенных рядов $K((h))$.

Теорема 3.2.1.1. *Пусть $h \in K[x]$, $\deg h = 1$ и $f \in K[h]$ свободный от квадратов многочлен. Пусть нормирование v_h поля $K(x)$ имеет два продолжения v_h^- и v_h^+ на поле $L = K(h)(\sqrt{f})$. Пусть $\alpha \in L \setminus K(h)$ является корнем уравнения (3.2.1.1) с дискриминантом $d = \omega^2 f$, $\omega \in K[h]$. Положим $r = \max(\deg \lambda_0,\ \deg \lambda_1,\ \deg \lambda_2)$. Тогда следующие условия эквивалентны:*

1. *непрерывная дробь α, построенная в поле формальных степенных рядов $K((h))$, квазипериодическая;*

2. *в поле L существует нетривиальная S_h-единица вида $u = h^{-m}(\omega_1 + \omega_2\sqrt{d})$, где $S_h = \{v_h^-,\ v_h^+\}$, $\omega_1, \omega_2 \in K[x]$, $v_h(\omega_2) = 0$, $\deg \omega_1 - \deg \omega_2 \geq r$;*

3. *уравнение*

$$\omega_1^2 - d\omega_2^2 = bh^{2m} \tag{3.2.1.2}$$

имеет решение $\omega_1, \omega_2 \in K[h]$ такое, что $v_h(\omega_2) = 0$, $\deg \omega_1 - \deg \omega_2 \geq r$, $b \in K^*$, $\deg \omega_1 = m$.

Доказательство. Докажем эквивалентность пунктов 1 и 3.

Положим $X = h^{-1}$, $\Lambda_i = h^{-r}\lambda_i$, $i = 0, 1, 2$, $D = \Lambda_1^2 - \Lambda_0\Lambda_2$, тогда $\Lambda_i, D \in K[X]$ и $\deg_X \Lambda_i = r - v_h(\lambda_i)$, $\deg_X D = 2r - v_h(d) = 2r - 2s_0$, $(\Lambda_0, \Lambda_1, \Lambda_2) \in K^*$, где $v_h(d) = 2s_0$ четно, поскольку нормирование v_h поля $K(x)$ имеет два продолжения на поле L. Разложение элемента α в непрерывную дробь имеет одинаковый вид в полях $K((h))$ и $K((1/X))$. Следовательно, по теореме 2 [118] непрерывная дробь α будет квазипериодической тогда и только тогда, когда найдутся элементы $\Omega_1, \Omega_2 \in K[X]$ такие, что $\Omega_1^2 - D\Omega_2^2 \in K^*$, $\Omega_2 \neq 0$. По Ω_1, Ω_2 можно восстановить ω_1, ω_2, удовлетворяющие условиям теоремы. Действительно, положим $e = \deg_X \Omega_2$, $\omega_1 = h^{r+e}\Omega_1$, $\omega_2 = h^e\Omega_2$, тогда справедливо $\omega_1^2 - d\omega_2^2 = bh^m$, причем $v_h(\omega_2) = 0$,

$\deg\omega_1 - \deg\omega_2 \geq r$ и $m = 2(r+e)$, $v_h(\omega_1) = s_0$. Так как по данным ω_1, ω_2 можно аналогичным образом восстановить Ω_1, Ω_2, то эквивалентность пунктов 1 и 3 доказана.

Докажем эквивалентность пунктов 2 и 3.

Наличие S_h-единицы степени $m_1 = m - s_0$, как в пункте 2, равносильно (2.3.5.4), где

$$\mu_1 = h^{-s_0}\omega_1, \quad \mu_2 = \omega\omega_2, \quad \deg\mu_1 \geq \deg\mu_2 + r - s_0.$$

Уравнение (2.3.5.4) с введенными обозначениями эквивалентно пункту 3.

Теорема 3.2.1.1 доказана. □

Далее нам понадобится следующее утверждение.

Лемма 3.2.1.2. *Пусть $Q, F \in K[X]$, многочлен Q неприводим в $K[X]$, $v_Q(F) > 0$, и поле $\mathcal{L} = K(X)(\sqrt{F})$ обладает фундаментальной единицей $\Psi_1 + \Psi_2\sqrt{F}$, где $\Psi_1, \Psi_2 \in K[X]$. Тогда для любой нетривиальной единицы $\Omega_1 + \Omega_2\sqrt{F}$ поля $\mathcal{L}$, где $\Omega_1, \Omega_2 \in K[X]$, справедливы соотношения $v_Q(\Omega_1) = v_Q(\Psi_1) = 0$ и $v_Q(\Omega_2) = v_Q(\Psi_2)$.*

Доказательство. Без ограничения общности можно считать, что для некоторых $n \in \mathbb{N}$ и $c \in K^*$ справедливы тождества

$$\Omega_1 + \Omega_2\sqrt{F} = c(\Psi_1 + \Psi_2\sqrt{F})^n =$$
$$= c\left(\sum_{0\leq j\leq n/2}\binom{n}{2j}\Psi_1^{n-2j}\Psi_2^{2j}F^j\right) + c\left(\sum_{0\leq j<n/2}\binom{n}{2j+1}\Psi_1^{n-2j-1}\Psi_2^{2j+1}F^j\right)\sqrt{F}.$$

Остается заметить, что из условия $v_Q(F) > 0$ следует $v_Q(\Psi_1) = 0$.

Лемма 3.2.1.2 доказана. □

Теорема 3.2.1.3. *Если выполнены условия теоремы 3.2.1.1 и непрерывная дробь элемента $\alpha \in L$ квазипериодическая, то справедливы следующие утверждения:*

1. *если $s \in \mathbb{Z}$ удовлетворяет неравенствам*

$$\deg\lambda_2 - \deg\omega_1 + \deg\omega_2 \leq s \leq \deg\omega_1 - \deg\omega_2 - \deg\lambda_0, \tag{3.2.1.3}$$

   то непрерывные дроби элементов $\alpha \cdot h^s$ и $\overline{\alpha} \cdot h^s$ квазипериодические;

2. *если степень многочлена d нечетная и s не удовлетворяет неравенствам (3.2.1.3), то непрерывные дроби элементов $\alpha \cdot h^s$ и $\overline{\alpha} \cdot h^s$ не квазипериодические.*

Доказательство. 1. Предполагая квазипериодичность непрерывной дроби α, докажем квазипериодичность непрерывных дробей элементов $\alpha \cdot h^s$ и $\overline{\alpha} \cdot h^s$ для всех целых s, удовлетворяющих условию (3.2.1.3).

Разделим промежуток, указанный в (3.2.1.3), на два промежутка (возможно пустых)

$$\deg\lambda_2 - \deg\omega_1 + \deg\omega_2 \leq s \leq 0, \quad 0 \leq s \leq \deg\omega_1 - \deg\omega_2 - \deg\lambda_0. \tag{3.2.1.4}$$

Сначала предположим, что s принадлежит второму промежутку (3.2.1.4). Элементы $\alpha \cdot h^s$ и $\overline{\alpha} \cdot h^s$ являются корнями уравнения

$$\lambda_2 X^2 + 2\lambda_1 h^s X + \lambda_0 h^{2s} = 0 \tag{3.2.1.5}$$

с дискриминантом $d_s = h^{2s} d$, $v_h(d_s) = 2(s_0 + s)$, где $v_h(d) = 2s_0$. Положим

$$r_s = \max(2s + \deg \lambda_0,\ s + \deg \lambda_1,\ \deg \lambda_2), \quad D_s = \frac{d_s}{h^{2r_s}} = \frac{d_0}{h^{2(r_s - s_0 - s)}}.$$

Отметим, что

$$2(r_s - s_0 - s) \geq \deg d_0. \tag{3.2.1.6}$$

Сохраняя обозначения, введенные в доказательстве теоремы 3.2.1.1, имеем $v_X(\Omega_1) = 0$ и $v_X(\Omega_2) = e - \deg \mu_2$, следовательно,

$$\deg \mu_1 - \deg \mu_2 = r - s_0 + v_X(\Omega_2). \tag{3.2.1.7}$$

Из (3.2.1.7), второго неравенства (3.2.1.4) и неравенства $\deg \mu_1 - \deg \mu_2 \geq r - s_0$ из пункта 2 теоремы 3.2.1.1 выводим

$$r_s - s_0 - s = \max(\deg \lambda_0 + s,\ \deg \lambda_1,\ \deg \lambda_2 - s) - s_0 \leq$$

$$\leq \deg \mu_1 - \deg \mu_2 = r - s_0 + v_X(\Omega_2).$$

Обозначим $t = r_s - r - s$, тогда $t \leq v_X(\Omega_2)$. В силу того, что $v_X(D) = 2r - \deg d = 2r - 2s_0 - \deg d_0 \geq 0$, с использованием (3.2.1.6), имеем

$$2t = 2(r_s - s) - 2r \geq \deg d_0 + 2s_0 - 2r = -v_X(D).$$

Таким образом, $-v_X(D) \leq 2t \leq 2v_X(\Omega_2)$ и $v_X(D_s) = 2(r_s - s_0 - s) - \deg d_0 = 2t + v_X(D)$. Так как $t \leq v_X(\Omega_2)$, то $\hat{\Omega}_2 = X^{-t}\Omega_2 \in K[X]$ и справедливо соотношение

$$\Omega_1^2 - D_s \hat{\Omega}_2^2 = \Omega_1^2 - D\Omega_2^2 \in K^*.$$

Отсюда, также, как в доказательстве эквивалентности пунктов 1 и 3 теоремы 3.2.1.1, следует квазипериодичность непрерывных дробей элементов $\alpha \cdot h^s$ и $\overline{\alpha} \cdot h^s$.

Пусть теперь s принадлежит первому промежутку (3.2.1.4). Положим $\xi = -s$, тогда элементы α/h^ξ и $\overline{\alpha}/h^\xi$ являются корнями уравнения

$$\lambda_2 h^{2\xi} X^2 + 2\lambda_1 h^\xi X + \lambda_0 = 0 \tag{3.2.1.8}$$

с дискриминантом $d_\xi = h^{2\xi} d$, $v_h(d_\xi) = 2(s_0 + \xi)$. Положим

$$r_\xi = \max(\deg \lambda_0, \xi + \deg \lambda_1, 2\xi + \deg \lambda_2), \quad D_\xi = \frac{d_\xi}{h^{2r_\xi}} = \frac{d_0}{h^{2(r_\xi - s_0 - \xi)}},$$

причем

$$2(r_\xi - s_0 - \xi) \geq \deg d_0. \tag{3.2.1.9}$$

Из (3.2.1.7), первого неравенства (3.2.1.4) и неравенства $\deg \mu_1 - \deg \mu_2 \geq r - s_0$ из пункта 2

теоремы 3.2.1.1 выводим

$$r_\xi - s_0 - \xi = \max(\deg\lambda_0 - \xi,\ \deg\lambda_1,\ \deg\lambda_2 + \xi) - s_0 \le \deg\mu_1 - \deg\mu_2 = r - s_0 + v_X(\Omega_2).$$

Обозначим $\rho = r_\xi - r - \xi$, тогда $\rho \le v_X(\Omega_2)$. Из (3.2.1.9) имеем

$$2\rho = 2(r_\xi - \xi) - 2r \ge \deg d_0 + 2s_0 - 2r = -v_X(D).$$

Таким образом, $-v_X(D) \le 2\rho \le 2v_X(\Omega_2)$ и $v_X(D_\xi) = 2(r_\xi - s_0 - \xi) - \deg d_0 = 2\rho + v_X(D)$. Так как $\rho \le v_X(\Omega_2)$, то $\tilde\Omega_2 = X^{-\rho}\Omega_2 \in K[X]$ и справедливо соотношение

$$\Omega_1^2 - D_\xi\tilde\Omega_2^2 = \Omega_1^2 - D\Omega_2^2 \in K^*.$$

Отсюда, следует квазипериодичность непрерывных дробей элементов α/h^ξ и $\overline{\alpha}/h^\xi$.

2. Предположим теперь, что $s > \deg\omega_1 - \deg\omega_2 - \deg\lambda_0$ и непрерывная дробь $\alpha\cdot h^s$ или $\overline{\alpha}\cdot h^s$ квазипериодическая. Сохраним обозначения введенные выше. По теореме 2 [118] найдутся элементы $\tilde\Omega_1, \tilde\Omega_2 \in K[X]$ такие, что $\tilde\Omega_1^2 - D_s\tilde\Omega_2^2 \in K^*$, $\tilde\Omega_2 \ne 0$. Аналогично уже проведенным рассуждениям имеем

$$t = r_s - r - s > v_X(\Omega_2), \quad v_X(D_s) = 2t + v_X(D), \quad D_s = X^{2t}D. \tag{3.2.1.10}$$

Элемент $\tilde\Omega_1 + \tilde\Omega_2\sqrt{D_s}$ является нетривиальной единицей в поле $\mathcal{L}$, причем $v_X(\Omega_1) = v_X\left(\tilde\Omega_1\right) = 0$. По лемме 3.2.1.2 в случае нечетной степени $\deg d$ имеем

$$v_X\left(D_s\tilde\Omega_2^2\right) = v_X\left(D\Omega_2^2\right). \tag{3.2.1.11}$$

Из (3.2.1.11) и (3.2.1.10) следует, что $v_X\left(\tilde\Omega_2\right) < 0$, что противоречит $\tilde\Omega_2 \in K[X]$.

Для $s < \deg\lambda_2 - \deg\omega_1 + \deg\omega_2$ доказательство аналогично.

Теорема 3.2.1.3 доказана. □

В пункте 2 теоремы 3.2.1.3 рассматривается только случай, когда степень многочлена f нечетная. Обобщения теоремы 3.2.1.3 на случай четной степени многочлена f будут рассмотрены в теоремах 4.2.2.1 и 4.2.4.1.

Следующие примеры показывают, что, если в пункте 2 теоремы 3.2.1.3 степень $\deg d$ четная, то может существовать целое значение s, не удовлетворяющее неравенствам (3.2.1.3), такое, что непрерывные дроби элементов $\alpha\cdot h^s$ и $\overline{\alpha}\cdot h^s$ квазипериодические.

Пример 3.2.1.4. *Рассмотрим*

$$f = -3h^4 + 12h^3 + 10h^2 + 4h + 1, \quad \alpha = \frac{\sqrt{f}}{h^2} \ -\ \textit{корень}\quad h^4X^2 - f = 0,\ d = h^4 f.$$

Непрерывная дробь α периодическая:

$$\alpha = \left[\frac{1}{h^2}\left(3h^2 + 2h + 1\right);\ \overline{-\frac{1}{6h^2}\left(3h^2 + 2h + 1\right), \frac{2}{h^2}\left(3h^2 + 2h + 1\right)}\right].$$

Фундаментальная S_h-единица поля $L = K(h)(\sqrt{f})$ имеет вид:

$$u = \frac{\mu_1 + \mu_2\sqrt{f}}{h^2} = \frac{3h^2 + 2h + 1 + \sqrt{f}}{h^2}, \quad u \cdot \overline{u} = 12, \quad \deg u = 2.$$

Имеем $s_0 = 2$, $\deg \omega_1 = 4$, $\deg \omega_2 = 0$, $\deg \lambda_2 = \deg \lambda_0 = 4$, следовательно, в (3.2.1.3) подходит только $s = 0$. Однако, элемент $\alpha \cdot h = \sqrt{f}/h$ имеет периодическое разложение в непрерывную дробь:

$$\alpha \cdot h = \left[2 + \tfrac{1}{h};\ \overline{\tfrac{1}{3h}, 3 + \tfrac{3}{2h}, \tfrac{2}{3h}, 1 + \tfrac{1}{2h}, -\tfrac{2}{h} - \tfrac{4h}{3h^2} - \tfrac{2}{3h^3}, 1 + \tfrac{1}{2h}, \tfrac{2}{3h}, 3 + \tfrac{3}{2h}, \tfrac{1}{3h}, 4 + \tfrac{2}{h}}\right].$$

Положим $X = 1/h$, $U = u(1/X)$, $F(X) = X^4 f(1/X)$, тогда U является фундаментальной единицей в поле $\mathcal{L} = K(X)(\sqrt{F})$ и

$$U \cdot \overline{U} = (X^2 + 2X + 3)^2 - F = 12,$$

$$\frac{(U\cdot\overline{U})^2}{144} = \left(-\tfrac{X^4}{6} - \tfrac{2X^3}{3} - \tfrac{5X^2}{3} - 2X - \tfrac{1}{2}\right)^2 - F\left(-\tfrac{X^2}{6} - \tfrac{X}{3} - \tfrac{1}{2}\right)^2 = 1,$$

$$\frac{(U\cdot\overline{U})^3}{144} = \left(-\tfrac{X^6}{3} - 2X^5 - 7X^4 - \tfrac{44X^3}{3} - 18X^2 - 12X\right)^2 -$$

$$-f\left(-\tfrac{X^4}{3} - \tfrac{4X^3}{3} - \tfrac{10X^2}{3} - 4X - 2\right)^2 = 12.$$

Обозначим $U^n = \Omega_1^{(n)} - \Omega_2^{(n)}\sqrt{F}$, тогда видно, что $v_X\left(\Omega_1^{(1)}\right) = v_X\left(\Omega_1^{(2)}\right) = 0$, но $v_X\left(\Omega_1^{(3)}\right) = 1$. Тем самым, при $Q = X$ утверждение леммы 3.2.1.2 с измененным условием $v_Q(F) = 0$ становится уже неверным.

Пример 3.2.1.5. *Рассмотрим*

$$f = -27h^4 + 18h^3 + 31h^2 + 10h + 1, \quad \alpha = \frac{\sqrt{f}}{h^2} \text{ — корень } \quad h^4X^2 - f = 0,\ d = h^4 f.$$

Непрерывная дробь α периодическая:

$$\alpha = \left[3 + \tfrac{5}{h} + \tfrac{1}{h^2};\ \overline{-\tfrac{1}{3} - \tfrac{1}{6h}, 4 + \tfrac{2}{h}, -\tfrac{1}{2} - \tfrac{5}{6h} - \tfrac{1}{6h^2}, 4 + \tfrac{2}{h}, -\tfrac{1}{3} - \tfrac{1}{6h}, 6 + \tfrac{10}{h} + \tfrac{2}{h^2}}\right].$$

Фундаментальная S_h-единица поля $L = K(h)(\sqrt{f})$ имеет вид:

$$u = \tfrac{\mu_1 + \mu_2\sqrt{f}}{h^4} = \tfrac{1}{h^4}\left(\left(12h^4 - \tfrac{22h^3}{3} - 8h^2 - \tfrac{3h}{2} - \tfrac{1}{12}\right) + \left(-\tfrac{h^2}{3} - \tfrac{2h}{3} - \tfrac{1}{12}\right)\sqrt{f}\right).$$

Имеем $u\cdot\overline{u} = 192$, $\deg u = 4$, $s_0 = 2$, $\deg \omega_1 = 6$, $\deg \omega_2 = 2$, $\deg \lambda_2 = \deg \lambda_0 = 4$, следовательно, в (3.2.1.3) подходит только $s = 0$. Однако, элемент $\alpha \cdot h = \sqrt{f}/h$ имеет периодическое разложение в непрерывную дробь:

$$\alpha \cdot h = \left[5 + \tfrac{1}{h};\ \overline{\tfrac{2}{3} + \tfrac{1}{3h}, -\tfrac{3}{2} + \tfrac{1}{h} + \tfrac{1}{2h^2}, -\tfrac{10}{3} - \tfrac{2}{3h}, -\tfrac{1}{2} - \tfrac{1}{2h}, 8 + \tfrac{2}{h}, -\tfrac{1}{6} + \tfrac{1}{6h},}\right.$$
$$\overline{-10 - \tfrac{2}{h}, -\tfrac{1}{24} - \tfrac{1}{12h}, 56 + \tfrac{16}{h}, -\tfrac{1}{16} + \tfrac{1}{32h} + \tfrac{5}{96h^2} + \tfrac{1}{96h^3}, 56 + \tfrac{16}{h}, -\tfrac{1}{24} - \tfrac{1}{12h},}$$
$$\left.\overline{-10 - \tfrac{2}{h}, -\tfrac{1}{6} + \tfrac{1}{6h}, 8 + \tfrac{2}{h}, -\tfrac{1}{2} - \tfrac{1}{2h}, -\tfrac{10}{3} - \tfrac{2}{3h}, -\tfrac{3}{2} + \tfrac{1}{h} + \tfrac{1}{2h^2}, \tfrac{2}{3} + \tfrac{1}{3h}, 10 + \tfrac{2}{h}}\right].$$

Пример 3.2.1.6. *Рассмотрим $f = -h^4 - 57h^3 - \frac{39h^2}{4} + 27h + 9$ и $\alpha = \sqrt{f}/h^2$ — корень уравнения*

$h^4X^2 - f = 0$, $d = h^4 f$. *Непрерывная дробь* α *периодическая:*

$$\alpha = \Big[-15 + \tfrac{9}{2h} + \tfrac{1}{h^2};\ \overline{\tfrac{1}{9} - \tfrac{1}{18h}, 18 + \tfrac{9}{h}, -\tfrac{1}{81} - \tfrac{1}{162h}, -162 + \tfrac{81}{h}, \tfrac{5}{243} - \tfrac{1}{162h} - \tfrac{1}{729h^2}, -162 + \tfrac{81}{h}, -\tfrac{1}{81} - \tfrac{1}{162h}, 18 + \tfrac{9}{h}, \tfrac{1}{9} - \tfrac{1}{18h}, -30 + \tfrac{9}{h} + \tfrac{2}{h^2}}\Big].$$

Фундаментальная S_h*-единица поля* $L = K(h)(\sqrt{f})$ *имеет вид* $u = h^{-6}(\mu_1 + \mu_2\sqrt{f})$, *где*

$$\mu_1 = 27h^6 - \tfrac{405h^5}{2} + \tfrac{351h^4}{2} - \tfrac{81h^3}{4} - \tfrac{45h^2}{4} + \tfrac{9h}{8} + \tfrac{1}{4}, \quad \mu_2 = -9h^4 + 18h^3 - \tfrac{15h^2}{2} + \tfrac{1}{4}.$$

Имеем $u \cdot \overline{u} = 1458$, $\deg u = 6$, $s_0 = 2$, $\deg \omega_1 = 8$, $\deg \omega_2 = 4$, $\deg \lambda_2 = \deg \lambda_0 = 4$, *следовательно, в* (3.2.1.3) *подходит только* $s = 0$. *Однако, элемент* $\alpha \cdot h = \sqrt{f}/h$ *имеет периодическое разложение в непрерывную дробь:*

$$\alpha \cdot h = \Big[\tfrac{9}{2} + \tfrac{1}{h};\ \overline{\tfrac{2}{25} - \tfrac{1}{15h}, -\tfrac{825}{16} + \tfrac{125}{8h}, \tfrac{272}{5625} + \tfrac{32}{5625h}, -\tfrac{16875}{256} + \tfrac{5625}{256h}, \tfrac{256}{5625} - \tfrac{256}{5625h}, \tfrac{5625}{512} + \tfrac{625}{256h}, \tfrac{64}{625} - \tfrac{128}{1875h}, -\tfrac{5625}{64} + \tfrac{625}{32h}, \tfrac{12}{625} + \tfrac{4}{1875h}, -\tfrac{1875}{4} + \tfrac{625}{4h}, \tfrac{4}{625} + \tfrac{2}{375h} - \tfrac{1}{625h^2} - \tfrac{2}{5625h^3}, -\tfrac{1875}{4} + \tfrac{625}{4h}, \tfrac{12}{625} + \tfrac{4}{1875h}, -\tfrac{5625}{64} + \tfrac{625}{32h}, \tfrac{64}{625} - \tfrac{128}{1875h}, \tfrac{5625}{512} + \tfrac{625}{256h}, \tfrac{256}{5625} - \tfrac{256}{5625h}, -\tfrac{16875}{256} + \tfrac{5625}{256h}, \tfrac{272}{5625} + \tfrac{32}{5625h}, -\tfrac{825}{16} + \tfrac{125}{8h}, \tfrac{2}{25} - \tfrac{1}{15h}, 9 + \tfrac{2}{h}}\Big].$$

3.2.2. О решении норменного уравнения

Основные утверждения этого параграфа представлены в статьях [17; 19].

Следующее предложение позволят привести норменное уравнение типа (3.2.1.2) или (2.3.5.4) к более структурированному виду.

Предложение 3.2.2.1. *Пусть многочлен* $d \in K[h]$ *имеет вид*

$$d = h^{2s_0}\omega^2 f, \quad \text{где} \quad \omega \in K[h], \quad v_h(\omega) = 0, \quad \operatorname{lc}(\omega) = 1, \quad s_0 \in \mathbb{Z}, \tag{3.2.2.1}$$

многочлен $f \in K[h]$ *свободен от квадратов.*

1. Существуют многочлены $\omega_1, \omega_2 \in K[h]$, *удовлетворяющие условиям*

$$\omega_1^2 - d\omega_2^2 = bh^m, \ \deg(\omega_1^2) \neq \deg(d\omega_2^2), \ m = \max\left(\deg(\omega_1^2), \ \deg(d\omega_2^2)\right), \ v_h(\omega_2) = 0, \tag{3.2.2.2}$$

для некоторых $b \in K^*$, $m \in \mathbb{N}$, *если и только если найдутся многочлены* $\mu_3, \mu_4 \in K[x]$, *свободные от квадратов многочлены* $f_1, f_2 \in K[x]$ *и* $b_0 \in K^*$ *такие, что*

$$f_2\mu_4^2 - f_1\mu_3^2 = h^{m_1}, \quad m_1 = \deg(f_2\mu_4^2) > \deg(f_1\mu_3^2), \quad \deg f_2 > 0, \tag{3.2.2.3}$$

$$f = b_0^2 f_1 f_2, \quad \operatorname{lc}(f_2) = \operatorname{lc}(\mu_4) = \operatorname{lc}(\mu_3) = 1, \ v_h(f_2) = v_h(\mu_4) = 0, \quad \omega \mid \mu_3\mu_4. \tag{3.2.2.4}$$

2. Существуют многочлены $\omega_1, \omega_2 \in K[h]$, *удовлетворяющие условиям*

$$\omega_1^2 - d\omega_2^2 = bh^m, \quad \deg(\omega_1^2) = \deg(d\omega_2^2) = m, \quad v_h(\omega_2) = 0, \tag{3.2.2.5}$$

для некоторых $b \in K^*$, $m \in \mathbb{N}$, *если и только если найдутся многочлены* $f_2, \mu_3, \mu_4 \in K[x]$ *и*

$f_1 = b_1 \in K^*$, $b_1 \neq 1$, *такие, что*

$$f_2\mu_4^2 - b_1\mu_3^2 = (1-b_1)h^{m_1}, \quad m_1 = \deg(f_2\mu_4^2) = \deg(\mu_3^2), \tag{3.2.2.6}$$

и справедливы условия (3.2.2.4).

Доказательство. Предположим, что многочлены $f_1, f_2, \mu_3, \mu_4 \in K[h]$ удовлетворяют соотношениям (3.2.2.3) и (3.2.2.4). Пусть $s_0 \in \mathbb{Z}$, $s_0 \geq 0$ и $\omega \in K[h]$ — некоторый многочлен такой, что $\omega \mid \mu_3\mu_4$. Тогда одно из возможных решений (3.2.2.2) может быть восстановлено следующим образом:

$$d = 4\omega^2 h^{2s_0} f_1 f_2, \quad \omega_1 = (f_2\mu_4^2 + f_1\mu_3^2)h^{s_0}, \quad \omega_2 = \mu_3\mu_4/\omega, \quad m = 2s_0 + 2m_1. \tag{3.2.2.7}$$

Теперь, пусть $\omega_1, \omega_2 \in K[h]$ удовлетворяют (3.2.2.2) для некоторых $b \in K^*$ и $m \in \mathbb{N}$, причем $m = \deg(d\omega_2^2) > \deg(\omega_1^2)$. Тогда $b = -\operatorname{lc}(d\omega_2^2) = -\operatorname{lc}(f)\operatorname{lc}(\omega_2)^2$. Положим $f_2 = f/\operatorname{lc}(f)$, $\mu_4 = \omega_2\omega/\operatorname{lc}(\omega_2)$, $f_1 = -\operatorname{lc}(\omega_1)^2/b \in K^*$, $\mu_3 = h^{-s_0}\omega_1/\operatorname{lc}(\omega_1)$. Тогда $b_0 = \operatorname{lc}(f)\operatorname{lc}(\omega_2)/\operatorname{lc}(\omega_1)$, $m_1 + 2s_0 = m$ и справедливы условия (3.2.2.3) и (3.2.2.4).

Далее, предположим, что справедливо тождество (3.2.2.2) и $\deg(\omega_1^2) > \deg(d\omega_2^2)$. В этом случае $m = 2s_0 + 2m_1$ и $b = b_1^2$, $b_1 \in K^*$. Запишем разность квадратов

$$\left(\frac{\omega_1}{b_1 h^{s_0}} - h^{m_1}\right)\left(\frac{\omega_1}{b_1 h^{s_0}} + h^{m_1}\right) = \frac{d\omega_2^2}{bh^{2s_0}}.$$

$$\text{Обозначим} \quad R^{\pm} = \frac{\omega_1}{b_1 h^{s_0}} \pm h^{m_1}, \quad f_2\mu_4^2 = \frac{R^+}{\operatorname{lc}(R^+)}, \quad f_1\mu_3^2 = \operatorname{lc}\left(R^+\right) R^-,$$

причем $f_1, f_2, \mu_3, \mu_4 \in K[h]$, $b_0 = \operatorname{lc}(\omega_1)/\operatorname{lc}(\omega_2)$, $\operatorname{lc}(f_2) = \operatorname{lc}(\mu_4) = \operatorname{lc}(\mu_3) = 1$, $v_h(f_2) = v_h(\mu_4) = 0$, и многочлен $f = b_0^2 f_1 f_2$ свободен от квадратов. Без ограничения общности мы считаем, что $\deg R^+ > \deg R^-$ (иначе поменяем местами R^+ и R^-), поэтому $\deg(f_1\mu_3^2) < \deg(f_2\mu_4^2) = \deg m_1$. Если $\deg f_2 = 0$, то тождество (3.2.2.3) имеет вид (3.2.2.2), с которого мы стартовали. Поэтому, положив $m_1 = 2m_2$, можно снова записать разность квадратов $(\mu_4 - h^{m_2})(\mu_4 - h^{m_2}) = b_0^2 f \mu_3^2$ и продолжить те же рассуждения, пока не придем к равенству вида (3.2.2.3) с $\deg f_2 > 0$.

Эквивалентность разрешимости уравнений (3.2.2.5) и (3.2.2.6) с условиями (3.2.2.4) доказывается аналогично.

Предложение 3.2.2.1 доказано. □

Предложение 3.2.2.2. *Пусть α является корнем* (3.2.1.1) *с дискриминантом* (3.2.2.1). *Пусть $r = \max(\deg\lambda_0, \deg\lambda_1, \deg\lambda_2)$. Непрерывная дробь элемента α квазипериодическая тогда и только тогда, когда существует решение* (3.2.2.3) *с условиями* (3.2.2.4) *и*

$$\deg f_2 + \deg\mu_4 - \deg\mu_3 \geq r - s_0. \tag{3.2.2.8}$$

Доказательство. Доказательство следует из теоремы 3.2.1.1 и предложения 3.2.2.1. □

3.2.3. О периодичности непрерывных дробей ключевых элементов

В статье [166] доказано, что для свободных от квадратов многочленов $f \in K[h]$ нечетной степени квазипериодичность разложения $\sqrt{f}/h^{s_0}$, $0 < s_0 < \deg f$, в непрерывную дробь влечет его периодичность. В статьях [141; 142] это утверждение доказано для $s \in \mathbb{Z}$. В этом параграфе мы предлагаем более короткое доказательство этого факта (см. дополнительно [3; 13]).

Пусть K — произвольное поле характеристики отличной от 2. Пусть $f \in K[x]$ — свободный от квадратов многочлен степени $2g+2$, $g \geq 1$, со старшим коэффициентом, являющимся полным квадратом в мультипликативной группе K^* поля K. Рассмотрим $\mathcal{L} = K(x)(\sqrt{f})$ — гиперэллиптическое поле. В статье [118] определено отношение эквивалентности "$\approx$" для элементов $\alpha, \beta \in \mathcal{L} \setminus K(x)$, а именно $\alpha \approx \beta$, если найдутся $T, R, U, V \in K[x]$ такие, что

$$\alpha = \frac{T + R\beta}{U + V\beta}, \quad TV - RU \in K^*.$$

В частности, легко проверить, что $\alpha \approx 1/\alpha$. В теореме 1 [118] доказано, что $\alpha \approx \beta$ для $\alpha, \beta \in \mathcal{L} \setminus K(x)$ тогда и только тогда, когда $\beta_m = c\alpha_n$ для некоторых $m, n \in \mathbb{N}_0$, $c \in K^*$. Отсюда следует, что непрерывные дроби элементов $\alpha \approx \beta$ одновременно квазипериодические (периодические) или не квазипериодические (не периодические).

Лемма 3.2.3.1. *Пусть в гиперэллиптическом поле $\mathcal{L} = K(x)(\sqrt{f})$ есть фундаментальная единица $\Omega_1 + \Omega_2\sqrt{f}$, где $\Omega_1, \Omega_2 \in K[x]$, $\Omega_2 \neq 0$. Тогда существуют такие многочлены $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$, что $\deg \Omega_3 \leq \deg \Omega_1$, $v_x(\Omega_3) = \max\{v_x(\Omega_1), v_x(\Omega_2)\}$ и для некоторого $b \in K^*$ справедливы условия*

$$f_2\Omega_4^2 - f_1\Omega_3^2 = 1, \quad f_1 \cdot f_2 = b^2 f, \quad \deg f_2 > 0, \quad v_x(f_2) = v_x(\Omega_4) = 0, \tag{3.2.3.1}$$

причем в случае $v_x(\Omega_2^2 f) > 0$ имеем $\deg f_1 > 0$.

Обратно, если даны многочлены $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$, удовлетворяющие условиям (3.2.3.1), то в поле $\mathcal{L} = K(x)(\sqrt{f})$ есть фундаментальная единица $\Omega_1 + \Omega_2\sqrt{f}$, причем $\deg \Omega_1 \leq \deg \Omega_3^2 f_1$.

Доказательство. Справедливо соотношение $\Omega_1^2 - \Omega_2^2 f = \gamma \in K^*$. В случае, если $v_x(\Omega_2^2 f) = 0$ в качестве многочленов $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$ можно взять

$$f_1 = -1/\gamma, \quad f_2 = -f/\gamma, \quad \Omega_3 = \Omega_1, \quad \Omega_4 = \Omega_2, \tag{3.2.3.2}$$

тогда $b = -1/\gamma$ и справедливы условия (3.2.3.1) и другие условия леммы.

Пусть теперь $v_x(\Omega_2^2 f) > 0$, тогда $\gamma = b^{-2}$ для некоторого $b \in K^*$. Выберем знак у постоянной b так, что

$$b^2\Omega_2^2 f = b^2\Omega_1^2 - 1 = \big(b\Omega_1 - 1\big)\big(b\Omega_1 + 1\big), \quad v_x(b\Omega_1 - 1) > 0.$$

Поскольку $\left(b\Omega_1 - 1,\ b\Omega_1 + 1\right) \in K^*$, то существуют многочлены $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$, удовлетворяющие условиям

$$b\Omega_1 - 1 = 2\Omega_3^2 f_1, \quad b\Omega_1 + 1 = 2\Omega_4^2 f_2, \quad \Omega_2 = 2\Omega_3\Omega_4, \quad b^2 f = f_1 f_2. \tag{3.2.3.3}$$

Для таких многочленов справедливы условия (3.2.3.1) и условия леммы, причем $\deg f_1 > 0$ и $\deg f_2 > 0$, поскольку в противном случае фундаментальная единица имела бы вид $\Omega_3 + \Omega_4\sqrt{f_2/f_1}$ или $\Omega_4 + \Omega_3\sqrt{f_1/f_2}$ соответственно.

Обратное утверждение следует из формул (3.2.3.2) или (3.2.3.3) соответственно при $\deg f_1 = 0$ или $\deg f_1 > 0$. □

Как известно еще по работам Абеля и Чебышева, условие периодичности непрерывной дроби элемента $\sqrt{f}$, построенной в поле $K((1/x))$, эквивалентно разрешимости функционального уравнения Пелля. В наших обозначениях разрешимость уравнения Пелля эквивалентна существованию многочленов $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$, удовлетворяющих (3.2.3.1).

Следующая лемма обобщает лемму 1 [13].

Лемма 3.2.3.2. *Пусть многочлены $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$ удовлетворяют (3.2.3.1) и $s \in \mathbb{Z}$. Если $-v_x(f_1) - v_x(\Omega_3) \le s \le v_x(\Omega_3)$, то*

$$\frac{1}{x^s\sqrt{f}} \approx x^s\sqrt{f} \approx x^s\sqrt{\frac{f_1}{f_2}} \approx x^{-s}\sqrt{\frac{f_2}{f_1}}, \tag{3.2.3.4}$$

а если $-v_x(\Omega_3) \le s \le v_x(\Omega_3) + v_x(f_1)$, то

$$\frac{x^s}{\sqrt{f}} \approx \frac{\sqrt{f}}{x^s} \approx x^{-s}\sqrt{\frac{f_1}{f_2}} \approx x^s\sqrt{\frac{f_2}{f_1}}. \tag{3.2.3.5}$$

Доказательство. Замена s на $-s$ превращает (3.2.3.4) в (3.2.3.5). Кроме того, поскольку $\alpha \approx 1/\alpha$, то достаточно доказать только соотношение $x^{-s}\sqrt{f} \approx x^{-s}\sqrt{f_1/f_2}$ для $-v_x(\Omega_3) \le s \le v_x(\Omega_3) + v_x(f_1)$.

Рассмотрим $T = x^{-s}\Omega_3 f_1$, $R = \Omega_4$, $U = \Omega_4 f_2$, $V = x^s\Omega_3$, тогда из (3.2.3.1) имеем

$$TV - RU = -(f_2\Omega_4^2 - f_1\Omega_3^2) \in K^*, \quad T, R, U, V \in K[x],$$

$$\frac{\sqrt{f}}{x^s} \approx \frac{T + R\sqrt{f}/x^s}{U + V\sqrt{f}/x^s} = x^{-s}\sqrt{\frac{f_1}{f_2}}.$$

Лемма 3.2.3.2 доказана. □

Теорема 3.2.3.3. *Пусть многочлены $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$ удовлетворяют (3.2.3.1) и $s \in \mathbb{Z}$. Если $-v_x(f_1) - v_x(\Omega_3) \le s \le v_x(\Omega_3)$, то непрерывные дроби элементов из (3.2.3.4) периодические, а если $-v_x(\Omega_3) \le s \le v_x(\Omega_3) + v_x(f_1)$, то непрерывные дроби элементов из (3.2.3.5) периодические.*

Доказательство. Поскольку f свободен от квадратов, то $0 \le v_x(f) \le 1$. В силу того, что $\deg_x f_2 > 0$, имеем

$$\min\left(v_\infty\left(x^{-s}/\sqrt{f}\right),\ v_\infty\left(x^s\sqrt{f}\right),\ v_\infty\left(x^s\sqrt{f_1/f_2}\right),\ v_\infty\left(x^{-s}\sqrt{f_2/f_1}\right)\right) < 0,$$
$$\min\left(v_\infty\left(x^{s}/\sqrt{f}\right),\ v_\infty\left(x^{-s}\sqrt{f}\right),\ v_\infty\left(x^{-s}\sqrt{f_1/f_2}\right),\ v_\infty\left(x^{s}\sqrt{f_2/f_1}\right)\right) < 0.$$

У всех этих элементов один и тот же дискриминант D, причем при $v_x(f) = 0$ или $s = 0$ имеем $D = x^{2|s|}f$, а при $v_x(f) = 1$ и $s \neq 0$ имеем $D = x^{2|s|-2}f$. Следовательно, по теореме 2 [118] получаем, что непрерывные дроби элементов $x^s\sqrt{f}$ и $x^{-s}\sqrt{f}$ квазипериодические. Наконец, по теореме 3 [118] и лемме 3.2.3.2 получаем периодичность непрерывных дробей всех элементов из (3.2.3.4) и (3.2.3.5) соответственно.

Теорема 3.2.3.3 доказана. □

Таким образом, в теореме 3.2.3.3 доказано, что квазипериодичность непрерывной дроби хотя бы одного элемента из (3.2.3.4) или (3.2.3.5) влечет периодичность непрерывных дробей всех элементов из (3.2.3.4) или (3.2.3.5) соответственно. В частности, из квазипериодичности непрерывных дробей вида $\sqrt{f}/x^s$ следует их периодичность (см. [166] и [142]).

Следующее предложение дает необходимые и достаточные условия для поиска свободных от квадратов многочленов $f \in K[h]$, имеющих периодическое разложение $\sqrt{f}$ в непрерывную дробь.

Предложение 3.2.3.4. *Свободный от квадратов многочлен $f \in K[h]$ имеет периодическое разложение $\sqrt{f}$ в непрерывную дробь в поле $K((h))$ тогда и только тогда, когда найдутся многочлены $\mu_3, \mu_4 \in K[x]$ и свободные от квадратов многочлены $f_1, f_2 \in K[x]$, удовлетворяющие соотношениям (3.2.2.3), (3.2.2.4) и*

$$\deg \mu_4 \ge \deg f_1 + \deg \mu_3. \tag{3.2.3.6}$$

Доказательство. Доказательство следует из предложения 3.2.2.2. □

Приведем пример многочлена f и связанных с ним квадратичных иррациональностей, имеющих квазипериодическое разложение в непрерывную дробь для различных значений параметров r и s_0, включая случай $r = g + 1$, $s_0 = 0$ (см. предложение 3.2.2.2).

Пример 3.2.3.5. *Рассмотрим решение уравнения (3.2.2.3):*

$$g = 2,\ m_1 = 4, \quad \mu_3 = \mu_4 = 1,\ f_1 = bh + c,\ f_2 = h^4 + bh + c, \quad b, c \in K^*,$$

тогда

$$f = (bh + c)(h^4 + bh + c), \quad \mu_1 = h^4 + 2(bh + c), \quad \mu_2 = 2.$$

Остается выбрать подходящим образом параметры r и s_0, чтобы были выполнены условия предложения 3.2.2.2.

Для $r = 6$, $s_0 = 3$ *рассмотрим* $\beta_1 = \sqrt{f}/h^3$ *— корень уравнения* $h^6X^2 - f = 0$. *Непрерывная дробь* β_1 *имеет вид*

$$\frac{\sqrt{f}}{h^3} = \left[\frac{b}{h^2} + \frac{c}{h^3}; \overline{\frac{2}{h}, \frac{2b}{h^2} + \frac{2c}{h^3}}\right].$$

Для $r = 5$, $s_0 = 2$ *рассмотрим* $\beta_2 = \sqrt{f}/h^2$ *— корень уравнения* $h^4X^2 - f = 0$. *Непрерывная дробь* β_2 *имеет вид*

$$\frac{\sqrt{f}}{h^2} = \left[\frac{b}{h} + \frac{c}{h^2}; \overline{\frac{2}{h^2}, \frac{2b}{h} + \frac{2c}{h^2}}\right].$$

Для $r = 4$, $s_0 = 1$ *рассмотрим* $\beta_3 = \sqrt{f}/(h \cdot f_1)$ *— корень уравнения* $h^2f_1X^2 - f_2 = 0$ *или* $\beta_4 = h\sqrt{f}/f_2$ *— корень уравнения* $f_2X^2 - h^2f_1 = 0$. *Непрерывные дроби* β_3 *и* β_4 *имеют вид*

$$\frac{\sqrt{f}}{h \cdot f_1} = \left[\frac{1}{h}; \overline{\frac{2b}{h^2} + \frac{2c}{h^3}, \frac{2}{h}}\right], \quad \frac{h\sqrt{f}}{f_2} = \left[0; \frac{1}{h}, \overline{\frac{2b}{h^2} + \frac{2c}{h^3}, \frac{2}{h}}\right].$$

Для $r = 3$, $s_0 = 0$ *положим*

$$\lambda_0 = h^3 - 2h^2 - \frac{h}{4} + \frac{3}{4}, \quad \lambda_1 = h^3 - \frac{h^2}{2} - \frac{5h}{4} + \frac{3}{4}, \quad \lambda_2 = h^3 - h.$$

Тогда при $b = 9/16$, $c = -9/16$ *имеем*

$$d = \lambda_1^2 - \lambda_0\lambda_2 = d_0 = \frac{16}{9}f = h^5 - h^4 + \frac{9h^2}{16} - \frac{9h}{8} + \frac{9}{16}.$$

Непрерывная дробь элемента

$$\beta_5 = \frac{-\lambda_1 + \sqrt{d}}{\lambda_2} = \frac{-4h^3 + 2h^2 + 5h - 3 + \sqrt{16h^5 - 16h^4 + 9h^2 - 18h + 9}}{4h^3 - 4h}$$

имеет квазипериодический, но не периодический вид

$$\beta_5 = \left[0; -2 + \frac{3}{2h}, \overline{1 + \frac{1}{h}, -3 + \frac{3}{2h}, \frac{1}{2} + \frac{1}{2h}, -6 + \frac{6}{h}}^{1/4}\right] =$$

$$= \left[0; -2 + \frac{3}{2h}, 1 + \frac{1}{h}, -3 + \frac{3}{2h}, \frac{1}{2} + \frac{1}{2h}, -6 + \frac{6}{h}, \frac{1}{4} + \frac{1}{4h}, -12 + \frac{6}{h}, \frac{1}{8} + \frac{1}{8h}, -24 + \frac{24}{h}, \ldots\right].$$

3.2.4. Алгоритм поиска квазипериодических непрерывных дробей

Далее мы предлагаем алгоритм для численного решения задачи сформулированной в (3.2.2.3)-(3.2.2.4) с полем констант $K = \mathbb{Q}$. Схема алгоритма выглядит следующим образом.

В качестве множеств $\mathcal{M}_1, \mathcal{M}_2$ удобно взять заранее сформированный массив дробей, например, дробей Фарея. Кроме того, подходящей заменой $h := ch$ для некоторой постоянной $c \in K^*$ мы можем зафиксировать один из коэффициентов многочлена f_2.

Сложность каждой итерации алгоритма 3 фактически определяется сложностью разложения (3.2.4.2). Для ускорения имеет смысл дополнительно проверять наличие кратных корней у многочлена E. Для этого можно вычислить дискриминант многочлена E или степень наибольшего общего делителя (E, E'), где E' — производная многочлена E. Если кратных корней

Алгоритм 3. Алгоритм решения задачи (3.2.2.3)-(3.2.2.4) при $K = \mathbb{Q}$.

1: **Дано:** $\mathcal{M}_1, \mathcal{M}_2,\ Q, R,\ r_1$. Здесь $\mathcal{M}_1, \mathcal{M}_2 \subset \mathbb{Q}$ — два конечных множества для организации перебора значений свободных коэффициентов многочленов f_2 и μ_4; $Q, R \in \mathbb{N}$ — верхние границы для $\deg f_2$ и $\deg \mu_4$; $r_1 \in \mathbb{Z}$, $0 \leq r_1 \leq R$ — количество старших коэффициентов многочлена $\deg \mu_4$, однозначно определяемых по данному многочлену f_2 так, что $\deg(f_2\mu_4^2 - h^{m_1}) \leq m_1 - r_1$. Положим $q = 0$, $r_2 = 0$.

2: **Определить:** многочлен $f_2 \in \mathbb{Q}[x]$, $f_2 = h^q + b_1 h^{q-1} + \ldots + b_q$, $b_0 = 1$, $b_q \neq 0$, где набор коэффициентов $(b_1, \ldots, b_q) \in \mathcal{M}_1^q$ по очереди пробегает все возможные значения;

3: **вычислить:** старшие r_1 коэффициентов $c_0 = 1, c_1, \ldots, c_{r_1-1}$ многочлена μ_4 из соотношений, уравнивающих коэффициенты при h^{m_1-j}, $j = 1, 2, \ldots, r_1$, в формуле (3.2.2.3) так, чтобы в итоге выполнялось неравенство $\deg(f_2\mu_4^2) - \deg(f_1\mu_3^2) \geq r_1$:

$$c_j = -\frac{1}{2}\left(S'_j + \sum_{k=1}^{q} b_k \cdot S_{j-k}\right), \quad \text{где} \quad S_n = \sum_{j=0}^{n} c_j c_{n-j},\ S'_n = \sum_{j=1}^{n-1} c_j c_{n-j}; \tag{3.2.4.1}$$

4: **вычислить:** $\mu_4 = h^t + c_1 h^{t-1} + \ldots + c_t$, $t \leq r_1 + r_2 - 1$, $c_t \neq 0$, где $(c_{r_1}, \ldots, c_{r_1+r_2-1}) \in \mathcal{M}_2^{r_2}$ по очереди перебегают все возможные значения (отбросить последние нулевые коэффициенты, если такие есть);

5: **вычислить:** $m_1 = \deg f_2 + 2\deg \mu_4 = q + 2t \in \mathbb{N}$ и $E = f_2\mu_4^2 - h^{m_1} \in \mathbb{Q}[x]$, причем $\deg E \leq m_1 - r_1$;

6: **вычислить:** представление

$$E = f_1\mu_3^2, \quad \text{где } \operatorname{lc}(\mu_3) = 1,\ f_1 - \text{ свободный от квадратов;} \tag{3.2.4.2}$$

7: **вычислить:** представление $d_0 = f\omega^2$, как в (3.2.4.2), где $d_0 = 4f_1f_2$, $\operatorname{lc}(\omega) = 1$, f — свободный от квадратов многочлен;

8: **если** $r_1 + r_2 < R$, **то** увеличить r_2 на 1 и перейти к шагу 4.; **иначе, если** $q < Q$, **то** увеличить q на 1, положить $r_2 = 0$ и перейти к шагу 2.; **иначе, если** $r_1 + r_2 = R$ и $q = Q$, **то** завершить алгоритм.

9: **Вернуть**: числа m_0, $r_0 = m_1 - \deg E > 0$, многочлены f, $\mu_1 = f_2\mu_4^2 + f_1\mu_3^2$, и $\mu_2 = \omega\mu_3\mu_4$, необходимые для построения S_h-единицы $h^{-m_1}(\mu_1 + \mu_2\sqrt{f})$;

нет, то $\deg \mu_3 = 0$, а этот случай может быть разобран отдельно.

Можно воспользоваться следующим алгоритмом для быстрого вычисления представления (3.2.4.2).

Алгоритм 4. Алгоритм выделения свободной от квадратов части многочлена.

1: **Дано:** многочлен E.
2: **Положить:** $L = 1$, $M = 1$;
3: **До тех пор, пока** $\deg E > 0$, **выполнить:**
4: **вычислить:** многочлен B, являющийся свободной от квадратов частью многочлена E: $R = (E,\ E')$, $B = E/R$, где наибольший общий делитель многочлена и его производной $(E,\ E')$ вычисляем по алгоритму Евклида;
5: **вычислить:** $C = (R,\ B)$, $E = R/C$, $G = B/C$, $L := L \cdot G$, $M := M \cdot C$.
6: **Конец цикла**
7: **Вернуть**: $f_1 = E \cdot L$, $\mu_3 = M$.

Также можно изначально выбирать только свободные от квадратов многочлены f_2.

В алгоритме 3 сначала задается многочлен f_2, а потом восстанавливается подходящим образом многочлен μ_4. Алгоритм 3 может быть легко изменен так, чтобы сначала задавался бы многочлен μ_4, а по нему уже восстанавливался бы многочлен f_2. Также ясно, что алгоритм 3 может быть незначительно изменен для численного решения задачи, сформулированной в (3.2.2.2) при условиях $m_1 = \deg(f_2\mu_4^2) = \deg(\mu_3^2)$.

Пусть $u = h^{-m_1}(\mu_1 + \mu_2\sqrt{f})$ — S_h-единица в поле $L = \mathbb{Q}(h)(\sqrt{f})$, где $\mu_1, \mu_2 \in \mathbb{Q}[h]$ и $\operatorname{lc}(\mu_1) = \operatorname{lc}(\mu_2) = 1$. Если $\deg(\mu_1^2) \neq \deg(f\mu_2^2)$, то при правильном подборе множеств $\mathcal{M}_1, \mathcal{M}_2 \subset K$ и параметров $Q, R, r_0 \in \mathbb{Z}$ данная S_h-единица u будет найдена с помощью приведенного алгоритма 3.

Пример 3.2.4.1. *В ходе работы алгоритма 3 найдены следующие многочлены*

$$f_2 = h^2 + 2h + 3, \quad \mu_4 = h^5 - h^4 + 2h^2 - \tfrac{7h}{2} + \tfrac{3}{2}, \quad f_1 = -12h^4 - 16h + 12, \quad \mu_3 = h - \tfrac{3}{4}.$$

По формулам (3.2.2.7) восстанавливаем

$$\mu_1 = h^{12} - 24h^6 + 36h^5 - \frac{27h^4}{2} - 32h^3 + 72h^2 - 54h + \frac{27}{2},$$

$$\mu_2 = 2h^6 - \frac{7h^5}{2} + \frac{3h^4}{2} + 4h^3 - 10h^2 + \frac{33h}{4} - \frac{9}{4},$$

$$f = 4\left(h^2 + 2h + 3\right)\left(-3h^4 - 4h + 3\right) = -12h^6 - 24h^5 - 36h^4 - 16h^3 - 20h^2 - 24h + 36.$$

Имеем соотношения

$$6 = \deg \mu_1 - \deg \mu_2 \geq \deg d_0 = \deg f = 2g + 2 = 6,$$

поэтому справедливы условия такие же, как в предложении 3.2.3.4, необходимые для пери-

одичности непрерывной дроби $\sqrt{f}$. *Непрерывная дробь* $\sqrt{f}$ *имеет вид*

$$\sqrt{f} = \Big[6; \tfrac{1}{2} - \tfrac{1}{2h}, \overline{2 + \tfrac{2}{h} + \tfrac{2}{h^2}, -\tfrac{1}{6} + \tfrac{1}{4h}, -30 + \tfrac{18}{h}, \tfrac{1}{9} + \tfrac{1}{9h} + \tfrac{1}{9h^2}, -30 + \tfrac{18}{h}, -\tfrac{1}{6} + \tfrac{1}{4h}, 2 + \tfrac{2}{h} + \tfrac{2}{h^2}, \tfrac{7}{12} - \tfrac{1}{2h}, -84 + \tfrac{72}{h}, -\tfrac{1}{72} - \tfrac{1}{72h} - \tfrac{1}{72h^2}, 24 - \tfrac{36}{h}, \tfrac{5}{24} - \tfrac{1}{8h}, -16 - \tfrac{16}{h} - \tfrac{16}{h^2}, \tfrac{5}{24} - \tfrac{1}{8h}, 24 - \tfrac{36}{h}, -\tfrac{1}{72} - \tfrac{1}{72h} - \tfrac{1}{72h^2}, -84 + \tfrac{72}{h}, \tfrac{7}{12} - \tfrac{1}{2h}}\Big].$$

Длина квазипериода равна 9, *коэффициент квазипериода* $c = -1/144$, *длина периода равна* 18. *Непрерывная дробь* $\sqrt{f}/h^3$ *имеет вид*

$$\tfrac{\sqrt{f}}{h^3} = \Big[-2 - \tfrac{2}{h} - \tfrac{2}{h^2} + \tfrac{6}{h^3}; \overline{\tfrac{1}{4} - \tfrac{1}{4h}, -4 - \tfrac{4}{h} - \tfrac{4}{h^2} + \tfrac{12}{h^3}}\Big].$$

Длина квазипериода совпадает с длиной периода и равна 2. *Фундаментальная* S_h*-единица и имеет вид*

$$u = \frac{1}{h^4}\left(\frac{h^4}{2} + 2h - \frac{3}{2} + \left(\frac{h}{4} - \frac{1}{4}\right)\sqrt{f}\right), \quad u \cdot \overline{u} = 1,$$

степень фундаментальной S_h*-единицы и равна* 4.

Пример 3.2.4.1 показывает, что по виду периодической непрерывной дроби $\sqrt{f}$ невозможно восстановить степень фундаментальной S_h-единицы u поля $L = \mathbb{Q}(h)(\sqrt{f})$, однако $\deg u$ можно восстановить по виду непрерывной дроби элемента $\sqrt{f}/h^{g+1}$ (см. [20]). Также пример 3.2.4.1 показывает, что при четной степени многочлена f с периодическим разложением $\sqrt{f}$ в непрерывную дробь длина периода $\sqrt{f}$ может быть значительно больше длины периода $\sqrt{f}/h^{g+1}$. В разделе 3.3 будет подробно изучен вопрос о возможных значениях длины квазипериода и периода функциональных непрерывных дробей. В частности будут даны оценки на длину периода для "ключевых" элементов вида $\sqrt{f}/h^s$, $s \in \mathbb{Z}$.

3.2.5. Пример непрерывной дроби с несимметричным периодом

Следующий пример является интересным сразу с нескольких сторон.

Во-первых, пример 3.2.5.1 иллюстрирует понятия обобщенных многочленов Мамфорда и обобщенного якобиана особой кривой. Данные понятия рассмотрены, например, в статье [167].

Во-вторых, в примере 3.2.5.1 построено поле $L = \mathbb{Q}(x)(\sqrt{f})$ и найден в нем элемент α, обладающий разложением в непрерывную дробь с достаточно большим периодом по сравнению со степенью фундаментальной S_h-единицы в поле L. Более точно, длины периодов непрерывных дробей элементов $\sqrt{f}/h^s$, $0 \le s \le 4$, совпадают и равны 2, а длина периода непрерывной дроби α равна $18 = 2 \times 3 \times 6$, в то время, как степень фундаментальной S_h-единицы в поле L равна 3, и подгруппа кручения в якобиане кривой $C : y^2 = f(x)$ имеет вид $\mathbb{Z}_3$. Отметим, что далее в теореме 3.3.3.4 будет доказано, что длины периодов элементов вида $\sqrt{f}/h^s$ не превосходят $6m$, где m — порядок группы кручения.

Наконец, в-третьих, непрерывная дробь $\alpha \in L$ имеет несимметричный вид, и период не может быть приведен к симметричному виду циклическими сдвигами. Ранее нам не встречались в литературе примеры таких непрерывных дробей элементов поля L. Это также отличает элемент α от элементов вида $\sqrt{f}/h^s$, для которых период обязательно должен быть симметричным с точностью до сдвига.

Пример 3.2.5.1. *Рассмотрим уравнение* $\lambda_2 X^2 + 2\lambda_1 X + \lambda_0 = 0$, *где*

$$\lambda_0 = -t_3^2 h^3 \left(t_1 - t_2 t_3 - 1\right)\left(t_1 - t_2 t_3 + 1\right) +$$
$$+ t_3 h^2 \left(t_1^2 t_3 - 2t_1^2 - 2t_1 t_2 t_3^2 + 4t_1 t_2 t_3 + 2t_2^2 t_3^3 - 2t_2^2 t_3^2 - t_3 + 2\right) +$$
$$+ h\left(2t_1^2 t_3 - t_1^2 + 2t_1 t_2 t_3^3 - 4t_1 t_2 t_3^2 + 2t_1 t_2 t_3 - t_2^2 t_3^4 + 2t_2^2 t_3^3 - t_2^2 t_3^2 - 2t_3 + 1\right) +$$
$$+ \left(t_1 + t_2 t_3^2 - t_2 t_3 - 1\right)\left(t_1 + t_2 t_3^2 - t_2 t_3 + 1\right),$$
$$\lambda_1 = t_1 t_3 h + t_1 + t_2 t_3^2 h^2 + t_2 t_3^2 - t_2 t_3, \quad \lambda_2 = h^2 + h + 1.$$

Тогда дискриминант этого уравнения имеет вид

$$D = \left(t_3 h + 1\right)^2 \left(h^3 (t_1 - t_2 t_3 - 1)(t_1 - t_2 t_3 + 1) + 1\right).$$

Обозначим $c = (t_1 - t_2 t_3)^2 - 1$, $f = ch^3 + 1$. *В поле* $L = \mathbb{Q}(x)(\sqrt{f})$ *существует* $u = u^{(1)} = (ch^3 + 2 + 2\sqrt{f})/(2h^3)$ — *фундаментальная* S_h*-единица, где* $S_h = \{v_h^-, v_h^+\}$. *Пусть* $u^n = u^{(n)} = (\mu_1^{(n)} + \mu_2^{(n)}\sqrt{f})/h^{3n}$. *Тогда*

$$\mu_2^{(6)} = \frac{2}{c^3 h^7}(ch^3 + 4)(3ch^3 + 4).$$

Мы хотим, чтобы норменное уравнение для $u^{(6)}$ *имело вид*

$$\left(\left(\mu_1^{(6)}\right)^2 - \left(\tilde{\mu}_2^{(6)}\right)^2 D\right)\frac{1}{h^{18}} = 1, \quad \mu_2^{(6)} = (t_3 h + 1)\tilde{\mu}_2^{(6)}.$$

Для этого найдем такие t_1, t_2, t_3, *что* $(t_3 h + 1) \mid (3ch^3 + 4)$. *Последнее условие равносильно уравнению*

$$3\left((t_1 - t_2 t_3)^2 - 1\right) - 4t_3^3 = 0.$$

Кривая $C:\ y^2 = 12x^3 + 9$ *содержит рациональные точки, например:*

$$(-2 : 21 : 3),\ (3 : 60 : 4),\ (6 : 51 : 1),\ (340 : 271173 : 147),$$
$$(-357 : 109560 : 400),\ (420 : 565437 : 289).$$

Следовательно, можно положить, например, $t_1 = 17 + 6t$, $t_2 = t$, $t_3 = 6$, *тогда*

$$\lambda_0 = -10368h^3 + 432h^2\left(3t^2 + 16\right) + 144h\left(9t^2 + 51t + 22\right) + (9t + 4)(144t + 72),$$
$$\lambda_1 = 36h^2 t + 6h(6t + 17) + 36t + 17,$$
$$\lambda_2 = h^2 + h + 1,$$
$$D = (6h + 1)^2\left(288h^3 + 1\right), \quad f = 288h^3 + 1.$$

Непрерывная дробь элемента

$$\alpha = (-\lambda_1 + \sqrt{D})/\lambda_2 = \frac{-(36h^2t + 6h\,(6t+17) + 36t + 17) + (6h+1)\sqrt{288h^3+1}}{h^2+h+1}$$

имеет вид

$$\alpha = \Big[-4\,(9t+4)\,;\, \tfrac{1}{h}\left(-\tfrac{3h}{200} - \tfrac{1}{80}\right),\, \overline{\tfrac{1}{h}\left(\tfrac{42400h}{361} - \tfrac{500}{19}\right),\, \tfrac{1}{h}\left(-\tfrac{2527h}{2535000} - \tfrac{6859}{2340000}\right),\, \tfrac{1}{h}\left(\tfrac{544180000h}{1172889} + \tfrac{21970000}{390963}\right),\, \tfrac{1}{h}\left(-\tfrac{245133801h}{120099005000} + \tfrac{3518667}{16565380000}\right),\, \tfrac{1}{h}\left(-\tfrac{8454969952h}{31668003} + \tfrac{69657422900}{95004009}\right),\, \tfrac{1}{h}\left(-\tfrac{4042948383h}{161605221128} - \tfrac{263900025}{323210442256}\right),\, \tfrac{1}{h}\left(\tfrac{6504610150402h}{164937515625} - \tfrac{40401305282}{32987503125}\right),\, \tfrac{1}{h}\left(\tfrac{4233396234375h}{40401305282} + \tfrac{91631953125}{40401305282}\right),\, \tfrac{1}{h}\left(-\tfrac{1959463306177h}{206171894531250} + \tfrac{20200652641}{82468757812500}\right),\, \tfrac{1}{h}\left(-\tfrac{121076015625000h}{20200652641} + \tfrac{27127880859375}{20200652641}\right),\, \tfrac{1}{h}\left(\tfrac{836713423h}{42833496093750} + \tfrac{1553896357}{27052734375000}\right),\, \tfrac{1}{h}\left(-\tfrac{2830078125000h}{119530489} - \tfrac{26367187500}{9194653}\right),\, \tfrac{1}{h}\left(\tfrac{175769h}{4394531250} - \tfrac{24389}{5859375000}\right),\, \tfrac{1}{h}\left(\tfrac{34375000h}{2523} - \tfrac{9765625}{261}\right),\, \tfrac{1}{h}\left(\tfrac{383h}{781250} + \tfrac{1}{62500}\right),\, \tfrac{1}{h}\left(-\tfrac{4025h}{2} + \tfrac{125}{2}\right),\, \tfrac{1}{h}\left(-\tfrac{154h}{75} - \tfrac{2}{45}\right),\, \tfrac{1}{h}\left(\tfrac{97h}{200} - \tfrac{1}{80}\right)}\Big].$$

Непрерывные дроби элементов α/h и α/h^2 также периодические и имеют вид

$$\tfrac{\alpha}{h} = \Big[\tfrac{1}{h}\,(-80h - 4\,(9t+4))\,;\, \overline{\tfrac{1}{h}\left(-\tfrac{h}{72} + \tfrac{1}{96}\right),\, \tfrac{1}{h}\left(-\tfrac{11376h}{121} - \tfrac{216}{11}\right),\, \tfrac{1}{h}\left(\tfrac{26015h}{2985984} - \tfrac{1331}{1119744}\right),\, \tfrac{1}{h}\left(-\tfrac{44789760h}{4231249} - \tfrac{23887872}{248897}\right),\, \tfrac{1}{h}\left(\tfrac{1011268511h}{37456183296} + \tfrac{71931233}{32105299968}\right),\, \tfrac{1}{h}\left(-\tfrac{674211299328h}{18787130219} + \tfrac{43698880512}{15896802493}\right),\, \tfrac{1}{h}\left(-\tfrac{1033292162045h}{6525699489792} + \tfrac{2686559621317}{29365647704064}\right),\, \tfrac{1}{h}\left(\tfrac{58731295408128h}{34925275077121} + \tfrac{39154196938752}{34925275077121}\right),\, \tfrac{1}{h}\left(-\tfrac{174626375385605h}{2114326634692608} - \tfrac{34925275077121}{2114326634692608}\right),\, \tfrac{1}{h}\left(\tfrac{58731295408128h}{34925275077121} - \tfrac{44048471556096}{34925275077121}\right),\, \tfrac{1}{h}\left(\tfrac{22802452323079h}{29365647704064} + \tfrac{3175025007011}{19577098469376}\right),\, \tfrac{1}{h}\left(-\tfrac{304475996160h}{288638637001} + \tfrac{3776446464}{26239876091}\right),\, \tfrac{1}{h}\left(\tfrac{41270645h}{472055808} + \tfrac{140320193}{177020928}\right),\, \tfrac{1}{h}\left(-\tfrac{26982144h}{8254129} - \tfrac{131712}{485537}\right),\, \tfrac{1}{h}\left(\tfrac{1859h}{6272} - \tfrac{2197}{96768}\right),\, \tfrac{1}{h}\left(\tfrac{3240h}{169} - \tfrac{144}{13}\right),\, \tfrac{1}{h}\left(-\tfrac{h}{72} - \tfrac{1}{108}\right),\, \tfrac{1}{h}\,(10h+2)}\Big],$$

$$\tfrac{\alpha}{h^2} = \Big[\tfrac{1}{h^2}\,(96h^2 - 80h - 4\,(9t+4))\,;\, \overline{\tfrac{1}{h}\left(-\tfrac{5h}{128} + \tfrac{1}{128}\right),\, \tfrac{1}{h}\left(\tfrac{13440h}{961} + \tfrac{128}{31}\right),\, \tfrac{1}{h}\left(-\tfrac{24025h}{705024} - \tfrac{29791}{1410048}\right),\, \tfrac{1}{h}\left(\tfrac{14981760h}{923521} - \tfrac{2996352}{923521}\right),\, \tfrac{1}{h}\left(-\tfrac{10571h}{528768} - \tfrac{29791}{1586304}\right),\, \tfrac{1}{h}\left(\tfrac{19764h}{961} + \tfrac{162}{31}\right),\, \tfrac{1}{h}\left(-\tfrac{5h}{162} + \tfrac{1}{162}\right),\, \tfrac{1}{h^2}\,(-12h^2 + 10h + 2)}\Big].$$

Отметим, что неполные частные непрерывных дробей α и α/h имеют коэффициенты с достаточно большой высотой, что, вообще говоря, не характерно для периодических и квазипериодических непрерывных дробей (см., например, [52]).

3.3. Оценки длин периодов и квазипериодов функциональных непрерывных дробей

В разделе 3.2 показано, что теория функциональных непрерывных дробей дает эффективные арифметические инструменты для исследования проблемы поиска и построения фундаментальных S-единиц гиперэллиптического поля и проблемы кручения в якобиане соответствующей гиперэллиптической кривой. На примере задачи о решении уравнений типа Пелля, классические проблемы из теории числовых непрерывных дробей приобрели особый интерес в функциональном случае, особенно, когда соответствующие результаты значительно отличаются от традиционного случая. Один из таких результатов дает задача о верхней оценке длин периодов функциональных непрерывных дробей элементов гиперэллиптического поля.

В этом разделе найдены верхние оценки на длины периодов для "ключевых" элементов гиперэллиптических полей над полями алгебраических чисел. В случае, когда гиперэллиптическое поле задается многочленом нечетной степени, конечная длина периода тривиальным образом оценивается сверху удвоенной степенью фундаментальной S-единицы. Эту тривиальную оценку можно уточнить (см. [62; 74; 168]), но более интересный и сложный случай, когда гиперэллиптическое поле задается многочленом четной степени.

В числовом случае хорошо известны классические результаты [169; 170] об оценках сверху на длину периода непрерывных дробей элементов вида $\sqrt{d}$, $d \in \mathbb{N}$. В функциональном случае над конечным полем $\mathbb{F}_q$ оценки на длину периода изучались в статьях [171—173].

В эллиптическом случае $\deg f = 4$ над полем констант $K = \mathbb{Q}$ в [113; 114] был поставлен вопрос о возможной длине периода непрерывной дроби $\sqrt{f}$. Согласно известной теореме Мазура, если класс дивизора $(\infty^- - \infty^+)$ имеет конечный порядок m в группе классов дивизоров степени ноль $\Delta^\circ(L)$ эллиптического поля $\mathcal{L}$, то $2 \leq m \leq 10$ или $m = 12$. Используя этот результат и параметризацию из статьи Куберта [35], в [69; 72] показано, что длина периода n непрерывной дроби $\sqrt{f}$, построенной в $\mathbb{Q}((1/x))$, принимает одно из значений

$$\{1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 18, 22\},$$

причем для каждого n из этого множества существует бесконечная серия соответствующих примеров бирационально неэквивалентных эллиптических кривых. Для квадратичного поля констант K и $\deg f = 4$ в [67] доказано, что длина периода n непрерывной дроби $\sqrt{f}$, построенной в $K((1/x))$, может принимать одно из значений

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 22, 26, 30, 34\}.$$

Для гиперэллиптических полей $\mathcal{L} = K(x)(\sqrt{f})$, $\deg f = 2g + 2$, $g \geq 1$, в статье [62] дана оценка сверху на длину квазипериода N непрерывной дроби элемента специального вида $\beta = (B + \sqrt{f})/A \in \mathcal{L}$, где $A, B \in K[x]$, $A \mid f - B^2$, согласно которой $N \leq m - p + 1$, где m

— порядок класса дивизора $(\infty^- - \infty^+)$ в группе классов дивизоров степени ноль $\Delta^\circ(L)$, p — порядок полюса элемента β в ∞^+.

Для удобства в данном разделе мы рассматриваем непрерывные дроби, построенные в поле формальных степенных рядов $K((1/x))$, но основные результаты об оценках длин периодов для "ключевых" элементов остаются справедливы и для непрерывных дробей, построенные в поле формальных степенных рядов $K((x))$ (см. §3.1.3 и [8], §2).

Параграф §3.3.1 посвящен вспомогательным утверждениям, которые мы используем для доказательства основных результатов этого раздела. В частности, проведено полное исследование мультипликативной структуры последовательностей многочленов $T_n(x)$ и $Q_n(x)$, определенных в (3.3.1.1). Изучение многочленов $T_n(x)$ и $Q_n(x)$ необходимо для понимания структуры группы единиц кольца целых элементов гиперэллиптического поля $\mathcal{L} = K(x)(\sqrt{f})$. Связь многочленов $T_n(x)$ и $Q_n(x)$ с группой единиц и их применение для решений функционального уравнения Пелля приведены в §3.3.3. Группа единиц взаимно однозначно соотносится с множеством решений функционального уравнения Пелля, а свойства решений, в свою очередь, позволяют сделать выводы о периодичности "ключевых" элементов вида $\sqrt{f}/x^s$, $s \in \mathbb{Z}$ (см. предложение 3.3.3.1).

Для непрерывных дробей элементов вида $\sqrt{f}/x^s$, $s \in \mathbb{Z}$, справедливо утверждение: если длина квазипериода конечна, то длина периода либо равна длине квазипериода, либо равна удвоенной длине квазипериода (см. §3.2.3, теорему 3.2.3.3, а также [13; 142; 166]). Поэтому относительно элементов вида $\sqrt{f}/x^s$, $s \in \mathbb{Z}$, основной задачей является оценка сверху длины квазипериода непрерывной дроби.

В §3.3.2 найдены верхние оценки на длину квазипериода непрерывной дроби квадритичной иррациональности в зависимости от степени фундаментального решения функционального уравнения типа Пелля, соответствующего дискриминанту рассматриваемой квадратичной иррациональности.

Для приведенных в этом разделе результатов важным шагом стало доказательство теоремы 3.2.1.3 о достаточных условия одновременной квазипериодичности непрерывных дробей элементов $\alpha, \alpha \cdot x^s \in \mathcal{L} \setminus K(x)$. Для гиперэллиптических полей $\mathcal{L} = K(x)(\sqrt{f})$, построенных с помощью свободных от квадратов многочленов $f \in K[x]$ нечетной степени $2g+1$ достаточные условия также являются необходимыми. В случае $\deg f = 2g+2$ найденные достаточные условия не являются необходимыми, что подтверждается примерами 3.2.1.4-3.2.1.6. Когда для элементов α и $\alpha \cdot x^s$ достаточные условия не являются необходимыми, длины квазипериодов непрерывных дробей этих элементов могут отличаться в несколько раз. Так, в примере 3.2.4.1 найден свободный от квадратов многочлен f степени 6, для которого длина периода непрерывной дроби, построенной в $\mathbb{Q}((x))$ для элемента $\alpha = \sqrt{f}/x^3$, равна 2, а длина периода непрерывной дроби элемента $\alpha \cdot x^3 = \sqrt{f}$ равна 18 при том, что поле $\mathcal{L} = \mathbb{Q}(x)(\sqrt{f})$ обладает

фундаментальной S-единицей степени 4, где $S = \{v_x^-, v_x^+\}$.

В §3.3.3 теорема 3.3.3.3 уточняет теорему 3.2.1.3 в части нерассмотренного случая, когда дискриминант квадратичной иррациональности имеет четную степень, а именно, для гиперэллиптических полей $\mathcal{L} = K(x)(\sqrt{f})$, $\deg f = 2g + 2$, найден точный промежуток значений $s \in \mathbb{Z}$ таких, что непрерывные дроби элементов вида $\sqrt{f}/x^s \in \mathcal{L} \setminus K(x)$ периодические, где K — конечное расширение поля $\mathbb{Q}$. На основании этих результатов найдены точные оценки сверху на длину квазипериода непрерывных дробей "ключевых" элементов гиперэллиптических полей, определенных над полями алгебраических чисел K. Полученные оценки зависят только от рода гиперэллиптического поля, степени расширения $[K : \mathbb{Q}]$ и порядка подгруппы кручения якобиана соответствующей гиперэллиптической кривой.

В качестве следствия из полученных в §3.3.3 результатов, в §3.3.5 для фиксированной неособой гиперэллиптической кривой получено интересное утверждение о конечности количества обобщенных якобианов ассоциированных с определенными над K модулями ограниченной степени и с непустой подгруппой K-точек кручения. Дальнейшее развитие этого направления см. в [154].

В случае, когда степень многочлена $f(x)$ четная в §3.3.3 обнаружен удивительный эффект: длина квазипериода непрерывной дроби квадратичной иррациональности гиперэллиптического поля $\mathcal{L} = \mathbb{Q}(x)(\sqrt{f})$ может быть значительно больше порядка подгруппы кручения якобиана соответствующей гиперэллиптической кривой. В связи с этим в §3.3.6 поставлен естественный вопрос: в каждом ли гиперэллиптическом поле $\mathcal{L} = \mathbb{Q}(x)(\sqrt{f})$, обладающем нетривиальными единицами кольца целых элементов, существует элемент α с длиной квазипериода непрерывной дроби больше наперед заданного числа. В теореме 3.3.6.1 получен положительный ответ на этот вопрос (дополнительно см. [1]).

Наконец, в §3.3.7 полученные результаты проиллюстрированы для случая квадратичных полей констант K, а также найдены примеры, демонстрирующие точность полученных оценок на длины квазипериодов и периодов.

Результаты раздела этого раздела опубликованы в статьях [1; 3; 10]. Этим результатам предшествовали статьи [13; 14], в которых рассмотрена проблема о верхней оценке длин периодов функциональных непрерывных дробей над полем $\mathbb{Q}$, а также доказан критерий периодичности 3.2.1.3.

3.3.1. Вспомогательные утверждения

Для натуральных n определим две последовательности многочленов $T_n, Q_n \in \mathbb{Z}[x]$:

$$T_n(x) = \sum_{0 \le j \le n/2} \binom{n}{2j} x^j, \quad Q_n(x) = \sum_{0 \le j < n/2} \binom{n}{2j+1} x^j. \tag{3.3.1.1}$$

Из определения следует, что степень многочлена T_n равна $\left[\frac{n}{2}\right]$, а степень многочлена Q_n равна $\left[\frac{n-1}{2}\right]$. Отметим, что многочлены $T_n(x)$ и $Q_n(x)$ похожи на многочлены Чебышева первого и второго рода и на многочлены Диксона, но их свойства не эквивалентны (см. [51]).

Положим $x = y^2$, тогда справедливо тождество

$$T_n(y^2) + yQ_n(y^2) = \sum_{0\le k\le n} \binom{n}{k} y^k = (1+y)^n. \tag{3.3.1.2}$$

Если подставить вместо y значение $-y$, то имеем

$$T_n(y^2) - yQ_n(y^2) = (1-y)^n. \tag{3.3.1.3}$$

Отсюда получаем формулы, которые можно использовать как альтернативное определение многочленов T_n, Q_n:

$$T_n(y^2) = \frac{1}{2}\Big((1+y)^n + (1-y)^n\Big), \tag{3.3.1.4}$$

$$Q_n(y^2) = \frac{1}{2y}\Big((1+y)^n - (1-y)^n\Big). \tag{3.3.1.5}$$

Докажем ряд вспомогательных утверждений.

Предложение 3.3.1.1. *При любом $n \in \mathbb{N}$ многочлены $T_n(x)$ и $Q_n(x)$ взаимно просты.*

Доказательство. Предположим, что $x_0 \in \mathbb{C}$ является общим корнем многочленов $T_n(x)$ и $Q_n(x)$. Тогда в силу (3.3.1.2) для $y_0 \in \mathbb{C}$ такого, что $y_0^2 = x_0$, справедливо тождество

$$(1+y_0)^n = T_n(x_0) + y_0Q_n(x_0) = 0,$$

откуда получаем $y_0 = -1$. Но это противоречит соотношениям

$$T_n\big((-1)^2\big) = \sum_{0\le j\le n/2} \binom{n}{2j} > 0, \quad Q_n\big((-1)^2\big) = \sum_{0\le j<n/2} \binom{n}{2j+1} > 0.$$

□

Предложение 3.3.1.2. *При любом $n \in \mathbb{N}$, $n \ge 2$, справедливы формулы*

$$T_n(x) = T_{n-1}(x) + xQ_{n-1}(x), \quad Q_n(x) = T_{n-1}(x) + Q_{n-1}(x). \tag{3.3.1.6}$$

Доказательство. Следует из формул (3.3.1.1). □

Предложение 3.3.1.3. *Многочлены $T_n(x)$ и $Q_n(x)$ удовлетворяют линейному рекуррентному соотношению*

$$\lambda_n = 2\lambda_{n-1} + (x-1)\lambda_{n-2}, \quad n \in \mathbb{N},\ n \ge 2, \tag{3.3.1.7}$$

с начальными условиями $T_0(x) = 1$, $T_1(x) = 1$, $Q_0(x) = 0$, $Q_1(x) = 1$.

Доказательство. Следует из предложения 3.3.1.2. □

Предложение 3.3.1.4. *При любом $n \in \mathbb{N}$, $n \geq 2$, справедливы формулы*

$$2T_n'(x) = nQ_{n-1}(x), \quad 2xQ_n'(x) + Q_n(x) = nT_{n-1}(x), \tag{3.3.1.8}$$

где штрихом обозначена производная.

Доказательство. Дифференцируя соотношение (3.3.1.1) имеем

$$T_n'(x) = \sum_{0<j\leq n/2} j\binom{n}{2j}x^{j-1} = \frac{n}{2}\sum_{0\leq j<(n-1)/2}\binom{n-1}{2j+1}x^j = \frac{n}{2}Q_{n-1}(x).$$

Дифференцируя соотношение (3.3.1.2), учитывая, что $y^2 = x$, получаем

$$2yT_n'(x) + 2xQ_n'(x) + Q_n(x) = n(y+1)^{n-1} = nT_{n-1}(x) + nyQ_{n-1}(x).$$

Следовательно, $2xQ_n'(x) + Q_n(x) = nT_{n-1}(x)$. □

Следствие 3.3.1.5. *При любом $n \in \mathbb{N}$ многочлены $T_n(x)$ и $Q_n(x)$ не имеют кратных корней.*

Доказательство. Пусть x_0 — кратный корень многочлена $T_n(x)$, тогда $T_n(x_0) = T_n'(x_0) = 0$. По предложению 3.3.1.4 имеем $Q_{n-1}(x_0) = 0$, а по предложению 3.3.1.2 имеем $T_{n-1}(x_0) = 0$. Но согласно предложению 3.3.1.1 это противоречит взаимной простоте многочленов $T_{n-1}(x)$ и $Q_{n-1}(x)$.

Пусть x_0 — кратный корень многочлена $Q_n(x)$, тогда $Q_n(x_0) = Q_n'(x_0) = 0$. По предложению 3.3.1.4 имеем $T_{n-1}(x_0) = 0$, а по предложению 3.3.1.2 имеем $Q_{n-1}(x_0) = 0$. Но согласно предложению 3.3.1.1 это противоречит взаимной простоте многочленов $T_{n-1}(x)$ и $Q_{n-1}(x)$. □

Предложение 3.3.1.6. *Для любых $n, m \in \mathbb{N}$ справедливы тождества*

$$T_{nm}(x) = \big(T_n(x)\big)^m \cdot T_m(z), \quad Q_{nm}(x) = \big(T_n(x)\big)^{m-1} \cdot Q_n(x) \cdot Q_m(z), \tag{3.3.1.9}$$

где $z = x\big(Q_n(x)/T_n(x)\big)^2$.

Доказательство. Из (3.3.1.2), сохраняя обозначение $x = y^2$, имеем

$$T_{nm}(y^2) + yQ_{nm}(y^2) = (1+y)^{nm} = \Big(T_n(y^2) + yQ_n(y^2)\Big)^m = \\ = \big(T_n(y^2)\big)^m \left(1 + y\frac{Q_n(y^2)}{T_n(y^2)}\right)^m. \tag{3.3.1.10}$$

Обозначим $u = yQ_n(y^2)/T_n(y^2)$ и $z = u^2 = x\big(Q_n(x)/T_n(x)\big)^2$, тогда, продолжая равенства (3.3.1.10), с помощью (3.3.1.2) получаем

$$T_{nm}(x) + yQ_{nm}(x) = \big(T_n(x)\big)^m \big(T_m(u^2) + uQ_m(u^2)\big) = \\ = \big(T_n(x)\big)^m \cdot T_m(z) + y\big(T_n(x)\big)^{m-1} Q_n(x) \cdot Q_m(z). \tag{3.3.1.11}$$

Поскольку $x = y^2$ и z есть функция от y^2, то из (3.3.1.11) получаем тождества (3.3.1.9). □

Следствие 3.3.1.7. *Пусть K — числовое поле, и даны числа $n, m \in \mathbb{N}$. Если у многочленов $T_n(x)$, $Q_n(x)$, $T_m(x)$ и $Q_m(x)$ нет корней в поле K, то у многочленов $T_{nm}(x)$ и $Q_{nm}(x)$ также нет корней в поле K.*

Доказательство. Следует из формул (3.3.1.9). □

В статье [14] были найдены все рациональные корни многочленов $T_n(x)$ и $Q_n(x)$ при всех натуральных n: для многочленов $T_n(x)$, $n \in \mathbb{N}$, корнями могут быть только $x \in \{-1, -1/3\}$, более точно, $T_{2(2k-1)}(-1) = 0$, $T_{3(2k-1)}(-1/3) = 0$ при всех $k \in \mathbb{N}$, причем указанные корни имеют кратность один и других рациональных корней нет; для многочленов $Q_n(x)$, $n \in \mathbb{N}$, корнями могут быть только $x \in \{-3, -1, -1/3\}$, более точно, $Q_{3k}(-3) = 0$, $Q_{4k}(-1) = 0$, $Q_{6k}(-1/3) = 0$ при всех $k \in \mathbb{N}$, причем указанные корни имеют кратность один и других рациональных корней нет.

Дальнейшая наша задача состоит в точном описании всех возможных корней многочленов T_n, Q_n для всех $n \in \mathbb{N}$. Оказывается, если некоторое алгебраическое число x_0 является корнем многочлена T_k для некоторого $k \in \mathbb{N}$, то в числовых последовательностях $\{T_n(x_0)\}_{n\in\mathbb{N}}$ и $\{Q_n(x_0)\}_{n\in\mathbb{N}}$ нули встречаются периодическим образом, а именно, индексы нулевых членов в $\{T_n(x_0)\}_{n\in\mathbb{N}}$ и $\{Q_n(x_0)\}_{n\in\mathbb{N}}$ образуют соответственно две бесконечные арифметические прогрессии. Аналогично, если алгебраическое число x_0 является корнем некоторого многочлена Q_k, то индексы нулевых членов в $\{Q_n(x_0)\}_{n\in\mathbb{N}}$ также образуют бесконечную арифметическую прогрессию. В общем случае для доказательства этого утверждения можно воспользоваться теоремой Сколем-Малера-Леха (см., например, [174]), поскольку по предложению 3.3.1.3 последовательности T_n и Q_n удовлетворяют линейному рекуррентному соотношению. Но теорема Сколем-Малера-Леха имеет неконструктивный характер, а нам важно получить явную структуру возможных корней многочленов $T_n(x)$ и $Q_n(x)$.

Утверждение о том, что обнуляющиеся члены последовательностей $T_n(x_0)$ и $Q_n(x_0)$ образуют арифметические прогрессии, легко следует из следующего предложения.

Предложение 3.3.1.8. *1. Пусть n нечетное. Тогда*

- $T_n(x) = x^{\deg Q_n} Q_n(1/x)$;
- *если $q \mid n$, то $T_q(x) \mid T_n(x)$, $Q_q(x) \mid Q_n(x)$.*

2. Пусть n четное. Тогда

- $T_n(x) = x^{\deg T_n} T_n(1/x)$;
- *если $n = qd$, q — нечетное, то $T_d(x) \mid T_n(x)$, $Q_q(x) \mid Q_n(x)$;*
- *если $n = qd$, d — четное, то $T_q(x) \mid Q_n(x)$.*

Доказательство. Пусть n нечетное, тогда $n-2j$ нечетное, $\binom{n}{2j} = \binom{n}{n-2j}$ и количество слагаемых в определении (3.3.1.1) многочленов $T_n(x)$, $Q_n(x)$ совпадает, откуда, $T_n(x) = x^{\deg Q_n} Q_n(1/x)$. Аналогично, при четном n число $n-2j$ также четно, и $\binom{n}{2j} = \binom{n}{n-2j}$, откуда $T_n(x) = x^{\deg T_n} T_n(1/x)$.

Остальные соотношения следуют из формул (3.3.1.9). □

Таким образом, задача описания всех алгебраических корней многочленов из последовательностей $\{T_n(x)\}_{n\in\mathbb{N}}$ и $\{Q_n(x)\}_{n\in\mathbb{N}}$ сводится к поиску корней x_0 и соответствующих им арифметических прогрессий индексов n_j, для которых $T_{n_j}(x_0) = 0$ или $Q_{n_j}(x_0) = 0$. Для решения этой задачи мы найдем для каждого $n \in \mathbb{N}$ разложения на неприводимые над $\mathbb{Q}$ множители многочленов $T_n(x)$ и $Q_n(x)$. Забегая вперед, отметим, что эти разложения будут зависеть от разложения индекса n на простые множители, а сами неприводимые над $\mathbb{Q}$ множители многочленов $T_n(x)$ и $Q_n(x)$ будут связаны с круговыми многочленами $\Phi_k(x)$ — неприводимыми над $\mathbb{Q}$ множителями многочлена $x^n + 1$.

Из предложения 3.3.1.8 следует, что некоторые множители $Q_n(x)$ лежат в последовательности многочленов $\{T_j(x)\}_{j\in\mathbb{N}}$, а некоторые — связаны с соответствующими многочленами из $\{T_j(x)\}_{j\in\mathbb{N}}$. Далее мы увидим, что на самом деле все неприводимые над $\mathbb{Q}$ множители многочлена $Q_n(x)$ однозначно восстанавливаются из некоторых неприводимых над $\mathbb{Q}$ множителей многочленов из $\{T_j(x)\}_{j\in\mathbb{N}}$. Поэтому сейчас в первую очередь обратимся к исследованию разложения на неприводимые множители над $\mathbb{Q}$ многочленов $T_n(x)$ при различных $n \in \mathbb{N}$.

Положим $L(T_n)$ — наименьшее общее кратное многочленов T_d, где d пробегает все такие делители числа n, что n/d нечетное и больше 1. Тогда по предложению 3.3.1.8 корректно определен многочлен $P(T_n) = T_n/L(T_n)$.

Положим $\tilde{P}(T_n)(x) = x^d P(T_n)(1/x)$, где $d = \deg P(T_n)(x)$. Отметим, что по предложению 3.3.1.8 при нечетном n справедливо соотношение $\tilde{P}(T_n)(x) \mid Q_n$, а при четном n справедливо равенство $\tilde{P}(T_n)(x) = P(T_n)(x)$.

При $k \in \mathbb{N}$ обозначим $\Phi_k(x)$ — круговой многочлен степени $\varphi(k)$:

$$\Phi_k(x) = \prod_{1\le j\le k,\quad (j,k)=1} \left(x - e^{2\pi i \frac{j}{k}}\right).$$

Лемма 3.3.1.9. *Пусть $n = 2^t q$, где q нечетно. Справедливо тождество*

$$x^n + 1 = \prod_{d\mid q} \Phi_{2^{t+1}d}(x). \tag{3.3.1.12}$$

Доказательство. Действительно,

$$x^{2n} - 1 = \prod_{r\mid 2n} \Phi_r(x) = \prod_{r\mid n} \Phi_r(x) \cdot \prod_{d\mid q} \Phi_{2^{t+1}d}(x) = (x^n - 1) \prod_{d\mid q} \Phi_{2^{t+1}d}(x).$$

□

В статье [175] определено понятие дробно-линейного преобразования многочленов. Обобщим это понятие на рациональные функции и докажем некоторые свойства, которые будем использовать в дальнейшем.

Пусть K - поле и $M \in \mathrm{GL}(2, K)$,

$$M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right). \tag{3.3.1.13}$$

Определим оператор $M : K(x) \to K(x)$ на поле рациональных функций $K(x)$ следующим образом:

$$M\alpha(x) = (cx + d)^{-v_\infty(\alpha)} \alpha\left(\frac{ax + b}{cx + d}\right), \tag{3.3.1.14}$$

где $\alpha = T(x)/Q(x) \in K(x)$, многочлены $T(x)$ и $Q(x)$ взаимно просты, $v_\infty(\alpha) = \deg Q - \deg T$. Если $\alpha \in K$, то положим $M\alpha = \alpha$. Отметим, что для $T(x) \in K[x]$ имеем $MT(x) \in K[x]$.

Положим

$$[M]x = \frac{ax + b}{cx + d}.$$

Для $\alpha \in K(x)$ назовем $M\alpha(x)$ *невырожденным*, если $v_\infty(M\alpha) = v_\infty(\alpha)$.

Оператор M *обратим слева*, если существует оператор $M_1 \in \mathrm{GL}(2, K)$, такой, что $M_1 M\alpha = \alpha$ для любого $\alpha \in K(x)$ с невырожденным $M\alpha$. Оператор M *обратим справа*, если существует $M_1 \in \mathrm{GL}(2, K)$, что $MM_1\alpha = \alpha$ для любого $\alpha \in K(x)$ с невырожденным $M_1\alpha$.

Предложение 3.3.1.10. *Пусть $\alpha, \beta \in K(x)$ и $M \in GL(2, K)$ определено как в (3.3.1.13). Тогда*

1. $M(\alpha \cdot \beta) = M\alpha \cdot M\beta$;
2. *$M\alpha$ невырождено тогда и только тогда, когда $c = 0$ или $v_h^-(\alpha) = 0$, где $h = cx - a$;*
3. *для оператора M существуют обратные операторы слева и справа, причем они совпадают и задаются матрицей M^{-1}.*

Доказательство. Первое утверждение тривиально следует из определения (3.3.1.14) оператора M, поскольку $v_\infty(\alpha \cdot \beta) = v_\infty(\alpha) + v_\infty(\beta)$ при $\alpha, \beta \in K(x) \setminus K$. Отдельно отметим, что $Mc\alpha = cM\alpha$ для $c \in K$.

Положим $\alpha = T(x)/Q(x)$, где многочлены $T(x)$ и $Q(x)$ взаимно просты. Из (3.3.1.14) следует, что $M\alpha(x) = MT(x)/MQ(x)$. Разложив многочлены $T(x)$ и $Q(x)$ на линейные множители над замыканием $\overline{K}$, замечаем, что для доказательства второго утверждение достаточно его проверить для случая $\alpha = x - x_0$. Имеем

$$M(x - x_0) = (ax + b) - x_0(cx + d) = (a - cx_0)x - (dx_0 - b).$$

Поскольку $\det M \neq 0$, то a и c не могут одновременно быть равны нулю. Значит $\deg M(x - x_0) = 1$ тогда и только тогда, когда $c = 0$ или $x_0 \neq a/c$, то есть $v_h^-(x - x_0) = 0$, где $h = cx - a$.

Третье утверждение также достаточно проверить для $\alpha = x - x_0$. Пусть $M(x - x_0)$ невырождено. Положим $\hat{x}_0 = [M^{-1}]x_0$, тогда $M(x - x_0) = (a - cx_0)(x - \hat{x}_0)$. Возьмем

$$M_1 = \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right),$$

тогда

$$M_1 M(x - x_0) = (a - cx_0)((a_1 x + b_1) - \hat{x}_0(c_1 x + d_1)) = (a - cx_0)(a_1 x + c_1) - (dx_0 - b)(c_1 x + d_1).$$

Приравнивая $M_1 M(x - x_0) = x - x_0$, находим $a_1 = d/D$, $b_1 = -b/D$, $c_1 = -c/D$, $d_1 = a/D$, где $D = \det M$. Таким образом, однозначно восстанавливается $M_1 = M^{-1}$. Обратимость справа проверяется аналогично. □

Лемма 3.3.1.11. *Пусть многочлен $P \in K[x]$ неприводим над полем K и $MP(x)$ невырожденный для некоторой матрицы $M \in GL(2, K)$. Тогда многочлен $MP(x)$ также неприводим над K.*

Доказательство. Предположим, что $P \in K[x]$ неприводим, $MP(x)$ невырожденный и $MP(x) = T(x)Q(x)$, где T, Q непостоянные многочлены. Тогда по предложению 3.3.1.10 имеем

$$P(x) = M^{-1}MP(x) = M^{-1}T(x) \cdot M^{-1}Q(x),$$

причем $M^{-1}T(x), M^{-1}Q(x) \in K[x]$ невырожденные, то есть $\deg M^{-1}T(x) = \deg T$ и $\deg M^{-1}Q(x) = \deg Q$. Это противоречит неприводимости многочлена P над K. □

Теорема 3.3.1.12. *Пусть $n = 2^t q$, где q нечетно. Тогда справедливо разложение на неприводимые над $\mathbb{Q}$ множители*

$$T_n(x) = \prod_{d|q} P(T_{2^t d})(x), \tag{3.3.1.15}$$

$$Q_n(x) = 2^t \prod_{d|q} \tilde{P}(T_d)(x) \cdot {\prod_{r|n}}' P(T_r)(x), \tag{3.3.1.16}$$

где последнее произведение берется по всем делителям r числа n таким, что n/r четное.

Доказательство. Согласно тождеству (3.3.1.4) и лемме 3.3.1.9 справедливо представление

$$T_n(y^2) = \frac{1}{2}\Big((1+y)^n + (1-y)^n\Big) = \frac{1}{2}(1-y)^n \left(1 + \frac{(1+y)^n}{(1-y)^n}\right) =$$
$$= \frac{1}{2}(1-y)^n \left(1 + \left(\frac{1+y}{1-y}\right)^n\right) = \frac{1}{2}(1-y)^n \prod_{d|q} \Phi_{2^{t+1}d}\left(\frac{1+y}{1-y}\right). \tag{3.3.1.17}$$

При $k > 1$ для кругового многочлена $\Phi_k(x)$ справедливо соотношение $\Phi_k(x) = x^{\varphi(k)}\Phi_k\left(\frac{1}{x}\right)$. Положим $M = \left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)$. Тогда

$$\Psi_k(y) = M\Phi_k(y) = (1-y)^{\varphi(k)}\Phi_k\left(\frac{1+y}{1-y}\right) = (1+y)^{\varphi(k)}\Phi_k\left(\frac{1-y}{1+y}\right) \in \mathbb{Z}[y],$$

откуда следует, что $\Psi_k(y)$ является четной функцией, то есть $\Psi_k(y) = R_k(y^2) = R_k(x) \in \mathbb{Z}[x]$. В силу неприводимости кругового многочлена $\Phi_k(x)$ над $\mathbb{Q}$ по лемме 3.3.1.11 при $k > 2$ заключаем, что многочлен $\Psi_k(y)$ неприводим над $\mathbb{Q}$, а, следовательно, и многочлен $R_k(x)$ также неприводим над $\mathbb{Q}$. Дополнительно отметим, что $\Psi_2(y) = M\Phi_2(y) = 2$. Таким образом, из (3.3.1.17) имеем разложение на неприводимые над $\mathbb{Q}$ множители

$$T_n(y^2) = \frac{1}{2}\prod_{d|q} R_{2^{t+1}d}(x). \tag{3.3.1.18}$$

Докажем, что $R_{2^{t+1}d}(x) = P(T_{2^t d})(x)$ при нечетном $d > 1$ и $R_{2^{t+1}}(x) = 2P(T_{2^t})(x)$. Доказательство проведем индукцией по количеству простых делителей нечетного числа q, где $n = 2^t q$. Обозначим за s количество не обязательно различных простых делителей нечетного числа q. При $s = 0$, то есть $q = 1$ и $n = 2^t$, сравнивая (3.3.1.15) и (3.3.1.18), имеем $R_{2^{t+1}}(x) = 2P(T_{2^t})(x)$. Пусть справедливо разложение (3.3.1.15) на неприводимые над $\mathbb{Q}$ множители и p — простое нечетное число. Тогда с одной стороны запишем

$$T_{pn}(x) = P(T_{pn})(x) \cdot \prod_{d|q} P(T_{2^t d})(x) \prod_{d|q,\ \ d\neq q} P(T_{2^t pd})(x) = \prod_{d|pq} P(T_{2^t d})(x),$$

а с другой стороны из (3.3.1.18) по предположению индукции имеем

$$T_{pn}(x) = \frac{1}{2}\prod_{d|pq} R(T_{2^{t+1}d})(x) = R(T_{2^{t+1}pq})(x) \cdot \prod_{d|q} P(T_{2^t d})(x) \prod_{d|q,\ \ d\neq q} P(T_{2^t pd})(x).$$

Следовательно, $R_{2^{t+1}pq}(x) = P(T_{pn})(x)$, что и требовалось доказать.

Для доказательство соотношения (3.3.1.16) аналогично запишем

$$Q_n(y^2) = \frac{1}{2y}\Big((1+y)^n - (1-y)^n\Big) = \frac{(1-y)^n}{2y}\left(\left(\frac{1+y}{1-y}\right)^n - 1\right) =$$
$$= \frac{(1-y)^n}{2y}\prod_{d|n}\Phi_d\left(\frac{1+y}{1-y}\right) = \frac{(1-y)^n}{2y}\prod_{d|q}\Phi_d\left(\frac{1+y}{1-y}\right)\prod_{d|\frac{n}{2}}\Phi_{2d}\left(\frac{1+y}{1-y}\right), \tag{3.3.1.19}$$

где последнее произведение считаем пустым, если n нечетно. Отметим, что $M\Phi_1(y) = 2y$, и при нечетных d справедливо $\Phi_d(y) = \Phi_{2d}(-y)$. Продолжая (3.3.1.19), получаем

$$Q_n(x) = \frac{1}{2y}\prod_{d|q} M\Phi_d(y)\prod_{d|\frac{n}{2}} M\Phi_{2d}(y) = \prod_{d|q,\ d>1} M\big(\Phi_{2d}(-y)\big)\prod_{d|\frac{n}{2}} M\Phi_{2d}(y).$$

Остается, как и ранее, по индукции по количеству не обязательно различных нечетных простых делителей n заметить, что $M\Phi_2(y) = 2$, и при $d > 1$ верно равенство

$$M\big(\Phi_{2d}(-y)\big) = (1-y)^{\varphi(2d)}\Phi_{2d}\left(-\frac{1+y}{1-y}\right) = \tilde{P}(T_d)(x).$$

Теорема 3.3.1.12 доказана. □

Следствие 3.3.1.13. *Пусть $n \in \mathbb{N}$, $n = 2^t q$, q нечетно, тогда* $\deg P(T_n) = \deg \tilde{P}(T_n) = 2^{t-1}\varphi(q)$.

Доказательство. В ходе доказательства теоремы 3.3.1.12 показано, что при $x = y^2$ и $n =$

$2^t q > 1$ справедливы равенства

$$P(T_{2^t q})(x) = R_{2^{t+1}q}(x) = \Psi_{2^{t+1}q}(y) = M\Phi_{2^{t+1}q}(y),$$

причем $\deg M\Phi_{2^{t+1}q}(y) = \deg \Phi_{2^{t+1}q}(y) = 2^t\varphi(q)$. Следовательно, $\deg P(T_n) = \deg \tilde{P}(T_n) = 2^{t-1}\varphi(q)$. □

Следствие 3.3.1.14. *Пусть $n \in \mathbb{N}$, $n = 2^t q$, q нечетно, тогда*

$$\omega(T_n) = \begin{cases} \tau(q),\ t > 0, \\ \tau(q) - 1,\ t = 0; \end{cases} \qquad \omega(Q_n) = \begin{cases} \tau(n/2) + \tau(q) - 2,\ t > 0, \\ \tau(q) - 1,\ t = 0, \end{cases} \tag{3.3.1.20}$$

где функция $\omega(R)$ обозначает количество нетривиальных неприводимых над $\mathbb{Q}$ множителей многочлена R.

Доказательство. Утверждение следствия сразу следует из теоремы 3.3.1.12. □

Теорема 3.3.1.12 позволяет восстановить все алгебраические корни многочленов $T_n(x)$ и $Q_n(x)$, через корни из 1 соответствующих степеней:

- если ξ — примитивный корень из 1 степени $2^{t+1}d$, где $n = 2^t q$, q нечетное, $d \mid q$, то $x_\xi = (\xi - 1)^2/(\xi + 1)^2$ — корень многочлена $T_n(x)$;
- если ξ — примитивный корень из 1 степени $2d$, где n четное, $d \mid \frac{n}{2}$, то $x_\xi = (\xi-1)^2/(\xi+1)^2$ — корень многочлена $Q_n(x)$;
- если ξ — примитивный корень из 1 степени $2d$, где $n = 2^t q$, q нечетно, $d \mid q$, то $x_\xi = (\xi + 1)^2/(\xi - 1)^2$ — корень многочлена $Q_n(x)$.

Следствие 3.3.1.15. *У многочленов $T_n(x)$ и $Q_n(x)$ в совокупности для всех $n \in \mathbb{N}$ количество различных неприводимых над $\mathbb{Q}$ множителей ограниченной степени конечно.*

Доказательство. Из теоремы 3.3.1.12 следует, что множество различных неприводимых над $\mathbb{Q}$ множителей многочленов $T_n(x)$ и $Q_n(x)$ при $n \in \mathbb{N}$ есть

$$\{P(T_k)(x), \quad k \in \mathbb{N}\}.$$

Из следствия 3.3.1.13 и нижних оценок на функцию $\varphi(n)$ получаем

$$P(T_n)(x) \geq \varphi(n) \geq \frac{n}{2\log_2 n},$$

то есть неравенство $\deg P(T_n)(x) \leq b$ для некоторой положительной величины b влечет $n \leq 2b(\log_2 b + \log_2\log_2 b + 1)$. □

3.3.2. Общие оценки на длину квазипериода и периода

Для $A, B, C, D \in K[x]$ и $\beta \in \mathcal{L}$ будем использовать обозначение

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\left[\begin{smallmatrix} \beta \\ 1 \end{smallmatrix}\right] = \frac{A\beta + B}{C\beta + D}. \tag{3.3.2.1}$$

Лемма 3.3.2.1. *Пусть*

$$\left(\begin{smallmatrix} R & S \\ T & U \end{smallmatrix}\right)\left[\begin{smallmatrix} \alpha \\ 1 \end{smallmatrix}\right] = \beta, \quad \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\left[\begin{smallmatrix} \beta \\ 1 \end{smallmatrix}\right] = \kappa, \tag{3.3.2.2}$$

тогда

$$\left(\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\left(\begin{smallmatrix} R & S \\ T & U \end{smallmatrix}\right)\right)\left[\begin{smallmatrix} \alpha \\ 1 \end{smallmatrix}\right] = \kappa, \tag{3.3.2.3}$$

где в левой части последнего равенства стоит произведение матриц.

Доказательство. Для доказательства достаточно используя (3.3.2.1) подставить выражение для β во второе равенство (3.3.2.2):

$$\kappa = \frac{A\beta + B}{C\beta + D} = \frac{A(R\alpha + S) + B(T\alpha + U)}{C(R\alpha + S) + D(T\alpha + U)} = \left(\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\left(\begin{smallmatrix} R & S \\ T & U \end{smallmatrix}\right)\right)\left[\begin{smallmatrix} \alpha \\ 1 \end{smallmatrix}\right].$$

Лемма 3.3.2.1 доказана. □

Дополнительные скобки в выражениях типа (3.3.2.3) будем опускать.

Следующее утверждение было доказано в [118] (лемма 1), но мы повторим рассуждения с новыми обозначениями.

Лемма 3.3.2.2. *Пусть $A, B, C, D \in K[x]$, $AD - BC = b \in K^*$, $\deg D < \deg C$. Пусть $\alpha, \beta \in \mathcal{L}$ такие, что $v_\infty^-(\beta) \le -1$ и*

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\left[\begin{smallmatrix} \beta \\ 1 \end{smallmatrix}\right] = \alpha.$$

Тогда найдется такой номер $n \in \mathbb{N}_0$ и $r \in K^*$, что

$$\beta = (-1)^{n-1} b r^{-2} \alpha_{n+1},\ A = r p_n,\ B = (-1)^{n-1} r^{-1} b p_{n-1},\ C = r q_n,\ D = (-1)^{n-1} r^{-1} b q_{n-1},$$

где p_j/q_j — j-ая подходящая дробь к α.

Доказательство. Запишем разложение в непрерывную дробь рационального выражения (см. матричное представление в [176]):

$$\frac{A}{C} = [a_0^*; a_1^*, \ldots, a_n^*] = \left(\begin{smallmatrix} a_0^* & 1 \\ 1 & 0 \end{smallmatrix}\right) \ldots \left(\begin{smallmatrix} a_n^* & 1 \\ 1 & 0 \end{smallmatrix}\right)\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left(\begin{smallmatrix} p_n^* & p_{n-1}^* \\ q_n^* & q_{n-1}^* \end{smallmatrix}\right)\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \frac{p_n^*}{q_n^*}.$$

Тогда для некоторой постоянной $r \in K^*$ имеем $A = r p_n^*$, $C = r q_n^*$. Учитывая (3.1.1.3), получаем

$$0 = (-1)^n (AD - BC) - b(q_n^* p_{n-1}^* - p_n^* q_{n-1}^*) = p_n^*\big((-1)^n r D + b q_{n-1}^*\big) - q_n^*\big((-1)^n r B + b p_{n-1}^*\big),$$

причем $(p_n^*, q_n^*) \in K^*$, и $\deg D < \deg C$, следовательно, $B = (-1)^{n-1} r^{-1} b p_{n-1}^*$, $D = (-1)^{n-1} r^{-1} b q_{n-1}^*$ (см. по аналогии с [164], §2.3). Пусть разложение α в непрерывную дробь имеет вид $[a_0; a_1, \ldots, a_n, \alpha_{n+1}]$.

тогда по условию леммы

$$\left(\begin{smallmatrix} a_0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \dots \left(\begin{smallmatrix} a_n & 1 \\ 1 & 0 \end{smallmatrix}\right) \left[\begin{smallmatrix} \alpha_{n+1} \\ 1 \end{smallmatrix}\right] = \alpha = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \left[\begin{smallmatrix} \beta \\ 1 \end{smallmatrix}\right] =$$
$$= \begin{pmatrix} p_n^* & p_{n-1}^* \\ q_n^* & q_{n-1}^* \end{pmatrix} \left[\begin{smallmatrix} (-1)^{n-1} r^2 b^{-1} \beta \\ 1 \end{smallmatrix}\right] = \left(\begin{smallmatrix} a_0^* & 1 \\ 1 & 0 \end{smallmatrix}\right) \dots \left(\begin{smallmatrix} a_n^* & 1 \\ 1 & 0 \end{smallmatrix}\right) \left[\begin{smallmatrix} (-1)^{n-1} r^2 b^{-1} \beta \\ 1 \end{smallmatrix}\right],$$

откуда, учитывая $v_\infty^-(\beta) \leq -1$, в силу единственности разложения в непрерывную дробь получаем $a_0 = a_0^*, \dots, a_n^* = a_n$, $\alpha_{n+1} = (-1)^{n-1} r^2 b^{-1} \beta$, что и требовалось доказать. □

Пусть элемент $\beta \in \mathcal{L} = K(x)(\sqrt{f})$ является корнем уравнения

$$\Lambda_2 X^2 + 2\Lambda_1 X + \Lambda_0 = 0, \tag{3.3.2.4}$$

где $\Lambda_0, \Lambda_1, \Lambda_2 \in K[x]$ взаимно простые многочлены. Обозначим $d = \Lambda_1^2 - \Lambda_0 \Lambda_2$. Известно, что (см., например, теорему 2 [118]) квазипериодичность непрерывной дроби $\beta = [a_0; a_1, \dots]$ в $K((1/x))$ эквивалентна наличию решения $\Theta_1, \Theta_2 \in K[x]$, $\Theta_2 \neq 0$, уравнения

$$\Theta_1^2 - \Theta_2^2 d = \gamma \in K^*. \tag{3.3.2.5}$$

В случае квазипериодичности непрерывная дробь элемента β может быть записана следующим образом

$$\beta = [a_0; a_1, \dots, a_{m-1}, \overline{a_m, \dots, a_{m+N-1}}^c], \tag{3.3.2.6}$$

где $a_m, \dots, a_{m+N-1}$ — квазипериод длины N, c — константа квазипериода. Напомним, что согласно предложению 3.1.6.3 длина предпериода m не превосходит 2.

Пункты 1., 2. следующей теоремы частично повторяют результаты [118], но их изложение необходимо для корректного обоснования пункта 3. теоремы, который будет необходим для доказательства верхних и нижних оценок на длину квазипериода.

Теорема 3.3.2.3. *Пусть β — корень уравнения (3.3.2.4).*

1. *Если $\Theta_1, \Theta_2 \in K[x]$ — решение уравнения (3.3.2.5), то существуют многочлены $R, S, T, U \in K[x]$ такие, что*

$$\left(\begin{smallmatrix} R & S \\ T & U \end{smallmatrix}\right) \left[\begin{smallmatrix} \beta \\ 1 \end{smallmatrix}\right] = \beta, \quad \deg(RU + ST) > 0, \quad RU - ST \in K^*. \tag{3.3.2.7}$$

2. *Если существуют многочлены $R, S, T, U \in K[x]$ такие, что справедливы соотношения (3.3.2.7), то непрерывная дробь элемента β квазипериодическая*

3. *Если непрерывная дробь элемента β квазипериодическая и имеет вид (3.3.2.6), то существуют нетривиальные решения $\Theta_1, \Theta_2 \in K[x]$, $\Theta_2 \neq 0$, уравнения (3.3.2.5), причем, если Θ_1 обладает минимальной степенью среди нетривиальных решений, то*

$$\sum_{j=m}^{m+N-1} \deg a_j = \deg \Theta_1. \tag{3.3.2.8}$$

Доказательство. Определим

$$R = \Theta_1 - \Theta_2\Lambda_1, \quad S = -\Theta_2\Lambda_0, \tag{3.3.2.9}$$

$$T = \Theta_2\Lambda_2, \quad U = \Theta_1 + \Theta_2\Lambda_1, \tag{3.3.2.10}$$

тогда $R, S, T, U \in K[x]$, $T \neq 0$ и

$$RU - ST = \Theta_1^2 - \Theta_2^2\Lambda_1^2 + \Theta_2^2\Lambda_0\Lambda_2 = \Theta_1^2 - \Theta_2^2 d = \gamma \in K^*.$$

Будем использовать обозначение (3.3.2.1). Учитывая, что β является корнем (3.3.2.4), имеем

$$\left(\begin{smallmatrix} R & S \\ T & U \end{smallmatrix}\right)\left[\begin{smallmatrix} \beta \\ 1 \end{smallmatrix}\right] = \frac{(\Theta_1 - \Theta_2\Lambda_1)\beta - \Theta_2\Lambda_0 - \beta(\Theta_2\Lambda_2\beta + \Theta_1 + \Theta_2\Lambda_1)}{\Theta_2\Lambda_2\beta + \Theta_1 + \Theta_2\Lambda_1} + \beta =$$

$$= \frac{-\Theta_2(\Lambda_2\beta^2 + 2\Lambda_1\beta + \Lambda_0)}{\Theta_2\Lambda_2\beta + \Theta_1 + \Theta_2\Lambda_1} + \beta = \beta. \tag{3.3.2.11}$$

Пункт 1. доказан.

Подставим тождество (см. соотношение (3.1.1.5))

$$\beta = \left(\begin{smallmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{smallmatrix}\right)\left[\begin{smallmatrix} \beta_{j+1} \\ 1 \end{smallmatrix}\right] \tag{3.3.2.12}$$

в левую часть соотношения (3.3.2), тогда в силу леммы 3.3.2.1 получаем

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\left[\begin{smallmatrix} \beta_{j+1} \\ 1 \end{smallmatrix}\right] = \beta, \quad \text{где} \quad \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = \left(\begin{smallmatrix} R & S \\ T & U \end{smallmatrix}\right)\left(\begin{smallmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{smallmatrix}\right), \tag{3.3.2.13}$$

причем $A, B, C, D \in K[x]$ и с учетом (3.1.1.3) имеем

$$AD - BC = (RU - ST)(p_jq_{j-1} - p_{j-1}q_j) = (-1)^{j-1}\gamma \in K^*.$$

Поскольку $v_\infty^-(q_j\alpha - p_j) \geq -v_\infty(q_j)$ (по аналогии с (3.1.1.8) с помощью отображения φ из §3.1.3), то

$$v_\infty(D) = v_\infty(Tp_{j-1} + Uq_{j-1}) = v_\infty(T\alpha + U) + v_\infty(q_{j-1}) >$$

$$> v_\infty(T\alpha + U) + v_\infty(q_j) = v_\infty(Tp_j + Uq_j) = v_\infty(C). \tag{3.3.2.14}$$

По замечанию 3.1.6.2 существует номер $0 \leq m \leq 2$ такой, что элемент β_m является первым приведенным (см. §3.1.5) полным частным и $v_\infty^-(\beta_m) \leq -1$. Положим $j + 1 = m$, тогда по лемме 3.3.2.2 найдется номер $n > m$ такой, что для некоторого $r \in K^*$ выполнены равенства

$$\beta_m = (-1)^{n-1}(-1)^m\gamma r^{-2}\beta_{n+1}, \tag{3.3.2.15}$$

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = \left(\begin{smallmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{smallmatrix}\right)\left(\begin{smallmatrix} r & 0 \\ 0 & (-1)^{n-1}r^{-1}(-1)^m\gamma \end{smallmatrix}\right) =$$

$$= \left(\begin{smallmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{smallmatrix}\right)\prod_{i=m}^{n}\left(\begin{smallmatrix} a_i & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} r & 0 \\ 0 & (-1)^{n+1-m}r^{-1}\gamma \end{smallmatrix}\right). \tag{3.3.2.16}$$

Из (3.3.2.16) следует, что непрерывная дробь β квазипериодическая, причем длина квазипериода N делит $n + 1 - m$.

Пункт 2. доказан.

Из (3.3.2.12) при $j = m-1$ имеем

$$\beta_m = \left(\begin{smallmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{smallmatrix}\right)^{-1} \left[\begin{smallmatrix} \beta \\ 1 \end{smallmatrix}\right]. \tag{3.3.2.17}$$

Из (3.3.2.6) имеем $\beta_{m+N} = c\beta_m$, поэтому по лемме 3.3.2.1 с подстановкой (3.3.2.17) получаем

$$\beta = \left(\begin{smallmatrix} p_{m+N-1} & p_{m+N-2} \\ q_{m+N-1} & q_{m+N-2} \end{smallmatrix}\right) \left[\begin{smallmatrix} \beta_{m+N} \\ 1 \end{smallmatrix}\right] = \left(\begin{smallmatrix} p_{m+N-1} & p_{m+N-2} \\ q_{m+N-1} & q_{m+N-2} \end{smallmatrix}\right) \left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right) \left[\begin{smallmatrix} \beta_m \\ 1 \end{smallmatrix}\right] =$$
$$= \left(\begin{smallmatrix} p_{m+N-1} & p_{m+N-2} \\ q_{m+N-1} & q_{m+N-2} \end{smallmatrix}\right) \left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{smallmatrix}\right)^{-1} \left[\begin{smallmatrix} \beta \\ 1 \end{smallmatrix}\right],$$

то есть существуют $R^*, S^*, T^*, U^* \in K[x]$ такие, что

$$\left(\begin{smallmatrix} R^* & S^* \\ T^* & U^* \end{smallmatrix}\right) \left[\begin{smallmatrix} \beta \\ 1 \end{smallmatrix}\right] = \beta, \quad R^*U^* - S^*T^* = (-1)^N c = \gamma^* \in K^*, \tag{3.3.2.18}$$

причем

$$\left(\begin{smallmatrix} R^* & S^* \\ T^* & U^* \end{smallmatrix}\right) \left(\begin{smallmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{smallmatrix}\right) = \left(\begin{smallmatrix} p_{m+N-1} & p_{m+N-2} \\ q_{m+N-1} & q_{m+N-2} \end{smallmatrix}\right) \left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right). \tag{3.3.2.19}$$

Первое равенство (3.3.2.18) равносильно уравнению $T^*\beta^2 + (U^* - R^*)\beta - S^* = 0$. Так как β является корнем (3.3.2.4) и многочлены $\Lambda_0, \Lambda_1, \Lambda_2 \in K[x]$ взаимно простые, то существует многочлен $\Theta_2^* \in K[x]$ такой, что

$$T^* = \Theta_2^*\Lambda_2, \quad U^* - R^* = 2\Theta_2^*\Lambda_1, \quad S^* = -\Theta_2^*\Lambda_0. \tag{3.3.2.20}$$

Из второго равенства (3.3.2.18) с помощью соотношений (3.3.2.20) следует, что квадратное уравнение $X^2 + 2\Lambda_1\Theta_2^*X + \Lambda_0\Lambda_2(\Theta_2^*)^2 = \gamma^*$ имеет решение $R^* \in K[x]$, значит сокращенный дискриминант этого уравнения является полным квадратом, который обозначим $(\Theta_1^*)^2$, где $\Theta_1^* \in K[x]$:

$$\Lambda_1^2(\Theta_2^*)^2 - \Lambda_0\Lambda_2(\Theta_2^*)^2 - \gamma^* = d(\Theta_2^*)^2 - \gamma^* = (\Theta_1^*)^2,$$

Следовательно, пара многочленов Θ_1^*, Θ_2^* является решением уравнения типа Пелля $(\Theta_1^*)^2 - d(\Theta_2^*)^2 = \gamma^* \in K^*$ и справедливо равенство $R^* = \Theta_1^* - \Lambda_1\Theta_2^*$.

Остается показать, что если непрерывная дробь β имеет вид (3.3.2.6) и $\Theta_1, \Theta_2 \in K[x]$, $\Theta_2 \neq 0$, нетривиальное решение уравнения (3.3.2.5), для которого справедливы соотношения (3.3.2.9)-(3.3.2.16) и $n + 1 - m = kN$, $k \geq 2$, то для полученного "минимального" решения Θ_1^*, Θ_2^* справедливо неравенство $\deg\Theta_1^* < \deg\Theta_1$.

Из (3.3.2.19) по аналогии с (3.3.2.14) имеем

$$v_\infty(p_{m+N-1}) = v_\infty(R^*p_{m-1} + S^*q_{m-1}) = v_\infty^-(R^*\beta + S^*) + v_\infty(q_{m-1}).$$

Без ограничения общности предположим, что корень β уравнения (3.3.2.4) имеет вид $\beta = (-\Lambda_1 + \sqrt{d})/\Lambda_2$, тогда справедливы равенства

$$R^*\beta + S^* = \frac{1}{\Lambda_2}\big(\Theta_1^*(-\Lambda_1 + \sqrt{d}) - \Lambda_1\Theta_2^*(-\Lambda_1 + \sqrt{d}) - \Lambda_0\Lambda_2\Theta_2^*\big) =$$
$$= \frac{1}{\Lambda_2}\big(\Theta_1^*(-\Lambda_1 + \sqrt{d}) + \Theta_2^*(-\Lambda_1\sqrt{d} + d)\big) = \frac{-\Lambda_1 + \sqrt{d}}{\Lambda_2}(\Theta_1^* + \Theta_2^*\sqrt{d}) = \beta U^*.$$

Следовательно, степень единицы $U^* = \Theta_1^* + \Theta_2^*\sqrt{d}$ равна

$$\deg \Theta_1^* = \deg U^* = -v_\infty^-(U^*) = v_\infty^-(\beta) - v_\infty^-(R^*\beta + S^*) =$$
$$= v_\infty^-(\beta) - v_\infty(p_{m+N-1}) + v_\infty(q_{m-1}) = v_\infty(p_{m-1}) - v_\infty(p_{m+N-1}).$$

Аналогичным образом для единицы $U = \Theta_1 + \Theta_2\sqrt{d}$ имеем

$$\deg \Theta_1 = \deg U = -v_\infty^-(U) = v_\infty^-(\beta) - v_\infty^-(R\beta + S) = \tag{3.3.2.21}$$
$$= v_\infty^-(\beta) - v_\infty(p_{m+kN-1}) + v_\infty(q_{m-1}) = v_\infty(p_{m-1}) - v_\infty(p_{m+kN-1}). \tag{3.3.2.22}$$

Значит, с учетом (3.1.1.7) получаем $\deg \Theta_1^* < \deg \Theta_1$. Таким образом, если как в условии пункта 3. решение Θ_1, Θ_2 с минимальной степенью Θ_1, то это решение с точностью до постоянного множителя совпадает с решением Θ_1^*, Θ_2^*. Следовательно, в веденных выше обозначениях $k = 1$, и равенство (3.3.2.8) следует из (3.3.2.22).

Теорема 3.3.2.3 доказана. □

Следствие 3.3.2.4. *Пусть существует решение $\Theta_1, \Theta_2 \in K[x]$, $\Theta_2 \neq 0$, уравнения (3.3.2.5) и непрерывная дробь элемента β, являющегося корнем уравнения (3.3.2.4), имеет вид (3.3.2.6), где N — длина квазипериода. Тогда справедливы неравенства*

$$\frac{\deg \Theta_1}{r} \leq N \leq \deg \Theta_1,$$

где $r = \max\big(\deg \Lambda_0, \deg \Lambda_1, \deg \Lambda_2\big)$.

Доказательство. Доказательство следует из теоремы 3.3.2.3 и оценок на степень неполных частных a_j из предложения 3.1.3.1. □

Теорема 3.3.2.5. *Элемент $\beta = \sqrt{f}/x^s \in \mathcal{L}$ для некоторого $s \in \mathbb{Z}$ имеет периодическое разложение в непрерывную дробь тогда и только тогда, когда существуют многочлены $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$, которые удовлетворяют условиям (3.2.3.1) для некоторого $b \in K^*$ и $-v_x(\Omega_3) \leq s \leq v_x(\Omega_3) + v_x(f_1)$. В случае периодичности непрерывной дроби элемента β для длины квазипериода N справедливы оценки*

$$N \leq \begin{cases} 2\big(\deg \Omega_3 + s + 1\big), & \text{если } \ s + g + 1 < \deg f_1, \\ 2\big(\deg \Omega_3 + \deg f_1 - g\big) - 1, & \text{если } \ s + g + 1 = \deg f_1, \\ 2\big(\deg \Omega_3 - g\big), & \text{если } \ \deg f_1 < s + g + 1 < \deg f, \\ 2\big(\deg \Omega_3 + \deg f_1 - g\big) - 1, & \text{если } \ s + g + 1 = \deg f, \\ 2\big(\deg \Omega_3 + \deg f_1 - s + 1\big), & \text{если } \ \deg f < s + g + 1, \end{cases}$$

где $\deg f = 2g + 2$.

Доказательство. Пусть существуют многочлены $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$, удовлетворяющие условиям (3.2.3.1) для некоторого $b \in K^*$, и дано $s \in \mathbb{Z}$ такое, что $-v_x(\Omega_3) \leq s \leq v_x(\Omega_3) + v_x(f_1)$.

Тогда по предложению 3.2.3.3 непрерывные дроби элементов из (3.2.3.5) периодические, и, в частности, периодическая непрерывная дробь элемента β.

Пусть теперь непрерывная дробь элемента β периодическая. Тогда по теореме 2 [118] существуют многочлены $\Theta_1, \Theta_2 \in K[x]$, являющиеся решением уравнения (3.3.2.5), где D — дискриминант элемента β, $D = \omega^2 f$. Без ограничения общности мы можем считать, что многочлены Θ_1, Θ_2 имеют минимальную степень среди возможных нетривиальных решений уравнения (3.3.2.5) при разных $\gamma \in K^*$. Имеем $\omega = x^{|s|}$ при $v_x(f) = 0$ или $s \leq 0$, и $\omega = x^{|s|-1}$ при $v_x(f) = 1$ и $s > 0$.

Если $v_x(\Theta_2^2 D) = 0$, то $s = 0$, $D = f$, и в качестве многочленов $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$ можно взять

$$f_1 = -1/\gamma, \quad f_2 = -f/\gamma, \quad \Omega_3 = \Theta_1, \quad \Omega_4 = \Theta_2,$$

тогда $b = -1/\gamma$ и справедливы условия (3.2.3.1).

Рассмотрим теперь случай $v_x(\Theta_2^2 D) > 0$. Тогда $\gamma = b^{-2}$ для некоторого $b \in K^*$, причем можно выбрать знак у постоянной b так, что

$$b^2\Theta_2^2 D = b^2\Theta_1^2 - 1 = \big(b\Theta_1 - 1\big)\big(b\Theta_1 + 1\big), \quad v_x(b\Theta_1 - 1) > 0.$$

Поскольку $\big(b\Theta_1 - 1,\ b\Theta_1 + 1\big) \in K^*$, то существуют многочлены $f_1, f_2, \Omega_3, \Omega_4 \in K[x]$, удовлетворяющие условиям

$$b\Theta_1 - 1 = 2\Omega_3^2 f_1, \quad b\Theta_1 + 1 = 2\Omega_4^2 f_2, \quad \Theta_2\omega = 2\Omega_3\Omega_4, \quad b^2 f = f_1 f_2.$$

Заметим, что $\deg f_2 > 0$, поскольку в противном случае при $f_2 \in K^*$ многочлены $\Omega_4, \Omega_3/\omega$ также являются решением уравнения типа (3.3.2.5), но меньшей степени, чем решение Θ_1, Θ_2. Таким образом, для многочленов $f_1, f_2, \Omega_3, \Omega_4$ справедливы условия (3.2.3.1) и $-v_x(\Omega_3) \leq s \leq v_x(\Omega_3) + v_x(f_1)$, поскольку многочлен ω делит Ω_3.

Перейдем к доказательству оценки на длину квазипериода N.

По предложению 3.2.3.3 непрерывные дроби элементов из (3.2.3.4) и (3.2.3.5) периодические, причем по лемме 3.2.3.2 периоды для элементов из (3.2.3.4) и (3.2.3.5) соответственно совпадают с точностью до сдвига и умножения на некоторую постоянную. Следовательно, среди неполных частных непрерывной дроби β, входящих в квазипериодическую часть, найдутся неполные частные каждой положительной степени из $-v_\infty^-(\alpha)$ для элементов α из (3.2.3.5). Значит, степени некоторых неполных частных a_j можно оценить сверху более точно значениями $\max\big(1, |g + 1 - s|\big)$, $\max\big(1, |s + g + 1 - \deg f_1|\big)$. Обозначим

$$\delta = \max\big(0, |g + 1 - s| - 1\big) + \max\big(0, |s + g + 1 - \deg f_1| - 1\big), \tag{3.3.2.23}$$

тогда $0 \leq \delta \leq 2\max(s - 1, g)$ и справедлива оценка

$$\deg A \geq \deg P_t = \sum_{j=0}^{t} \deg a_j \geq \deg P_{n-1} + N + \delta. \tag{3.3.2.24}$$

Далее, по предложению 3.3.2.3, для элемента $\beta = \sqrt{f}/x^s$ получаем

$$N + \delta \le \max\left(\deg \Theta_1,\ \deg \Theta_2 + \frac{\deg \Lambda_0 + \deg \Lambda_2}{2}\right) = \deg \Theta_1 \le 2 \deg \Omega_3 + \deg f_1.$$

Далее, раскрывая значение модулей в δ, получаем требуемые оценки на длину квазипериода N.

Теорема 3.3.2.5 доказана. □

Из предложения 3.2.3.3 и теоремы 3.3.2.5 следует, что для "ключевых" элементов вида $\sqrt{f}/x^s$ условие квазипериодичности непрерывной дроби, построенной в поле $K((1/x))$, эквивалентно условию ее периодичности. Это следствие эквивалентно результату, полученному впервые в статье [142] о периодичности непрерывных дробей, построенных в поле $K((x))$, для "ключевых" элементов вида $\sqrt{f}/x^s$.

Из оценок теоремы 3.3.2.5 на длину квазипериода N следует, что для любых $s \in \mathbb{Z}$ справедливо неравенство $N \le 2\deg(\Omega_3 + \deg f_1 - g)$. В случае, когда многочлен f неприводим, имеем $f_1 \in K^*$ и длина квазипериода N не превосходит $2(\deg \Omega_3 - g)$.

3.3.3. Оценка сверху длин периодов непрерывных дробей ключевых элементов над полями алгебраических чисел

Пусть в поле $\mathcal{L} = K(x)(\sqrt{f})$ существует фундаментальная единица $\Psi_1 + \Psi_2\sqrt{f}$, где $\Psi_1, \Psi_2 \in K[x]$. Для $j \in \mathbb{N}$ положим $\Omega_1^{(j)}, \Omega_2^{(j)} \in K[x]$ такие многочлены, что

$$\Omega_1^{(j)} + \Omega_2^{(j)}\sqrt{f} = \left(\Psi_1 + \Psi_2\sqrt{f}\right)^j. \tag{3.3.3.1}$$

Положим $Z = \Psi_2^2 f/\Psi_1^2$, тогда

$$\Omega_1^{(j)} + \Omega_2^{(j)}\sqrt{f} = \Psi_1^j\left(T_j(Z) + Q_j(Z)\sqrt{Z}\right), \tag{3.3.3.2}$$

где многочлены $T_n(x), Q_n(x) \in \mathbb{Z}[x]$, $n \in \mathbb{N}$, определены в (3.3.1.1).

Предложение 3.3.3.1. *Пусть $\beta \in \mathcal{L}$ — квадратичная иррациональность с дискриминантом $D(\beta) = \omega^2 f \in K[x]$. Для того, чтобы разложение элемента β в непрерывную дробь в поле $K((1/x))$ было квазипериодическим, необходимо и достаточно, чтобы нашелся номер $n \in \mathbb{N}$ такой, что $\omega \mid \Omega_2^{(n)}$.*

Доказательство. Согласно теореме 2 [118] элемент β имеет квазипериодическую непрерывную дробь в поле $K((1/x))$ тогда и только тогда, когда для дискриминанта $D(\beta) = \omega^2 f$ справедливо соотношение (3.3.2.5) для некоторых ненулевых многочленов $\Theta_1, \Theta_2 \in K[x]$. Так как в поле $\mathcal{L}$ есть фундаментальная единица $\Psi_1 + \Psi_2\sqrt{f}$, то без ограничения общности можно считать, что разрешимость соотношения (3.3.2.5) в многочленах Θ_1, Θ_2 равносильна для некоторого $n \in \mathbb{N}$ равенствам $\Theta_1 = \Omega_1^{(n)}$, $\Theta_2\omega = \Omega_2^{(n)}$, где многочлены $\Omega_1^{(n)}$, $\Omega_2^{(n)}$ определе-

ны в (3.3.3.1). Таким образом, необходимым и достаточным условием квазипериодичности непрерывной дроби элемента β является $\omega \mid \Omega_2^{(n)}$ для некоторого $n \in \mathbb{N}$. $\square$

Пусть выполнены условия предложения 3.3.3.1, и число a является корнем многочлена ω. Необходимым условием того, что $\omega \mid \Omega_2^{(n)}$ является условие $\Omega_2^{(n)}(a) = 0$, которое согласно (3.3.3.2) равносильно условию

$$\lim_{x \to a} \Psi_1^{n-1}(x) \cdot \Psi_2(x) \cdot Q_n(Z) = 0, \quad \text{где} \quad Z = Z(x) = \Psi_2^2(x) f(x) / \Psi_1^2(x).$$

Обозначим $Q_n(Z, W)$ — однородный многочлен, соответствующий многочлену $Q_n(Z)$. Если $\Psi_1(a) = 0$, то $Q_n\big(\Psi_2^2(a)f(a), \Psi_1^2(a)\big) \neq 0$, поскольку $\Psi_2^2(a)f(a) \neq 0$, ибо $\Psi_1^2(x) - \Psi_2^2(x)f(x) \in K^*$. Таким образом, для квазипериодичности непрерывной дроби элемента β с дискриминантом $D(\beta) = \omega^2 f$ необходимо, чтобы для каждого корня a многочлена ω либо $\Psi_1(a) = 0$, либо $\Psi_2(a) = 0$, либо $Q_n(Z_a) = 0$, где $Z_a = Z(a)$ при $\Psi_1(a) \neq 0$. В случае, если у многочлена ω нет кратных корней, то приведенные необходимые условия являются также достаточными.

Предложение 3.3.3.2. *Пусть $\mathcal{L} = K(x)(\sqrt{f})$ — гиперэллиптическое поле, в котором есть фундаментальная единица $\Psi_1 + \Psi_2\sqrt{f}$ такая, что $\Psi_1^2 - \Psi_2^2 f = \gamma \in K^*$. Пусть элемент α поля $\mathcal{L}$ имеет дискриминант $D = D(\alpha) = \omega^2 f$. Тогда следующие условия равносильны:*

1. *непрерывная дробь элемента α квазипериодическая;*

2. *найдется такое число $n \in \mathbb{N}$, что*

$$\omega(x) \mid \Psi_2(x) \sum_{j \le \left[\frac{n-1}{2}\right]} \binom{n}{2j+1} \Psi_1(x)^{n-2j-1} (\Psi_1(x)^2 - \gamma)^j.$$

Доказательство. В силу предложения 3.3.3.1 условие квазипериодичности непрерывной дроби элемента α равносильно условию $\omega \mid \Omega_2^{(n)}$ для некоторого $n \in \mathbb{N}$. Из равенств (3.3.3.2) и (3.3.1.19) имеем

$$\Omega_2^{(n)}(x) = \Psi_1^n(x) Q_n\left(\frac{\Psi_2^2(x)}{\Psi_1^2(x)} f(x)\right) \frac{\Psi_2(x)}{\Psi_1(x)} =$$

$$= \frac{1}{2} \frac{\Psi_2(x)}{\sqrt{\Psi_1(x)^2 - \gamma}} \Big(\big(\Psi_1(x) + \sqrt{\Psi_1(x)^2 - \gamma}\big)^n - \big(\Psi_1(x) - \sqrt{\Psi_1(x)^2 - \gamma}\big)^n \Big) =$$

$$= \frac{\Psi_2(x)}{\Psi_1(x)} \sum_{j \le \left[\frac{n-1}{2}\right]} \binom{n}{2j+1} \Psi_1(x)^{n-2j} (\Psi_1(x)^2 - \gamma)^j.$$

Предложение 3.3.3.2 доказано. $\square$

Теорема 3.3.3.3. *Пусть K — расширение поля рациональных чисел $\mathbb{Q}$ степени k. Пусть $f \in K[x]$ — свободный от квадратов многочлен, и в кольце целых элементов поля $\mathcal{L} = K(x)(\sqrt{f})$ есть фундаментальная единица $u = \Psi_1 + \Psi_2\sqrt{f}$ степени m, где $\Psi_1, \Psi_2 \in K[x]$. Пусть для $j \in \mathbb{N}$ многочлены $\Omega_1^{(j)}, \Omega_2^{(j)} \in K[x]$ определены соотношениями (3.3.3.1).*

1. *Если хотя бы одно из значений* $v_x(f), v_x(\Psi_1), v_x(\Psi_2)$ *отлично от нуля, то непрерывная дробь элемента* $\sqrt{f}/x^s$, *построенная в* $K((1/x))$, *периодическая тогда и только тогда, когда*

$$-v_x(\Psi_1) - v_x(\Psi_2) \le s \le v_x(\Psi_1) + v_x(\Psi_2) + v_x(f).$$

В случае периодичности непрерывной дроби $\sqrt{f}/x^s$, *длина квазипериода* N *не превосходит* $m - \delta$, *где значение* δ *определено в* (3.3.2.23) *при некотором* $f_1 \mid f$, $\deg f_1 < \deg f$.

2. *Если* $v_x(f) = v_x(\Psi_1) = v_x(\Psi_2) = 0$, *то непрерывная дробь элемента* $\sqrt{f}/x^s$, *построенная в* $K((1/x))$, *периодическая тогда и только тогда, когда найдется такой номер* n, *что* $v_x\left(\Omega_2^{(1)}\right) = \ldots = v_x\left(\Omega_2^{(n-1)}\right) = 0$, $|s| \le v_x\left(\Omega_2^{(n)}\right)$ *и* $\varphi(n) \mid 2k$. *В случае периодичности непрерывной дроби* $\sqrt{f}/x^s$, *длина квазипериода* N *не превосходит* $nm - \delta$, *где значение* δ *определено в* (3.3.2.23) *при некотором* $f_1 \mid f$, $\deg f_1 < \deg f$.

Доказательство. Пункт 1 следует из результатов теоремы 3.2.1.3 (см. также теорему 4.2.4.1 и [13]).

Предположим, что $v_x(f) = v_x(\Psi_1) = v_x(\Psi_2) = 0$. Положим $Z = Z(x) = \Psi_2^2 f/\Psi_1^2$, тогда для всех $n \in \mathbb{N}$ справедливо равенство (3.3.3.2). Отметим, что $Z_0 = Z(0)$ определено корректно, поскольку $\Psi_1(0) \ne 0$. Согласно предложению 3.3.3.1 для периодичности элемента $\sqrt{f}/x^s$, $s \ne 0$ необходимо, чтобы для некоторого минимального $n \in \mathbb{N}$ было выполнено равенство $Q_n(Z)|_{x=0} = 0$, то есть число Z_0 должно быть корнем многочлена $Q_j(x)$. В силу минимальности n, число Z_0 не должно быть корнем многочленов $Q_1(x), \ldots, Q_{n-1}(x)$. По теореме 3.3.1.12 число Z_0 должно быть корнем либо многочлена $P(T_{n/2})$ при четном n, либо многочлена $\tilde{P}(T_n)$ при нечетном n, поскольку остальные неприводимые над $\mathbb{Q}$ множители в разложении (3.3.1.16) содержатся в соответствующих разложениях на неприводимые над $\mathbb{Q}$ множители многочленов $Q_1(x), \ldots, Q_{n-1}(x)$. По следствию 3.3.1.13 при четном $n = 2^t q$, $t \ge 1$, имеем $\deg P(T_{n/2}) = 2^{t-2}\varphi(q)$, при нечетном $n = q$ имеем $\deg \tilde{P}(T_n) = \varphi(q)/2$, откуда в силу неприводимости соответственно многочленов $P(T_{n/2})$ и $\tilde{P}(T_n)$ получаем условие $\varphi(n) \mid 2k$. Более того, поле K в качестве подполя должно содержать поле разложения соответственно многочлена $P(T_{n/2})$ или многочлена $\tilde{P}(T_n)$.

Из оценок на длину квазипериода в теоремах 3.3.2.3 и 3.3.2.4 следует, что $N \le \deg \Theta_1 - \delta = \deg \Omega_1^{(n)} - \delta = nm - \delta$.

Теорема 3.3.3.3 доказана. □

По теореме 3.3.3.3 из условия $\varphi(n) \mid 2k$ получаем в таблице 3.1 возможные значения n для различных значений $k = [K : \mathbb{Q}]$, $k \le 10$. В статье [13] доказано, что при $k = 1$ все соответствующие значения n из таблицы 3.1 достигаются. Примеры 3.3.7.2-3.3.7.5 ниже показывают, что при $k = 2$ также достигаются все соответствующие значения n из таблицы

Таблица 3.1: Возможные значения n из теоремы 3.3.3.3 для различных значений $k = [K : \mathbb{Q}] \leq 10$.

$k = [K : \mathbb{Q}]$	Множество значений n
1	$1, 2, 3, 4, 6$
2	$1, \ldots, 6, 8, 10, 12$
3	$1, 2, 3, 4, 6, 7, 9, 14, 18$
4	$1, \ldots, 6, 8, 10, 12, 15, 16, 20, 24, 30$
5	$1, 2, 3, 4, 6, 11, 22$
6	$1, \ldots, 10, 12, 13, 14, 18, 21, 26, 28, 36, 42$
7	$1, 2, 3, 4, 6$
8	$1, \ldots, 10, 12, 13, 14, 18, 21, 26, 28, 36, 42$
9	$1, 2, 3, 4, 6, 7, 9, 14, 18, 19, 27, 38, 54$
10	$1, \ldots, 6, 8, 10, 11, 12, 22, 25, 33, 44, 50, 66$

3.1. В частности, пример 3.3.7.5 показывает, что существуют примеры элементов вида $\sqrt{f}/x^s$, определенные над полем K, $[K : \mathbb{Q}] = 2$, длина квазипериода непрерывных дробей которых почти в 12 раз больше степени соответствующей фундаментальной единицы.

Следствие 3.3.3.4. *Пусть $s \in \mathbb{Z}$ и гиперэллиптическое поле $\mathcal{L} = \mathbb{Q}(X)(\sqrt{F})$ содержит фундаментальную S_∞-единицу степени m, где $S_\infty = \{v_\infty^-, v_\infty^+\}$. Если длина квазипериода непрерывной дроби $\sqrt{F}/X^s$ конечна, то она не превосходит $6m - \delta$, а длина периода не превосходит $12m - 2\delta$, где значение δ определено в (3.3.2.23) при некотором $f_1 \mid f$, $\deg f_1 < \deg f$.*

Доказательство. Из теоремы 3.3.3.3 и таблицы 3.1 при $K = \mathbb{Q}$ имеем $n \leq 6$. □

В статье [14] приведен пример эллиптического поля $\mathcal{L} = \mathbb{Q}(X)(\sqrt{F})$, $\deg F = 4$, в котором есть фундаментальная S_∞-единица степени 4, квазипериод непрерывной дроби элемента $\sqrt{F}/X$ совпадает с периодом и равен 20, квазипериод непрерывной дроби элемента $\sqrt{F}/X^2$ равен 19, а период — 38 (см. этот и другие примеры в §3.3.4). Таким образом, для многочленов F четной степени длины периодов непрерывных дробей вида $\sqrt{F}/X^s$ могут значительно превышать степень фундаментальной S_∞-единицы.

В следующем следствии в случае $K = \mathbb{Q}$ найдены оценки длин периодов непрерывных дробей, построенных в поле формальных степенных рядов $\mathbb{Q}((x))$.

Следствие 3.3.3.5. *Пусть $f \in \mathbb{Q}[x]$ — свободный от квадратов многочлен, и $h \in \mathbb{Q}[x]$ — линейный многочлен. Пусть $u_h = h^{-m}(\mu_1 + \mu_2\sqrt{f})$ — фундаментальная S_h-единица в поле $L = \mathbb{Q}(x)(\sqrt{f})$.*

Для $\deg f = 2g + 1$ непрерывная дробь $\sqrt{f}/h^{s_0}$ квазипериодическая тогда и только тогда, когда $s_0 \in \mathbb{Z}$ удовлетворяет неравенству $|s_0 - g - 1/2| \leq \deg \mu_1 - \deg \mu_2 - g$, причем в случае

квазипериодичности непрерывная дробь $\sqrt{f}/h^{s_0}$ *является периодической, длина квазипериода не превосходит* m*, длина периода не превосходит* $2m$*.*

Для $\deg f = 2g+2$ *положим*

$$u_h^n = h^{-nm}(\mu_1^{(n)} + \mu_2^{(n)}\sqrt{f}), \quad r_n = \left|\deg \mu_1^{(n)} - \deg \mu_2^{(n)} - g - 1\right|.$$

1. *Если* $r_1 \neq 0$*, то элементы вида* $\sqrt{f}/h^{s_0}$ *имеют квазипериодическое разложение в непрерывную дробь тогда и только тогда, когда* $g+1-r_1 \leq s_0 \leq g+1+r_1$*, причем в случае квазипериодичности непрерывная дробь* $\sqrt{f}/h^{s_0}$ *является периодической, длина квазипериода не превосходит* m*, длина периода не превосходит* $2m$*.*

2. *Если* $r_1 = 0$*,* $r_2 \neq 0$*, то элементы вида* $\sqrt{f}/h^{s_0}$ *имеют квазипериодическое разложение в непрерывную дробь тогда и только тогда, когда* $g+1-r_2 \leq s_0 \leq g+1+r_2$*, причем в случае квазипериодичности непрерывная дробь* $\sqrt{f}/h^{s_0}$ *является периодической, длина квазипериода не превосходит* $4m$*, длина периода не превосходит* $8m$*.*

3. *Если* $r_1 = r_2 = 0$*, то элементы вида* $\sqrt{f}/h^{s_0}$ *имеют квазипериодическое разложение в непрерывную дробь тогда и только тогда, когда* $g+1-r_3 \leq s_0 \leq g+1+r_3$*, причем в случае квазипериодичности непрерывная дробь* $\sqrt{f}/h^{s_0}$ *является периодической, длина квазипериода не превосходит* $6m$*, длина периода не превосходит* $12m$*.*

Доказательство. Доказательство следует из теоремы 3.3.3.3 и связи непрерывных дробей, построенных в полях формальных степенных рядов $\mathbb{Q}((1/x))$ и $\mathbb{Q}((x))$ (см. §3.1.3). □

Следствие 3.3.3.6. *Пусть справедливы обозначения теоремы 3.3.3.3, и непрерывная дробь элемента* $\sqrt{f}/x^s$ *периодическая. Пусть дополнительно выполнено одно из трех условий: либо* $v_x(\Psi_1) > 0$*, либо* $v_x(f) = v_x(\Psi_1) = v_x(\Psi_2) = 0$*, и* n *четно, либо* $v_x(f) = v_x(\Psi_1) = v_x(\Psi_2) = 0$ *и многочлен* f *неприводим. Тогда справедливы неравенства*

$$N \leq \begin{cases} mn - 2g, & \text{если } |s| < g+1, \\ mn - 2g - 1, & \text{если } |s| = g+1, \\ mn - 2|s| - 2, & \text{если } |s| > g+1. \end{cases}$$

Доказательство. Если $v_x(\Psi_1) > 0$ или многочлен f неприводим или n четно, то $f_1 \in K^*$. Следовательно, из (3.3.2.23) имеем $\delta = 2g$ при $|s| < g+1$, $\delta = 2g+1$ при $|s| = g+1$, $\delta = 2|s|+2$ при $|s| > g+1$. □

Отметим, что следствие 3.3.3.5 уточняет оценку длины квазипериода в статье [62] для элементов вида $\sqrt{F} - M$, $\deg M \leq g+1$, $\deg(F - M^2) \leq g+1$, $g \geq 2$, для непрерывных дробей в $K((1/X))$ или для элементов вида $(\sqrt{f} - V)/h^{g+1}$, где $h^{g+1} \mid f - V^2$, $\deg V \leq g+1$, $g \geq 2$, для непрерывных дробей в $K((h))$.

3.3.4. Примеры элементов, имеющих большую длину периода

Приведем несколько примеров, показывающих эффективность и точность найденных в §3.3.3 оценок.

Пример 3.3.4.1. *Рассмотрим* $F = X^4 + 20X^3 + 124X^2 + 144X - 432$. *Непрерывная дробь элемента* $\sqrt{F}$ *в* $\mathbb{Q}((1/X))$ *имеет вид*

$$\sqrt{F} = \Big[X^2 + 10X + 12;\ \overline{-\tfrac{X}{48} - \tfrac{1}{12},\ 4X + 16,\ -\tfrac{X^2}{96} - \tfrac{5X}{48} - \tfrac{1}{8},\ 4X + 16,\ -\tfrac{X}{48} - \tfrac{1}{12},\ 2X^2 + 20X + 24}\Big].$$

Длина квазипериода равна 3, коэффициент квазипериода равен $-1/96$, *длина периода равна 6. В поле* $\mathcal{L}$ *существует фундаментальная единица степени* $m = 4$, *порядок класса дивизора* $(\infty^- - \infty^+)$ *в группе классов дивизоров* $\Delta^\circ(L)$ *равен 4. Заметим, что* $\operatorname{tc}(p_3) \neq 0$, $\operatorname{tc}(q_3) \neq 0$, *поэтому в обозначениях следствия 3.3.3.5 имеем* $r_1 = 0$, *но* $\operatorname{tc}(p_3)^2 + 3\operatorname{tc}(F)\operatorname{tc}(q_3)^2 = 0$, *поэтому* $\operatorname{tc}\left(\mu_1^{(3)}\right) = 0$, *следовательно, непрерывная дробь элемента* $\sqrt{F}/X$ *периодическая*

$$\sqrt{F}/X = \Big[X + 10;\ \overline{\tfrac{X}{12} + \tfrac{1}{3},\ \tfrac{X^2}{4} + X - 3,\ -\tfrac{X}{6} - \tfrac{5}{3},\ -\tfrac{X}{2} - 1,\ \tfrac{X}{2} + 4,\ \tfrac{X}{6} - \tfrac{1}{3},\ -\tfrac{X}{2} - 5,\ -\tfrac{X}{12} - \tfrac{1}{12},\ 4X + 28,\ \tfrac{X^3}{384} + \tfrac{5X^2}{192} + \tfrac{X}{32} - \tfrac{1}{8},\ 4X + 28,\ -\tfrac{X}{12} - \tfrac{1}{12},\ -\tfrac{X}{2} - 5,\ \tfrac{X}{6} - \tfrac{1}{3},\ \tfrac{X}{2} + 4,\ -\tfrac{X}{2} - 1,\ -\tfrac{X}{6} - \tfrac{5}{3},\ \tfrac{X^2}{4} + X - 3,\ \tfrac{X}{12} + \tfrac{1}{3},\ 2X + 20}\Big].$$

Длина периода совпадает с длиной квазипериода и равна $20 < 6m - 2g$.

Пример 3.3.4.2. *Рассмотрим* $F = X^4 + 36X^3 + 420X^2 + 1472X - 256$. *Непрерывная дробь элемента* $\sqrt{F}$ *в* $\mathbb{Q}((1/X))$ *имеет вид*

$$\sqrt{F} = \Big[X^2 + 18X + 48;\ \overline{-\tfrac{X}{128} - \tfrac{1}{16},\ 4X + 32,\ -\tfrac{X^2}{256} - \tfrac{9X}{128} - \tfrac{3}{16},\ 4X + 32,\ -\tfrac{X}{128} - \tfrac{1}{16},\ 2X^2 + 36X + 96}\Big].$$

Длина квазипериода равна 3, коэффициент квазипериода равен $-1/256$, *длина периода равна 6. В поле* $\mathcal{L}$ *существует фундаментальная единица степени* $m = 4$, *порядок класса дивизора* $(\infty^- - \infty^+)$ *в группе классов дивизоров* $\Delta^\circ(L)$ *равен 4. Заметим, что* $\operatorname{tc}(p_3) \neq 0$, $\operatorname{tc}(q_3) \neq 0$, *поэтому в обозначениях следствия 3.3.3.5 имеем* $r_1 = 0$, *но* $\operatorname{tc}(p_3)^2 + \operatorname{tc}(F)\operatorname{tc}(q_3)^2 = 0$, *поэтому* $\operatorname{tc}\left(\mu_1^{(2)}\right) = 0$, *следовательно, непрерывная дробь элемента* $\sqrt{F}/X$ *периодическая*

$$\sqrt{F}/X = \Big[X + 18;\ \overline{\tfrac{X}{48} + \tfrac{1}{18},\ -\tfrac{27X}{8} - \tfrac{153}{4},\ \tfrac{2X}{81} + \tfrac{4}{81},\ \tfrac{81X}{64} + \tfrac{729}{32},\ \tfrac{4X}{81} + \tfrac{16}{81},\ -\tfrac{81X}{64} - \tfrac{243}{16},\ -\tfrac{X^3}{648} - \tfrac{X^2}{36} - \tfrac{2X}{27} + \tfrac{16}{81},\ -\tfrac{81X}{64} - \tfrac{243}{16},\ \tfrac{4X}{81} + \tfrac{16}{81},\ \tfrac{81X}{64} + \tfrac{729}{32},\ \tfrac{2X}{81} + \tfrac{4}{81},\ -\tfrac{27X}{8} - \tfrac{153}{4},\ \tfrac{X}{48} + \tfrac{1}{18},\ 2X + 36}\Big].$$

Длина периода совпадает с длиной квазипериода и равна $14 = 4m - 2g$.

Пример 3.3.4.3. *Рассмотрим* $F = (X+6)\left(X^3 - 2X^2 + 32X - 32\right)$. *Непрерывная дробь элемента* $\sqrt{F}$ *в* $\mathbb{Q}((1/X))$ *имеет вид*

$$\sqrt{F} = \left[X^2 + 2X + 8;\ \overline{\tfrac{X}{64} + \tfrac{1}{16},\ 4X - 16,\ \tfrac{X}{64} + \tfrac{1}{16},\ 2X^2 + 4X + 16}\right].$$

Длина периода совпадает с длиной квазипериода и равна 4. В поле $\mathcal{L}$ *существует фундаментальная единица степени* $m = 5$, *порядок класса дивизора* $(\infty^- - \infty^+)$ *в группе классов дивизоров* $\Delta^\circ(L)$ *равен 5. Заметим, что* $\operatorname{tc}(p_3) \neq 0$, $\operatorname{tc}(q_3) \neq 0$, *поэтому в обозначениях следствия 3.3.3.5 имеем* $r_1 = 0$, *но* $3\operatorname{tc}(p_3)^2 + \operatorname{tc}(F)\operatorname{tc}(q_3)^2 = 0$, *поэтому* $\operatorname{tc}\left(\mu_2^{(3)}\right) = 0$, *следовательно, непрерывная дробь элемента* $\sqrt{F}/X$ *периодическая*

$$\sqrt{F}/X = \Bigg[X + 2;\ \overline{\tfrac{X}{8} - 1,\ \tfrac{X}{12} + \tfrac{8}{9},\ -\tfrac{27X}{8} - \tfrac{45}{4},\ -\tfrac{2X}{81} + \tfrac{4}{81},\ -\tfrac{81X}{32} - \tfrac{81}{16},\ \tfrac{4X}{81} + \tfrac{16}{81},\ -\tfrac{81X^2}{256} + \tfrac{81X}{64} - \tfrac{81}{8},\ \tfrac{4X}{81} + \tfrac{16}{81},\ -\tfrac{81X}{32} - \tfrac{81}{16},\ -\tfrac{2X}{81} + \tfrac{4}{81},\ -\tfrac{27X}{8} - \tfrac{45}{4},\ \tfrac{X}{12} + \tfrac{8}{9},\ \tfrac{X}{8} - 1,\ 2X + 4}\Bigg].$$

Длина периода совпадает с длиной квазипериода и равна $14 < 4m - 2g$.

Пример 3.3.4.4. *Рассмотрим* $F = (X+6)\left(X^3 + 30X^2 + 224X - 32\right)$. *Непрерывная дробь элемента* $\sqrt{F}$ *в* $\mathbb{Q}((1/X))$ *имеет вид*

$$\sqrt{F} = \left[X^2 + 18X + 40;\ \overline{-\tfrac{X}{64} - \tfrac{1}{16},\ 4X + 48,\ -\tfrac{X}{64} - \tfrac{1}{16},\ 2X^2 + 36X + 80}\right].$$

Длина периода совпадает с длиной квазипериода и равна 4. В поле $\mathcal{L}$ *существует фундаментальная единица степени* $m = 5$, *порядок класса дивизора* $(\infty^- - \infty^+)$ *в группе классов дивизоров* $\Delta^\circ(L)$ *равен 5. Заметим, что* $\operatorname{tc}(p_4) \neq 0$, $\operatorname{tc}(q_4) \neq 0$, *поэтому в обозначениях следствия 3.3.3.5 имеем* $r_1 = 0$, *но* $3\operatorname{tc}(p_4)^2 + \operatorname{tc}(F)\operatorname{tc}(q_4)^2 = 0$, *поэтому* $\operatorname{tc}\left(\mu_2^{(3)}\right) = 0$, *следовательно, непрерывная дробь элемента* $\sqrt{F}/X$ *периодическая*

$$\sqrt{F}/X = \Bigg[X + 18;\ \overline{\tfrac{X}{40} + \tfrac{1}{25},\ -\tfrac{125X}{12} - \tfrac{850}{9},\ \tfrac{27X}{10000} + \tfrac{9}{400},\ -\tfrac{10000X}{81} - \tfrac{10000}{81},\ -\tfrac{81X}{320000} - \tfrac{729}{160000},\ -\tfrac{40000X}{81} - \tfrac{160000}{81},\ -\tfrac{81X^2}{2560000} - \tfrac{243X}{640000} + \tfrac{81}{80000},\ -\tfrac{40000X}{81} - \tfrac{160000}{81},\ -\tfrac{81X}{320000} - \tfrac{729}{160000},\ -\tfrac{10000X}{81} - \tfrac{10000}{81},\ \tfrac{27X}{10000} + \tfrac{9}{400},\ -\tfrac{125X}{12} - \tfrac{850}{9},\ \tfrac{X}{40} + \tfrac{1}{25},\ 2X + 36}\Bigg].$$

Длина периода совпадает с длиной квазипериода и равна $14 < 4m - 2g$. *Этот пример показывает, что при сравнительно небольших коэффициентах многочлена* F *коэффициенты неполных частных периодической непрерывной дроби могут быть достаточно велики.*

Приведем пример элемента эллиптического поля $\mathcal{L} = \mathbb{Q}(X)(\sqrt{F})$, $F \in \mathbb{Q}[X]$, $\deg F = 4$, у которого длина квазипериода непрерывной дроби значительно превосходит порядок класса дивизора $(\infty^- - \infty^+)$ в группе классов дивизоров $\Delta^\circ(L)$. Этот пример был найден с помощью символьных компьютерных вычислений и параметризации Куберта [35] всех эллиптических кривых, имеющих точку конечного порядка.

Пример 3.3.4.5. *Положим* $F = 4X^4 - 8X^3 - 8X^2 - 12X - 3$. *Бесконечное нормирование поля* $\mathbb{Q}(X)$ *имеет два неэквивалентных продолжения на поле* $\mathcal{L} = \mathbb{Q}(X)(\sqrt{F})$. *Рассмотрим элемент* $\alpha = \sqrt{F}$ *и его непрерывную дробь.*

В обозначениях следствия 3.3.3.5 справедливы соотношения $v_X\left(\Omega_1^{(1)}\right) = v_X\left(\Omega_1^{(2)}\right) = 0$, $v_X\left(\Omega_1^{(3)}\right) = 2$, *то есть* $r_1 = r_2 = 0$, $r_3 = 2$. *Поэтому, согласно пункту 3 следствия 3.3.3.5, элементы* $\sqrt{F} \cdot X^s$ *для* $-2 \leq s \leq 2$ *имеют периодическое разложение в непрерывную дробь.*

Непрерывная дробь элемента $\sqrt{F}$ *в* $\mathbb{Q}((1/X))$ *имеет вид*

$$\sqrt{F} = \Big[2X^2 - 2X - 3;\ \overline{-\tfrac{X}{6} + \tfrac{1}{4}, 8X - 12,}$$
$$\overline{-\tfrac{X^2}{12} + \tfrac{X}{12} + \tfrac{1}{8}, 8X - 12, -\tfrac{X}{6} + \tfrac{1}{4}, 4X^2 - 4X - 6}\Big].$$

Длина квазипериода равна 3, длина периода равна 6, коэффициент квазипериода $c = -48$, *период имеет симметричный вид. В поле* $\mathcal{L}$ *существует фундаментальная единица степени* $m = 4$, *порядок класса дивизора* $(\infty^- - \infty^+)$ *в группе классов дивизоров* $\Delta^\circ(L)$ *равен 4. В отличии от элементов* $\sqrt{F}/X$ *и* $\sqrt{F}/X^2$ *для элемента* $\sqrt{F}$ *справедливы условия утверждения из статьи [62] об оценке длины квазипериода.*

Непрерывная дробь элемента $\sqrt{F}/X$ *в* $\mathbb{Q}((1/X))$ *имеет вид*

$$\tfrac{\sqrt{F}}{X} = \Big[2X - 2;\ \overline{-\tfrac{X}{3} + \tfrac{2}{3}, -3X - 6, -\tfrac{2X}{27} + \tfrac{2}{9}, 27X - 27, -\tfrac{X}{27} + \tfrac{1}{18},}$$
$$\overline{24X^2 - 36X - 18, -\tfrac{X}{36} + \tfrac{1}{36}, 24X - 24, -\tfrac{X}{12} + \tfrac{1}{6}, \tfrac{16X^3}{3} - \tfrac{16X^2}{3} - 8X - 16,}$$
$$\overline{-\tfrac{X}{12} + \tfrac{1}{6}, 24X - 24, -\tfrac{X}{36} + \tfrac{1}{36}, 24X^2 - 36X - 18, -\tfrac{X}{27} + \tfrac{1}{18},}$$
$$\overline{27X - 27, -\tfrac{2X}{27} + \tfrac{2}{9}, -3X - 6, -\tfrac{X}{3} + \tfrac{2}{3}, 4X - 4}\Big].$$

Длина периода совпадает с длиной квазипериода и равна 20, период имеет симметричный вид.

Непрерывная дробь элемента $\sqrt{F}/X^2$ *в* $\mathbb{Q}((1/X))$ *имеет вид*

$$\tfrac{\sqrt{F}}{X^2} = \Big[2; -\tfrac{X}{2} + \tfrac{3}{4},\ \overline{\tfrac{8X}{3} + 4, -\tfrac{X^2}{24} + \tfrac{X}{8} - \tfrac{1}{6}, 48X - 96, -\tfrac{X}{24} + \tfrac{1}{48}, \tfrac{32X}{3} - 16,}$$
$$\overline{\tfrac{X}{16} + \tfrac{1}{16}, 8X - 22, -\tfrac{2X}{3} + \tfrac{3}{2}, \tfrac{X^4}{3} - \tfrac{X^3}{3} - \tfrac{X^2}{2} - X - \tfrac{3}{2}, -\tfrac{2X}{3} + \tfrac{3}{2}, 8X - 22, \tfrac{X}{16} + \tfrac{1}{16},}$$
$$\overline{\tfrac{32X}{3} - 16, -\tfrac{X}{24} + \tfrac{1}{48}, 48X - 96, -\tfrac{X^2}{24} + \tfrac{X}{8} - \tfrac{1}{6}, \tfrac{8X}{3} + 4, -\tfrac{X}{2} + 1, 8X - 16,}$$
$$\overline{-\tfrac{X}{6} - \tfrac{1}{4}, \tfrac{2X^2}{3} - 2X + \tfrac{8}{3}, -3X + 6, \tfrac{2X}{3} - \tfrac{1}{3}, -\tfrac{2X}{3} + 1, -X - 1, -\tfrac{X}{2} + \tfrac{11}{8},}$$
$$\overline{\tfrac{32X}{3} - 24, -\tfrac{X^4}{48} + \tfrac{X^3}{48} + \tfrac{X^2}{32} + \tfrac{X}{16} + \tfrac{3}{32}, \tfrac{32X}{3} - 24, -\tfrac{X}{2} + \tfrac{11}{8}, -X - 1, -\tfrac{2X}{3} + 1,}$$
$$\overline{\tfrac{2X}{3} - \tfrac{1}{3}, -3X + 6, \tfrac{2X^2}{3} - 2X + \tfrac{8}{3}, -\tfrac{X}{6} - \tfrac{1}{4}, 8X - 16, -\tfrac{X}{2} + 1}\Big].$$

Длина квазипериода равна 19, длина периода равна 38, коэффициент квазипериода $c = -1/16$, *период имеет сдвинутый симметричный вид.*

3.3.5. Ограниченность числа обобщенных якобианов с нетривиальной подгруппой кручения

В следующей теореме доказано, что для гиперэллиптического поля $\mathcal{L}$, определенного над полем K алгебраических чисел, существует только конечное число многочленов D со старшим коэффициентом 1 и ограниченной степени, которые реализуются как дискриминанты элементов $\beta \in \mathcal{L}$, имеющих квазипериодическую непрерывную дробь.

Теорема 3.3.5.1. *Пусть K — поле алгебраических чисел, $\mathcal{L} = K(x)(\sqrt{f})$ — гиперэллиптическое поле и b — некоторая положительная постоянная. Пусть $M = M(b)$ — множество многочленов D со старшим коэффициентом 1 вида $D = \omega^2 f$, $\omega \in K[x]$, $\deg \omega \le b$, таких, что элементы поля $\mathcal{L}$ с дискриминантом $D \in M$ обладают квазипериодическим разложением в непрерывную дробь. Тогда множество M конечно.*

Доказательство. Если в поле $\mathcal{L}$ нет нетривиальных единиц, то множество M пусто, поскольку тогда в поле $\mathcal{L}$ нет элементов с квазипериодической непрерывной дробью. Пусть $\Psi_1 + \Psi_2\sqrt{f}$ — фундаментальная единица поля $\mathcal{L}$. Пусть для $n \in \mathbb{N}$ многочлены $\Omega_1^{(n)}, \Omega_2^{(n)} \in K[x]$ определены соотношениями (3.3.3.1). Из (3.3.1.2) справедливо представление

$$\Omega_1^{(n)} + \Omega_2^{(n)}\sqrt{f} = \Psi_1^n \left(T_n\left(\frac{\Psi_2^2}{\Psi_1^2} f\right) + Q_n\left(\frac{\Psi_2^2}{\Psi_1^2} f\right) \frac{\Psi_2}{\Psi_1}\sqrt{f} \right). \tag{3.3.5.1}$$

По предложению 3.3.3.1 для того, чтобы непрерывная дробь квадратичной иррациональности $\alpha \in \mathcal{L}$, принадлежащей дискриминанту $D = \omega^2 f$, была квазипериодической необходимо и достаточно, чтобы нашелся номер n такой, что $\omega \mid \Omega_2^{(n)}$. По следствию 3.3.1.15 в совокупности для всех $n \in \mathbb{N}$ у многочленов Q_n количество различных неприводимых множителей ограниченной степени конечно, поэтому количество возможных делителей ω многочленов $\Omega_2^{(n)}$ при $n \in \mathbb{N}$, таких, что $\deg \omega \le b$, также конечно.

Теорема 3.3.5.1 доказана. □

Напомним понятие обобщенного якобиана особой кривой согласно конструкции Розенлихта [177; 178], изложенной в монографии Серра [46]. Особой гиперэллиптической кривой соответствует неособая кривая $C : y^2 = f(x)$ и эффективный дивизор $\mathfrak{m}$, называемый модулем. Обобщенный якобиан $J_{\mathfrak{m}}$, ассоциированный с модулем m, есть расширение якобиана J неособой гиперэллиптической кривой C на линейную группу $\Lambda = \Lambda_{\mathfrak{m}}$ так, что последовательность $0 \to \Lambda \to J_{\mathfrak{m}} \to J \to 0$ точна. В статьях [52; 167] установлена связь периодических функциональных непрерывных дробей с точками конечного порядка на обобщенных якобианах.

Пусть $P \in C(K)$ и образ дивизора $P - \iota P$ имеет конечный порядок в якобиане J, где ιP — гиперэллиптическая инволюция точки P. Пусть b — некоторая положительная постоянная.

Положим $\mathcal{M} = \mathcal{M}(b)$ — множество обобщенных якобианов $J_{\mathfrak{m}}$, удовлетворяющих следующим свойствам:

- обобщенный якобиан $J_{\mathfrak{m}}$ ассоциирован с определенными над K модулем $\mathfrak{m}$ таким, что $\mathfrak{m} = \iota\mathfrak{m}$ и $\deg \mathfrak{m} \leq b$;
- образ дивизора $P - \iota P$ имеет конечный порядок в обобщенном якобиане $J_{\mathfrak{m}}$.

Тогда по теореме 3.3.5.1 множество $\mathcal{M}(b)$ конечно, поскольку каждому дискриминанту $D \in M(b)$ соответствует конечное число модулей $\mathfrak{m}$, удовлетворяющих приведенным выше условиям. Более подробно о теоремах конечности для обобщенных якобианов см. [154].

3.3.6. Непрерывные дроби со сколь угодно большой длиной периода

В статье [52] получен удивительный результат о том, что последовательность $\{\deg a_j\}$ степеней неполных частных непрерывной дроби функциональной квадратичной иррациональности $\beta \in \mathcal{L}$ всегда периодическая. Доказательство опирается на неконструктивную теорему Скулема-Малера-Леха о нулях линейной рекуррентной последовательности. Это обстоятельство не позволяет сделать вывод о возможных оценках на длину периода $\kappa(\beta)$ в последовательности $\{\deg a_j\}$.

Пусть $\beta \in \mathcal{L} = K(x)(\sqrt{f})$ является корнем уравнения

$$\Lambda_2 X^2 + 2\Lambda_1 X + \Lambda_0 = 0, \tag{3.3.6.1}$$

где $\Lambda_0, \Lambda_1, \Lambda_2 \in K[x]$ в совокупности взаимно простые многочлены, $\Lambda_0 \neq 0$, $\Lambda_2 \neq 0$. Обозначим $d = \Lambda_1^2 - \Lambda_0\Lambda_2$ — сокращенный дискриминант уравнения (3.3.6.1). Поскольку $\beta \in \mathcal{L}$, то $d = \omega^2 f$ для некоторого $\omega \in K[x]$. По предложению 3.3.3.1 для квазипериодичности непрерывной дроби элемента β необходимо и достаточно, чтобы нашлась такая нетривиальная единица $U = \Omega_1 + \Omega_2\sqrt{f} \in \mathcal{O}_\infty$, что $\omega \mid \Omega_2$. В следствии 3.3.2.4 найдены оценки на длину квазипериода $N = N(\beta)$ элемента β (при условии, что длина квазипериода конечна), и, в частности, получена верхняя оценка $N(\beta) \leq \deg \Omega_1$.

Цель этого параграфа — изучить вопрос о достижимости этой верхней оценки, и, в частности, ответить на естественный вопрос: ограничена ли величина $N_{\mathcal{L}} = \sup_{\beta \in \mathcal{L}} N(\beta)$ для зафиксированного гиперэллиптического поля $\mathcal{L}$? Оказывается, что если в $\mathcal{O}_\infty \subset \mathcal{L}$ существуют нетривиальные единицы, то $N_{\mathcal{L}} = +\infty$ (см. теорему 3.3.6.1). Также мы докажем, что в этом случае и $\kappa_{\mathcal{L}} = +\infty$ (см. следствие 3.3.6.2), где $\kappa_{\mathcal{L}} = \sup_{\beta \in \mathcal{L}} \kappa(\beta)$, что частично дает ответ на вопрос из [52] о возможных значениях длин периодов последовательности степеней неполных частных функциональных непрерывных дробей квадратичных иррациональностей.

Теорема 3.3.6.1. *Пусть K — поле алгебраических чисел, и $\mathcal{L} = K(x)(\sqrt{f})$ — гиперэллиптическое поле, кольцо целых элементов которого обладает нетривиальными единицами.*

Тогда для любого сколь угодно большого значения $b \in \mathbb{N}$ найдется такой элемент $\beta \in \mathcal{L}$, у которого длина периода непрерывной дроби конечна и больше b.

Доказательство. Сначала докажем, что для любого значения $b \in \mathbb{N}$ найдется такой элемент $\beta \in \mathcal{L}$, у которого длина квазипериода непрерывной дроби конечна и больше b.

Пусть в данном поле $\mathcal{L} = K(x)(\sqrt{f})$ существует фундаментальная единица $\Psi_1 + \Psi_2\sqrt{f}$, где $\Psi_1, \Psi_2 \in K[x]$. Пусть заданы многочлены $T_n(x), Q_n(x) \in \mathbb{Z}[x]$, $n \in \mathbb{N}$, как в (3.3.1.1) и определены многочлены $\Omega_1^{(j)}, \Omega_2^{(j)} \in K[x]$ по формулам (3.3.3.1). По предложению 3.3.3.1 элемент $\beta \in \mathcal{L}$ с сокращенным дискриминантом $D = \omega^2 f$ обладает квазипериодической непрерывной дробью, тогда и только тогда, когда найдется номер $n \in \mathbb{N}$ такой, что $\omega \mid \Omega_2^{(n)}$. Наша задача — построить подходящую последовательность элементов $\beta = \beta^{(n)}$, у которых длины квазипериодов непрерывных дробей $\beta^{(n)}$ стремятся к бесконечности при n, пробегающим некоторую последовательность натуральных чисел, стремящуюся к бесконечности. В силу предложения 3.3.3.1 достаточно построить соответствующую последовательность дискриминантов $D^{(n)} = \left(\omega^{(n)}\right)^2 f$, где $\omega^{(n)} \mid \Omega_2^{(n)}$.

Рассмотрим последовательность нечетных чисел $\{n_k\}_{k\in\mathbb{N}}$, для которой справедливо соотношение $\varphi(n_k)/n_k \to 0$ при $k \to \infty$. Существование такой последовательности и точные оценки на нижний предел функции $\varphi(n)/n$ доказаны в [179]. В качестве последовательности $\{n_k\}_{k\in\mathbb{N}}$ можно взять, например, $n_k = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ — произведение последовательных нечетных простых чисел $p_1 = 3$, $p_2 = 5$, ...

Пусть $n = 2n_k$, тогда по следствию 3.3.1.13 имеем $\deg P(T_n) = \varphi(n_k)$ (см. определение многочлена $P(T_n)(x) \in \mathbb{Z}[x]$ в §3.3.1). Так как последовательность $\varphi(n_k)$ монотонно стремится к бесконечности при $k \to \infty$, то без ограничения общности сразу считаем, что номера k выбираются достаточно большими, а именно такими, что $\varphi(n_k) > [K : \mathbb{Q}]$. В связи с представлением (3.3.5.1) в качестве $\omega^{(k)}(x)$ выберем один из неприводимых над K делителей многочлена

$$\left(\Psi_1(x)\right)^{2\varphi(n_k)} P(T_n)\left(\frac{\Psi_2^2(x)f(x)}{\Psi_1^2(x)}\right) = \overline{P(T_n)}\left(\Psi_2^2(x)f(x), \Psi_1^2(x)\right) \in K[x],$$

где $\overline{P(T_n)}(x)$ — однородный многочлен, соответствующий многочлену $P(T_n)(x)$. По теореме 3.3.1.12 многочлен $P(T_n)(x)$ делит $Q_{2n}(x)$, причем при $j < 2n$ многочлен $P(T_n)(x)$ не делит $Q_j(x)$. Поскольку многочлен $P(T_n)(x)$ неприводим над полем $\mathbb{Q}$ (см. теорему 3.3.1.12), то справедливы оценки

$$\varphi(n_k) = \deg P(T_n)(x) \leq \deg \omega^{(k)}(x) \leq 2m \deg P(T_n)(x) = 2m\varphi(n_k),$$

где $\deg \Psi_1(x) = m$ — степень фундаментальной единицы $\Psi_1 + \Psi_2\sqrt{f}$. Итак, по построению имеем $\omega^{(k)}(x) \mid \Omega_2^{(2n)}(x)$ и $\omega^{(k)}(x) \nmid \Omega_2^{(j)}(x)$ при $j < 2n = 4n_k$.

Пусть $\beta^{(k)} \in \mathcal{L}$ является корнем некоторого многочлена

$$\Lambda_2^{(k)} Y^2 + 2\Lambda_1^{(k)} Y + \Lambda_0^{(k)} = 0,$$

где $\Lambda_2^{(k)}, \Lambda_1^{(k)}, \Lambda_0^{(k)} \in K[x]$ в совокупности взаимно простые многочлены и сокращенный дискриминант имеет вид

$$d^{(k)}(x) = (\Lambda_1^{(k)})^2 - \Lambda_0^{(k)}\Lambda_2^{(k)} = \left(\omega^{(k)}(x)\right)^2 f(x).$$

Дополнительно предполагаем, что

$$r_k = \max\{\deg \Lambda_0^{(k)}(x),\ \deg \Lambda_1^{(k)}(x),\ \deg \Lambda_2^{(k)}(x)\} \le \deg d^{(k)}(x). \tag{3.3.6.2}$$

Такая тройка многочленов $\left(\Lambda_2^{(k)}, \Lambda_1^{(k)}, \Lambda_0^{(k)}\right)$ с ограничением (3.3.6.2) всегда существует: например, можно взять $\left(1, 0, d^{(k)}(x)\right)$.

Положим $\Theta_1^{(2n)}(x) = \Omega_1^{(2n)}(x)$, $\Theta_2^{(2n)}(x) = \Omega_2^{(2n)}(x)/\omega^{(k)}(x)$. По следствию 3.3.2.4 справедливы оценки на длину квазипериода N_k непрерывной дроби элемента $\beta^{(k)}$:

$$\frac{4n_k m}{r_k} = \frac{2nm}{r_k} = \frac{\deg \Theta_1^{(2n)}}{r_k} \le N_k \le \deg \Theta_1^{(2n)} = 2nm = 4n_k m. \tag{3.3.6.3}$$

Пусть $\deg f = 2g + 2$, тогда

$$r_k \le \deg d^{(k)}(x) = 2\deg \omega^{(k)}(x) + \deg f \le 2m\varphi(n_k) + 2g + 2. \tag{3.3.6.4}$$

Из (3.3.6.3) и (3.3.6.4) получаем

$$N_k \ge \frac{4n_k m}{2m\varphi(n_k) + 2g + 2}. \tag{3.3.6.5}$$

Значения m и g определены в поле $\mathcal{L}$ однозначно. В силу того, что $\varphi(n_k)/n_k \to 0$ при $k \to \infty$, имеем $N_k \to \infty$ при $k \to \infty$.

Теперь докажем, что для любого значения $b \in \mathbb{N}$ найдется такой элемент $\beta \in \mathcal{L}$, у которого длина периода непрерывной дроби конечна и больше b. Как и выше, рассмотрим последовательность дискриминантов $d^{(k)} = \left(\omega^{(k)}(x)\right)^2 f(x)$. По построению элемент $\beta^{(k)} = \sqrt{d^{(k)}} = \omega^{(k)}(x)\sqrt{f(x)}$ имеет квазипериодическое разложение в непрерывную дробь, а по теореме 3.1.7.3 (или следствию из теоремы 3 [118]) такой элемент $\beta^{(k)}$ имеет периодическое разложение в непрерывную дробь, причем длина периода равна длине квазипериода или равна удвоенной длине квазипериода. Таким образом, для длины периода справедлива такая же нижняя оценка, как в (3.3.6.5), следовательно, длина периода непрерывной дроби элемента $\beta^{(k)} = \sqrt{d^{(k)}} \in \mathcal{L}$ стремится к бесконечности при $k \to \infty$.

Теорема 3.3.6.1 доказана. □

Ниже показано, что в любом гиперэллиптическом поле $\mathcal{L}$, определенном как в теореме 3.3.6.1, существует квазипериодический (периодический) элемент со сколь угодно большой длиной периода в последовательности степеней неполных частных.

Следствие 3.3.6.2. *Пусть $\mathcal{L}$ — гиперэллиптическое поле, определенное как в теореме 3.3.6.1. Тогда для любого $b \in \mathbb{N}$ существует квазипериодический (периодический) элемент $\alpha \in \mathcal{L}$, для которого длина периода степеней неполных частных не меньше b.*

Доказательство. Будем использовать те же обозначения, как в доказательстве теоремы 3.3.6.1. Обозначим $2t = \deg d^{(k)} = \deg\big((\omega^{(k)})^2 f\big)$. Положим $\Lambda_1^{(k)} = \Big[\sqrt{d^{(k)}}\Big]_\infty^-$, $\Lambda_0^{(k)} = (\Lambda_1^{(k)})^2 - d^{(k)}$ и $\Lambda_0^{(k)} = 1$, тогда $\deg \Lambda_1^{(k)} = t$ и $\Lambda_0^{(k)} < t$. Рассмотрим $\alpha^{(k)} = \Lambda_1^{(k)} + \sqrt{d^{(k)}}$ — корень квадратного уравнения

$$Y^2 - 2\Lambda_1^{(k)} Y + \Lambda_0^{(k)} = 0 \tag{3.3.6.6}$$

с дискриминантом $d^{(k)}$.

Непрерывная дробь $\sqrt{d^{(k)}}$ периодическая и имеет вид

$$[a_0; \overline{a_1, \dots, a_{N_k-1}, a_{N_k}}^c] = [a_0; \overline{a_1, \dots, a_{N_k-1}, 2ca_0}^c],$$

где N_k — длина квазипериода, c — константа квазипериода, длина периода равна N_k, если $c = 1$, и $2N_k$ иначе. Значит, непрерывная дробь $\alpha^{(k)}$ чисто периодическая и имеет вид (см. теорему 3.1.7.3 и предложение 3.1.7.1 или [68])

$$[\overline{2a_0, a_1, \dots, a_{N_k-1}, 2ca_0, a_{N_k-1}, \dots, a_1}].$$

В уравнении (3.3.6.6) имеем $r_k = \max\{\deg \Lambda_0^{(k)},\ \deg \Lambda_1^{(k)}\} = t$, следовательно, для многочленов A_j, B_j, определенных как в (3.1.2.2), в соответствие с замечанием 3.1.2.7 получаем $\deg A_j, \deg B_j \le r_k = t$.

Отметим, что в случае $\deg A_{j-1} = 0$ для некоторого $j \in \mathbb{N}$ из тождества (3.1.4.2) многочлены $|B_{j-1} - \Lambda_1^{(k)}|$ и $|B_j - \Lambda_1^{(k)}|$ определены однозначно и равны $\Lambda_1^{(k)}$. Значит, с учетом (3.1.4.1) и (3.1.2.4) получаем $\alpha^{(k)} = c\alpha_j^{(k)}$. Кроме того, из (3.1.2.4) имеем $\deg a_j = t$ тогда и только тогда, когда $\deg A_{j-1} = 0$. Отсюда следует, что $\deg a_0 = \deg a_{N_k} = t$ и $\deg a_j < t$ при $1 \le i \le N_k - 1$.

Наконец, как в теореме 3.3.6.1, имеем $N_k \to \infty$ при $k \to \infty$, откуда и получается утверждение следствия 3.3.6.2. □

Из этого, в частности, следует, что в отличие от "ключевых" элементов, рассмотренных в теореме 3.3.3.3 (см. [3], теорема 3) в общем случае оценка на длину квазипериода непрерывной дроби квадратичной иррациональности не может зависеть только от параметров, гиперэллиптического поля $\mathcal{L}$: от рода g поля $\mathcal{L}$, степени расширения $[K : \mathbb{Q}]$ и степени m фундаментальной единицы кольца целых элементов поля $\mathcal{L}$.

В следующем примере для квадратичной иррациональности α дается оценка на длину квазипериода (или периода), которая зависит от дополнительного параметра — степени дискриминанта α.

Пример 3.3.6.3. *Рассмотрим несколько простейших примеров с функцией вида* $f(x) = x^2 + a$ *над полем* $K = \mathbb{Q}$, *где в качестве параметра* a *будем брать свободные от квадратов целые числа, отличные от* 0. *Фундаментальная единица кольца* $\mathcal{O}_\infty$ *целых элементов гиперэллиптического поля* $\mathcal{L} = \mathbb{Q}(x)(\sqrt{f})$ *имеет вид* $u = x + \sqrt{f}$. *Рассмотрим последовательность единиц* $\Omega_1^{(n)} + \Omega_2^{(n)}\sqrt{f} = u^n$, $n = 3, \dots, 105$, *кольца* $\mathcal{O}_\infty$.

Таблица 3.2: Значения длин квазипериодов $N_{n,j}$ при $a = -7$.

n	3	4	6	12	14	21	24	30	33	36	39	42	70
$N_{n,j}$	1	2	4	6	8	9	10	12	13	14	15	30	42

Таблица 3.3: Значения длин квазипериодов $N_{n,j}$ при $a = -6$.

n	3	4	6	12	21	24	30	33	36	51	54	57	60	84
$N_{n,j}$	1	2	4	8	9	10	12	13	18	19	20	21	32	42

Таблица 3.4: Значения длин квазипериодов $N_{n,j}$ при $a = -5$.

n	3	4	5	6	12	15	25	35	45	55	65	75	85	95	105
$N_{n,j}$	1	2	3	4	6	11	15	23	31	35	41	49	53	59	75

Таблица 3.5: Значения длин квазипериодов $N_{n,j}$ при $a = -3$.

n	3	4	6	12	15	18	30	42	54	66	78	90	102
$N_{n,j}$	1	2	5	6	7	14	20	28	38	40	48	52	60

Таблица 3.6: Значения длин квазипериодов $N_{n,j}$ при $a = -2$.

n	3	4	6	12	20	28	36	44	52	60	76	84	100
$N_{n,j}$	1	3	4	8	12	14	18	20	24	30	32	38	46

Таблица 3.7: Значения длин квазипериодов $N_{n,j}$ при $a = -1$.

n	3	6	12	15	21	30	33	39	48	51	57	69	81	87	93	105
$N_{n,j}$	2	4	6	8	10	12	14	16	18	20	22	26	28	32	34	36

Таблица 3.8: Значения длин квазипериодов $N_{n,j}$ при $a \in [1, 2, 3, 5, 6, 7]$.

n	3	4	6	12	15	18	21	24	30	33	36	39	42	48	51	54	57	69	72	81	87	93	96
$N_{n,j}$	1	2	4	6	7	8	9	10	12	13	14	15	16	18	19	20	21	25	26	27	31	33	34

Для каждого неприводимого над $\mathbb{Q}$ множителя $\omega_{n,j}$ многочлена $\Omega_2^{(n)}(x)$ посчитаем длину квазипериода $N_{n,j} = N_{n,j}(a)$ непрерывной дроби элемента $\omega_{n,j}\sqrt{f}$. Индекс j соответствует

нумерации неприводимых над $\mathbb{Q}$ *делителей многочлена* $\Omega_2^{(n)}(x)$ *по возрастанию их степеней. Число* $105 = 3 \cdot 5 \cdot 7$ *в качестве верхней границы значений* n *выбрано не случайно, поскольку в соответствие с доказательством теоремы 3.3.6.1 при числе* n*, равном произведению нечетных простых чисел, ожидается сравнительно большое значение* $N_{n,j}$*.*

Ниже в таблицах 3.2-3.8 для различных значений параметра a *приведены возрастающие последовательности номеров* n *и значений* $N_{n,j}$*. Таблицы построены по принципу рекордного значения длины квазипериода: в таблицу включается очередное значение* $N_{n,j}$*, если* $N_{n,j} > N_{k,i}$ *для всех* $k \le n$*,* $i < j$*. По этим таблицам можно оценить порядок роста величины* $\max_{i \le j, k \le n} N_{k,i}$*.*

В таблице 3.8 указаны соответствующие значения длин квазипериодов $N_{n,j}$ *при* $a \in [1, 2, 3, 5, 6, 7]$*. Мы предполагаем, что таблица будет иметь тот же вид для всех* $a \in \mathbb{N}$*.*

3.3.7. Оценка сверху длин периодов непрерывных дробей ключевых элементов над квадратичным полем

В статье [13] были найдены все рациональные корни последовательностей многочленов $T_n(x)$ и $Q_n(x)$, определенных в (3.3.1.1). Исходя из этого в той же статье были даны оценки на возможные длины периодов непрерывных дробей "ключевых" элементов вида $\sqrt{f}/x^s$, а также приведены соответствующие примеры, определенные над полем $\mathbb{Q}$.

Для квадратичных полей K из теоремы 3.3.3.3 и таблицы 3.1 следуют возможные оценки сверху на длины периодов непрерывных дробей "ключевых" элементов вида $\sqrt{f}/x^s$, которые в первую очередь зависят от поля K и от степени фундаментальной единицы гиперэллиптического поля $\mathcal{L} = K(x)(\sqrt{f})$.

Исследуем последовательности многочленов $T_n(x)$ и $Q_n(x)$, на наличие корней в квадратичных полях, чтобы явно найти квадратичные поля K, над которыми выполнены соответствующие оценки на длину квазипериода из теоремы 3.3.3.3 при $k = 2$, а также все остальные квадратичные поля, над которыми справедливы такие же оценки, как над $\mathbb{Q}$. Далее приведем соответствующие примеры.

Предложение 3.3.7.1. *Множество корней последовательности многочленов* $T_n(x)$ *и* $Q_n(x)$*, принадлежащих квадратичным полям, исчерпывается множеством*

$$M = \left\{ -1,\ -\frac{1}{3},\ -3,\ -3 \pm 2\sqrt{2},\ \frac{-5 \pm 2\sqrt{5}}{5},\ -5 \pm 2\sqrt{5},\ -7 \pm 4\sqrt{3} \right\}.$$

Доказательство. Имеем $\deg T_n = \left[\frac{n}{2}\right]$, $\deg Q_n = \left[\frac{n-1}{2}\right]$ и

$$T_1(x) = 1, \quad Q_1(x) = 1, \quad T_2(x) = x + 1, \quad Q_2(x) = 2,$$
$$T_3(x) = 3x + 1, \quad Q_3(x) = x + 3, \quad T_4(x) = x^2 + 6x + 1, \quad Q_4(x) = 4(x + 1),$$
$$T_5(x) = 5x^2 + 10x + 1, \quad Q_5(x) = x^2 + 10x + 5,$$
$$T_6(x) = (x + 1)\left(x^2 + 14x + 1\right), \quad Q_6(x) = 2\,(x + 3)\,(3x + 1), \ldots$$

Множество различных корней многочленов $T_n(x)$ и $Q_n(x)$ при $n \leq 6$ в точности совпадает с множеством M. Из теоремы 3.3.1.12 и следствия 3.3.1.13 получаем, что при $n > 6$ справедливы соотношения $\deg P(T_n) = \deg \tilde{P}(T_n) \geq 3$. Значит, при $n > 6$ у многочленов $T_n(x)$ и $Q_n(x)$ нет других корней, лежащих в квадратичных полях, по сравнению с корнями из множества M. □

Пример 3.3.7.2. *Рассмотрим гиперэллиптическое поле $\mathcal{L} = K(x)(\sqrt{f})$ рода $g = 1$, заданное над полем $K = \mathbb{Q}(\sqrt{5})$ с помощью многочлена*

$$f = x^4 + 4x^3 - 4\sqrt{5}x^2 - 8x^2 - 72x - 24\sqrt{5}x - 40 - 8\sqrt{5} =$$
$$= \left(-x^2 - 2\sqrt{5}x - 4x - 6\sqrt{5} - 10\right)\left(-x^2 + 2\sqrt{5}x - 2 + 2\sqrt{5}\right).$$

В поле $\mathcal{L}$ есть фундаментальная единица $\Psi_1 + \Psi_2\sqrt{f}$ степени $m = 4$,

$$\Psi_1 = -\frac{3x^4}{8} + \frac{\sqrt{5}x^4}{8} - \frac{3x^3}{4} + \frac{\sqrt{5}x^3}{4} + 2x^2 + 6x - 6 - 2\sqrt{5},$$
$$\Psi_2 = -\frac{3x^2}{8} + \frac{\sqrt{5}x^2}{8} + 1 = \left(-\frac{\sqrt{5}x}{4} + \frac{x}{4} - 1\right)\left(-\frac{x}{4} + \frac{\sqrt{5}x}{4} - 1\right).$$

Непрерывная дробь элемента $\sqrt{f}$ имеет вид

$$\sqrt{f} = \left[x^2 + 2x - 6 - 2\sqrt{5};\ \overline{\frac{x\left(-3 + \sqrt{5}\right)}{32},\ 4x,\ \frac{-3x^2 + \sqrt{5}x^2 - 6x + 2\sqrt{5}x + 8}{64},}\right.$$
$$\left.\overline{4x,\ \frac{x\left(-3 + \sqrt{5}\right)}{32},\ 2\left(x^2 + 2x - 6 - 2\sqrt{5}\right)}\right].$$

Длина квазипериода равна 3, коэффициент квазипериода равен $-32(3 + \sqrt{5})$, длина периода

равна 6. Непрерывная дробь элемента $\sqrt{f}/x$ *имеет вид*

$$\frac{\sqrt{f}}{x} = \Bigg[x+2;\ \overline{-\tfrac{x-4}{2\left(\sqrt{5}+3\right)},\ -\tfrac{\sqrt{5}x+3x+7\sqrt{5}+19}{8},\ 2\left(-18x+8\sqrt{5}x-3\sqrt{5}+7\right),\ \tfrac{\left(4\sqrt{5}+9\right)(x+2)}{32},\ -4\left(-11x+5\sqrt{5}x-6+2\sqrt{5}\right),\ -\tfrac{-x+\sqrt{5}x+12}{64},\ -8\left(2x+\sqrt{5}x-3-\sqrt{5}\right),\ -\tfrac{\left(-9+4\sqrt{5}\right)(x+2)}{32},\ 4\left(11x+5\sqrt{5}x+16\sqrt{5}+36\right),\ \tfrac{-29x+13\sqrt{5}x-72+32\sqrt{5}}{64},\ 4\left(11x+5\sqrt{5}x+16\sqrt{5}+36\right),\ -\tfrac{\left(-9+4\sqrt{5}\right)(x+2)}{32},\ -8\left(2x+\sqrt{5}x-3-\sqrt{5}\right),\ -\tfrac{-x+\sqrt{5}x+12}{64},\ -4\left(-11x+5\sqrt{5}x-6+2\sqrt{5}\right),\ \tfrac{\left(4\sqrt{5}+9\right)(x+2)}{32},\ 2\left(-18x+8\sqrt{5}x-3\sqrt{5}+7\right),\ -\tfrac{\sqrt{5}x+3x+7\sqrt{5}+19}{8},\ -\tfrac{x-4}{2\left(\sqrt{5}+3\right)},\ 2\left(x+2\right)}\Bigg].$$

Длина квазипериода равна $N = 20$ *и совпадает с длиной периода. В данном примере при обозначениях теоремы 3.3.3.3 имеем* $s = 1$, $n = 5$, $v_x\left(\Omega_2^{(1)}\right) = \ldots = v_x\left(\Omega_2^{(4)}\right) = 0$, $v_x\left(\Omega_2^{(5)}\right) = 1$, $k = [K\ :\ \mathbb{Q}] = 2$ *и* $\varphi(n) \mid 2k$. *По теореме 3.3.3.3 имеем оценку на длину квазипериода* $N \leq nm - \delta = 20$, *поскольку* $\deg f_1 = 2$, $\delta = 0$. *Получается, что на этом примере достигается верхняя оценка на длину квазипериода теоремы 3.3.3.3.*

Пример 3.3.7.3. *Рассмотрим гиперэллиптическое поле* $\mathcal{L} = K(x)(\sqrt{f})$ *рода* $g = 1$, *заданное над полем* $K = \mathbb{Q}(\sqrt{2})$ *с помощью многочлена*

$$f = x^4 + 4x^3 - 12x^2 - 8\sqrt{2}x^2 - 96x - 48\sqrt{2}x - 32.$$

В поле $\mathcal{L}$ *есть фундаментальная единица* $\Psi_1 + \Psi_2\sqrt{f}$ *степени* $m = 4$,

$$\Psi_1 = -\frac{x^4}{4} + \frac{\sqrt{2}x^4}{8} - \frac{x^3}{2} + \frac{\sqrt{2}x^3}{4} + 2x^2 + 6x - 8 - 4\sqrt{2}, \quad \Psi_2 = -\frac{x^2}{4} + \frac{\sqrt{2}x^2}{8} + 1.$$

Непрерывная дробь элемента $\sqrt{f}$ *имеет вид*

$$\sqrt{f} = \Bigg[x^2 + 2x - 8 - 4\sqrt{2};\ \overline{\tfrac{x\left(-2+\sqrt{2}\right)}{32},\ 4x,\ \tfrac{-2x^2+\sqrt{2}x^2-4x+2\sqrt{2}x+8}{64},\ 4x,\ \tfrac{x\left(-2+\sqrt{2}\right)}{32},\ 2\left(x^2+2x-8-4\sqrt{2}\right)}\Bigg].$$

Длина квазипериода равна 3, коэффициент квазипериода равен $-64(\sqrt{2}+2)$, *длина периода*

равна 6. Непрерывная дробь элемента $\sqrt{f}/x$ *имеет вид*

$$\frac{\sqrt{f}}{x} = \Bigg[x+2;\ \overline{-\tfrac{x-4}{4\left(\sqrt{2}+2\right)},\ -\tfrac{\sqrt{2}x+2x+8\sqrt{2}+14}{4},\ -10x+7\sqrt{2}x-4\sqrt{2}+6,}$$
$$\overline{\tfrac{\left(7\sqrt{2}+10\right)(x+2)}{16},\ -2\left(-7x+5\sqrt{2}x-6+4\sqrt{2}\right),\ -\tfrac{x+\sqrt{2}x+6\sqrt{2}+10}{8},}$$
$$\overline{-\sqrt{2}x+x-2\sqrt{2}+4,\ \tfrac{x+2}{4},\ -x+2\sqrt{2}+4,\ \tfrac{-3x+2\sqrt{2}x-10+6\sqrt{2}}{8},}$$
$$\overline{-2\left(2\sqrt{2}+3\right)(x-2),\ -\tfrac{\left(-10+7\sqrt{2}\right)(x+2)}{16},\ -3x^2-2\sqrt{2}x^2+28\sqrt{2}+40,}$$
$$\overline{-\tfrac{-17x^3+12\sqrt{2}x^3-34x^2+24\sqrt{2}x^2-28\sqrt{2}x+40x-112\sqrt{2}+160}{64},}$$
$$\overline{-3x^2-2\sqrt{2}x^2+28\sqrt{2}+40,\ -\tfrac{\left(-10+7\sqrt{2}\right)(x+2)}{16},\ -2\left(2\sqrt{2}+3\right)(x-2),}$$
$$\overline{\tfrac{-3x+2\sqrt{2}x-10+6\sqrt{2}}{8},\ -x+2\sqrt{2}+4,\ \tfrac{x+2}{4},\ -\sqrt{2}x+x-2\sqrt{2}+4,}$$
$$\overline{-\tfrac{x+\sqrt{2}x+6\sqrt{2}+10}{8},\ -2\left(-7x+5\sqrt{2}x-6+4\sqrt{2}\right),\ \tfrac{\left(7\sqrt{2}+10\right)(x+2)}{16},}$$
$$\overline{-10x+7\sqrt{2}x-4\sqrt{2}+6,\ -\tfrac{\sqrt{2}x+2x+8\sqrt{2}+14}{4},\ -\tfrac{x-4}{4\left(\sqrt{2}+2\right)},\ 2\left(x+2\right)}\Bigg].$$

Длина квазипериода равна $N = 28$ *и совпадает с длиной периода. В данном примере при обозначениях теоремы 3.3.3.3 имеем* $s = 1$, $n = 8$, $v_x\left(\Omega_2^{(1)}\right) = \ldots = v_x\left(\Omega_2^{(7)}\right) = 0$, $v_x\left(\Omega_2^{(8)}\right) = 1$, $k = [K\ :\ \mathbb{Q}] = 2$ *и* $\varphi(n) \mid 2k$. *По следствию 3.3.3.6 имеем оценку на длину квазипериода* $N \leq nm - 2g = 30$.

Пример 3.3.7.4. *Рассмотрим гиперэллиптическое поле* $\mathcal{L} = K(x)(\sqrt{f})$ *рода* $g = 1$, *заданное над полем* $K = \mathbb{Q}(\sqrt{5})$ *с помощью многочлена*

$$f = x^4 + 4x^3 - 16x^2 - 4\sqrt{5}x^2 - 120x - 24\sqrt{5}x - 40 + 8\sqrt{5}.$$

В поле $\mathcal{L}$ *есть фундаментальная единица* $\Psi_1 + \Psi_2\sqrt{f}$ *степени* $m = 4$,

$$\Psi_1 = -\frac{x^4}{8} + \frac{\sqrt{5}x^4}{40} - \frac{x^3}{4} + \frac{\sqrt{5}x^3}{20} + 2x^2 + 6x - 10 - 2\sqrt{5}, \quad \Psi_2 = -\frac{x^2}{8} + \frac{\sqrt{5}x^2}{40} + 1.$$

Непрерывная дробь элемента $\sqrt{f}$ *имеет вид*

$$\sqrt{f} = \Bigg[x^2+2x-10-2\sqrt{5};\ \overline{\tfrac{x\left(-5+\sqrt{5}\right)}{160},\ 4x,\ \tfrac{-5x^2+\sqrt{5}x^2-10x+2\sqrt{5}x+40}{320},}$$
$$\overline{4x,\ \tfrac{x\left(-5+\sqrt{5}\right)}{160},\ 2\left(x^2+2x-10-2\sqrt{5}\right)}\Bigg].$$

Длина квазипериода равна 3, коэффициент квазипериода равен $-32(\sqrt{5}+5)$, *длина периода*

равна 6. Непрерывная дробь элемента $\sqrt{f}/x$ имеет вид

$$\frac{\sqrt{f}}{x} = \Bigg[x+2;\ \overline{-\frac{x-4}{2\left(\sqrt{5}+5\right)},\ -\frac{\sqrt{5}x+5x+9\sqrt{5}+35}{8},\ \frac{2\left(-10x+4\sqrt{5}x-5\sqrt{5}+15\right)}{25},\ \frac{5\left(2\sqrt{5}+5\right)(x+2)}{32},\ -\frac{4\left(-15x+7\sqrt{5}x-70+30\sqrt{5}\right)}{25},\ -\frac{15x+7\sqrt{5}x+52\sqrt{5}+120}{64},\ -\frac{8\left(-20x+9\sqrt{5}x-25+11\sqrt{5}\right)}{5},\ \frac{\left(4\sqrt{5}+9\right)(x+2)}{32},\ \frac{4\left(-25x+11\sqrt{5}x-8\sqrt{5}+20\right)}{5},\ \frac{5(x+8)}{16\left(-5+\sqrt{5}\right)},\ -\frac{4\left(\sqrt{5}x+5x-20\right)}{25},\ -\frac{5\left(-5+2\sqrt{5}\right)(x+2)}{32},\ -\frac{8\left(2\sqrt{5}x+5x-35-15\sqrt{5}\right)}{25},\ \frac{-25x+11\sqrt{5}x-120+52\sqrt{5}}{64},\ -\frac{4\left(11\sqrt{5}+25\right)(x-2)}{5},\ -\frac{\left(-9+4\sqrt{5}\right)(x+2)}{32},\ -\frac{2\left(11\sqrt{5}x^2+25x^2-360-160\sqrt{5}\right)}{5},\ -\frac{-65x^3+29\sqrt{5}x^3-130x^2+58\sqrt{5}x^2-160\sqrt{5}x+360x-640\sqrt{5}+1440}{1280},\ -\frac{2\left(11\sqrt{5}x^2+25x^2-360-160\sqrt{5}\right)}{5},\ -\frac{\left(-9+4\sqrt{5}\right)(x+2)}{32},\ -\frac{4\left(11\sqrt{5}+25\right)(x-2)}{5},\ \frac{-25x+11\sqrt{5}x-120+52\sqrt{5}}{64},\ -\frac{8\left(2\sqrt{5}x+5x-35-15\sqrt{5}\right)}{25},\ -\frac{5\left(-5+2\sqrt{5}\right)(x+2)}{32},\ -\frac{4\left(\sqrt{5}x+5x-20\right)}{25},\ \frac{5(x+8)}{16\left(-5+\sqrt{5}\right)},\ \frac{4\left(-25x+11\sqrt{5}x-8\sqrt{5}+20\right)}{5},\ \frac{\left(4\sqrt{5}+9\right)(x+2)}{32},\ -\frac{8\left(-20x+9\sqrt{5}x-25+11\sqrt{5}\right)}{5},\ -\frac{15x+7\sqrt{5}x+52\sqrt{5}+120}{64},\ -\frac{4\left(-15x+7\sqrt{5}x-70+30\sqrt{5}\right)}{25},\ \frac{5\left(2\sqrt{5}+5\right)(x+2)}{32},\ \frac{2\left(-10x+4\sqrt{5}x-5\sqrt{5}+15\right)}{25},\ -\frac{\sqrt{5}x+5x+9\sqrt{5}+35}{8},\ -\frac{x-4}{2\left(\sqrt{5}+5\right)},\ 2\,(x+2)}\Bigg].$$

Длина квазипериода равна $N = 36$ и совпадает с длиной периода. В данном примере при обозначениях теоремы 3.3.3.3 имеем $s = 1$, $n = 10$, $v_x\left(\Omega_2^{(1)}\right) = \ldots = v_x\left(\Omega_2^{(9)}\right) = 0$, $v_x\left(\Omega_2^{(10)}\right) = 1$, $k = [K : \mathbb{Q}] = 2$ и $\varphi(n) \mid 2k$. По следствию 3.3.3.6 имеем оценку на длину квазипериода $N \leq nm - 2g = 38$.

Пример 3.3.7.5. *Рассмотрим гиперэллиптическое поле $\mathcal{L} = K(x)(\sqrt{f})$ рода $g = 1$, заданное над полем $K = \mathbb{Q}(\sqrt{3})$ с помощью многочлена*

$$f = x^4 + 4x^3 - 8\sqrt{3}x^2 - 12x^2 - 96x - 48\sqrt{3}x - 16.$$

В поле $\mathcal{L}$ есть фундаментальная единица $\Psi_1 + \Psi_2\sqrt{f}$ степени $m = 4$,

$$\Psi_1 = -\frac{x^4}{2} + \frac{\sqrt{3}x^4}{4} - x^3 + \frac{\sqrt{3}x^3}{2} + 2x^2 + 6x - 8 - 4\sqrt{3}, \quad \Psi_2 = -\frac{x^2}{2} + \frac{\sqrt{3}x^2}{4} + 1.$$

Непрерывная дробь элемента $\sqrt{f}$ *имеет вид*

$$\sqrt{f} = \left[x^2+2x-8-4\sqrt{3};\ \overline{\tfrac{x\left(-2+\sqrt{3}\right)}{16}, 4x, \tfrac{-2x^2+\sqrt{3}x^2-4x+2\sqrt{3}x+4}{32}, 4x, \tfrac{x\left(-2+\sqrt{3}\right)}{16}, 2\left(x^2+2x-8-4\sqrt{3}\right)}\right].$$

Длина квазипериода равна 3, коэффициент квазипериода равен $-64(\sqrt{3}+2)$*, длина периода равна 6. Непрерывная дробь элемента* $\sqrt{f}/x$ *имеет вид*

$$\frac{\sqrt{f}}{x} = \left[x+2;\ \overline{-\tfrac{x-4}{4\left(\sqrt{3}+2\right)}, -\tfrac{\sqrt{3}x+2x+8\sqrt{3}+15}{4}, 4\left(-26x+15\sqrt{3}x-4\sqrt{3}+7\right), \tfrac{\left(15\sqrt{3}+26\right)(x+2)}{32}, -\tfrac{8\left(-45x+26\sqrt{3}x-14+8\sqrt{3}\right)}{3}, -\tfrac{3\left(3x+2\sqrt{3}x+14\sqrt{3}+26\right)}{32}, -\tfrac{8\left(-3x+2\sqrt{3}x-12+6\sqrt{3}\right)}{27}, \tfrac{27(x+2)}{32}, \tfrac{4\left(-3x+\sqrt{3}x+6\right)}{27}, \tfrac{3\left(-3x+\sqrt{3}x-10\right)}{16}, \tfrac{-3x+\sqrt{3}x+4}{3}, \tfrac{x+2}{4}, -\sqrt{3}x+x+4, -\tfrac{-x+\sqrt{3}x+6}{16}, -4\left(-x+\sqrt{3}x-2\right), \tfrac{x+2}{32}, -8\left(x-4-2\sqrt{3}\right), \tfrac{-7x+4\sqrt{3}x-18+10\sqrt{3}}{32}, -8\left(4\sqrt{3}+7\right)(x-2), -\tfrac{\left(-26+15\sqrt{3}\right)(x+2)}{32}, -4\left(4\sqrt{3}x^2+7x^2-104-60\sqrt{3}\right), -\tfrac{-97x^3+56\sqrt{3}x^3-194x^2+112\sqrt{3}x^2-60\sqrt{3}x+104x-240\sqrt{3}+416}{128}, \overline{-4\left(4\sqrt{3}x^2+7x^2-104-60\sqrt{3}\right), -\tfrac{\left(-26+15\sqrt{3}\right)(x+2)}{32}, -8\left(4\sqrt{3}+7\right)(x-2), \tfrac{-7x+4\sqrt{3}x-18+10\sqrt{3}}{32}, -8\left(x-4-2\sqrt{3}\right), \tfrac{x+2}{32}, -4\left(-x+\sqrt{3}x-2\right), -\tfrac{-x+\sqrt{3}x+6}{16}, -\sqrt{3}x+x+4, \tfrac{x+2}{4}, \tfrac{-3x+\sqrt{3}x+4}{3}, \tfrac{3\left(-3x+\sqrt{3}x-10\right)}{16}, \tfrac{4\left(-3x+\sqrt{3}x+6\right)}{27}, \tfrac{27(x+2)}{32}, -\tfrac{8\left(-3x+2\sqrt{3}x-12+6\sqrt{3}\right)}{27}, -\tfrac{3\left(3x+2\sqrt{3}x+14\sqrt{3}+26\right)}{32}, -\tfrac{8\left(-45x+26\sqrt{3}x-14+8\sqrt{3}\right)}{3}, \tfrac{\left(15\sqrt{3}+26\right)(x+2)}{32}, 4\left(-26x+15\sqrt{3}x-4\sqrt{3}+7\right), -\tfrac{\sqrt{3}x+2x+8\sqrt{3}+15}{4}, -\tfrac{x-4}{4\left(\sqrt{3}+2\right)}, 2(x+2)}\right].$$

Длина квазипериода равна $N = 44$ *и совпадает с длиной периода. В данном примере при обозначениях теоремы 3.3.3.3 имеем* $s = 1$, $n = 12$, $v_x\left(\Omega_2^{(1)}\right) = \ldots = v_x\left(\Omega_2^{(11)}\right) = 0$, $v_x\left(\Omega_2^{(12)}\right) = 1$, $k = [K : \mathbb{Q}] = 2$ *и* $\varphi(n) \mid 2k$*. По следствию 3.3.3.6 имеем оценку на длину квазипериода* $N \leq nm - 2g = 46$.

Глава 4. Классификация эллиптических полей по принципу периодичности ключевых элементов

Пусть $F \in K[X]$ — свободный от квадратов многочлен четной степени $\deg F = 2g + 2$, и $\mathcal{L} = K(X)(\sqrt{F})$ — гиперэллиптическом поле. Для функциональных непрерывных дробей, построенных в поле $K((1/X))$, рассматриваемых в классических работах Абеля [127], Чебышева [129], Золотарева [180], Артина [131], известно, что в случае наличия периодических или квазипериодических элементов в $\mathcal{L}$ элемент $\sqrt{F}$ также будет периодическим (эквивалентные условия квазипериодичности см. в §3.2.1). Тем самым элемент $\sqrt{F}$, а также элементы вида $\sqrt{F}/X^s$, которые также могут быть периодическими при некоторых значениях $s \in \mathbb{Z}$ (см. следствие 3.3.3.5), играют ключевую роль в исследовании наличия периодических или квазипериодических элементов в поле $\mathcal{L}$. Элементы вида $\sqrt{F}/X^s$, $s \in \mathbb{Z}$, будем называть *ключевыми элементами* поля $\mathcal{L}$. Замена $(X, Y) \to (1/x, y/x^{g+1})$ ключевые элементы поля $\mathcal{L}$ переводит в ключевые элементы поля $L = K(x)(\sqrt{f})$, а бесконечные нормирования v_∞^- и v_∞^- в нормирования v_x^- и v_x^+. В частности, при такой замене элемент $\sqrt{F}$ переходит в $\sqrt{f}/x^{g+1}$, и, если изначально элемент $\sqrt{F}$ имел периодическое разложение в непрерывную дробь в $K((1/X))$, то элемент $\sqrt{f}/x^{g+1}$ тоже будет иметь периодическое разложение в непрерывную дробь в $K((x))$.

Основной целью этой главы является описание эллиптических полей L, обладающих периодическими ключевыми элементами при фиксированных значениях s.

В 2017 году В.П. Платонов в [19] сформулировал проблему классификации полей L по признаку периодичности непрерывных дробей, построенных в поле $K((x))$ для ключевых элементов вида $\sqrt{f}/x^s$, $s \in \mathbb{Z}$. Над конечным полем констант K ответ тривиально следует из следующего результата (см., например, [130]): любой элемент квадратичного функционального поля над конечным полем констант имеет периодическое разложение в непрерывную дробь.

В разделе 4.1 (дополнительно см. [17]) получено полное решение сформулированной проблемы классификации для эллиптических полей, заданных кубическими многочленами над полем $K = \mathbb{Q}$. В разделе 4.2 (дополнительно см. [8]) получено полное решение этого вопроса для эллиптических полей, заданных многочленами степени 4 над полем $K = \mathbb{Q}$. Наконец, в разделе 4.3 (дополнительно см. [4; 5]) получено решение этого вопроса для эллиптических

полей, заданных многочленами степени 4 над квадратичными полями K, и имеющих рациональную параметризацию модулярными кривыми.

В разделе 4.2 отмечено, что в случае четной степени многочлена f исследование проблемы классификации полей по признаку периодичности является значительно более трудоемким. Это связано со теоремой 3.3.3.3, в которой утверждается, что в случае четной степени многочлена f для поиска периодических элементов $\sqrt{f}$ недостаточно знания коэффициентов фундаментальной S-единицы, $S = \{v_x^-, v_x^+\}$, но также необходимо знание коэффициентов степеней n фундаментальной S-единицы, где число n пробегает конечное множество значений в зависимости от степени расширения $[K : \mathbb{Q}]$ (см. таблицу 3.1).

Проблема описания гиперэллиптических кривых рода $g \geq 2$ над $\mathbb{Q}$, якобиан которых содержит нетривиальную подгруппу кручения, не решена. Более того, над полем рациональных чисел проблема ограниченности порядков подгрупп кручения в якобианах гиперэллиптических кривых считается трудной даже для кривых рода два. Для эллиптических кривых, заданных многочленом $f \in \mathbb{Q}[x]$ степени 3 и 4 значения $s = 0$ и $s = \deg f$ в проблеме описания периодических ключевых элементов являются "пограничными" в том смысле, что не существует многочленов $f \in \mathbb{Q}[x]$, $3 \leq \deg f \leq 4$, для которых разложение $\sqrt{f}/x^s$ в непрерывную дробь периодично при $s < 0$ или $s > \deg f$, а при $0 \leq s \leq \deg f$ такие многочлены есть. В связи с этим, поиск многочленов $f \in \mathbb{Q}[x]$, $\deg f \geq 3$, для которых разложение $\sqrt{f}$ в непрерывную дробь в поле $\mathbb{Q}((x))$ периодично, имеет особый интерес.

Мы высказываем две гипотезы.

1. Для каждого $d \geq 3$ существует только конечное число свободных от квадратов многочленов $f \in \mathbb{Q}[x]$, $\deg f \leq d$, с периодическим разложением $\sqrt{f}$ в непрерывную дробь в поле $\mathbb{Q}((x))$ с точностью до эквивалентности, заданной заменой многочлена f на многочлен $a^2 f(bx^n)$ для некоторых $n \in \mathbb{N}$ и $a, b \in \mathbb{Q}^*$.

2. Для $d \geq 3$ и $s < 0$ или $s > d$ не существует свободных от квадратов многочленов $f \in \mathbb{Q}[x]$, $\deg f = d$, для которых разложение $\sqrt{f}/x^s$ в непрерывную дробь периодично.

Для $d = 3$ эти гипотезы доказаны в этой главе, а для $d = 4$ эти гипотезы доказаны в разделе 4.2. Данные гипотезы также могут рассматриваться при $d \geq 3$ над полями алгебраических чисел K.

Дадим краткий обзор других результатов, относящихся к проблеме классификации по признаку периодичности ключевых элементов. Отметим, что эти результаты в основном относятмя к эллиптическому случаю $d = \deg f = 3$, а также в [181] для $d = \deg f = 2g + 1$, $g \geq 1$.

К настоящему моменту над полями алгебраических чисел K, $[K : \mathbb{Q}] \geq 2$, приведенные гипотезы полностью доказаны только в случае $d = 3$ над квадратичными расширениями поля $\mathbb{Q}$ в статье [145] и над кубическими расширениями поля $\mathbb{Q}$ в статьях [143; 144]. Отметим,

что ранее в статье [182] были доказаны приведенные гипотезы для эллиптических полей, заданных кубическими многочленами над полями $K = \mathbb{Q}(\sqrt{5})$ и $K = \mathbb{Q}(\sqrt{-15})$. Для этих полей описание многочленов f с периодическим разложением $\sqrt{f}/x$ в непрерывную дробь в поле $K((x))$ отлично от соответствующего описания над полем рациональных чисел, но для них нет новых примеров многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь в поле $K((x))$. Однако для поля констант $K = \mathbb{Q}(\sqrt{21})$ в статье [182] найден новый пример многочлена $f \in K[x]$, $\deg f = 3$, с периодическим разложением $\sqrt{f}$ в непрерывную дробь в поле $K((x))$. Для произвольного поля K характеристики ноль в статьях [183; 184] с точностью до естественного отношения эквивалентности, заданного допустимыми заменами многочлена f на многочлен $a^2 f(bx^n)$, доказана конечность числа кубических многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь в поле $K((x))$, для которых соответствующая эллиптическая кривая содержит K-точку четного порядка, не превосходящего 18 или K-точку нечетного порядка не превосходящего 11. В [143] доказана теорема конечности для кубических многочленов $f \in K[x]$ с периодическим разложением $\sqrt{f}$ для расширений $\mathbb{Q}$ степени не более 6. Также в [143] получено описание периодических элементов $\sqrt{f}$ для кубических многочленов $f(x)$, определяющих эллиптические кривые с точками порядка $3 \leq N \leq 42$, $N \neq 37, 41$. Наконец, в [181] получено полное описание многочленов $f(x)$ нечетной степени $2g+1$ (вне зависимости от степени расширения $[K : \mathbb{Q}]$ и величины g), при условии, что степень k фундаментальной S-единицы, $S = \{v_x^-, v_x^+\}$, соответствующего гиперэллиптического поля $K(x)(\sqrt{f})$ не превосходит 12, а при четном значении k — не превосходит 20.

Доказательства основных результатов этой главы существенным образом опираются на компьютерные вычисления, с использованием символьных преобразований. В этой главе мы приводим необходимые теоретические сведения и рассуждения в виде схем доказательств указанных выше утверждений. На основании алгоритмов, следующих из приведенных схем, реализован программный код на языке Python с применением системы компьютерной алгебры Sympy [185; 186]. В частности, использовались базовые арифметические функции над кольцом многочленов $K[x]$, а также встроенные алгоритмы символьного вычисления дискриминанта многочлена относительно переменной x, разложения многочлена на множители, анализ и решение систем алгебраических уравнений с помощью базисов Гребнера. Без подобных вычислений получить заявленные результаты не представляется возможным.

4.1. Классификация эллиптических полей, заданных кубическим многочленом над полем рациональных чисел

В этом разделе получен следующий результат (дополнительно см. [17]): для квадратичных расширений, определяемых кубическими многочленами с коэффициентами из поля ра-

циональных чисел $\mathbb{Q}$: за исключением тривиальных случаев с точностью до эквивалентности существует только три кубических многочлена над $\mathbb{Q}$, квадратный корень из которых разлагается в периодическую непрерывную дробь в поле формальных степенных рядов $\mathbb{Q}((x))$ (теорема 4.1.3.1). Отметим, что в §4.1.1 эти три примера построены методом, основанным на решении системы полиномиальных уравнений, и более того, построены три семейства многочленов f_n степени n, $n \geq 3$, для которых $\sqrt{f_n}$ имеет периодическую непрерывную дробь в $\mathbb{Q}((x))$. В §4.1.3.1 с помощью символьных компьютерных вычислений и параметризации эллиптических кривых и точек конечного порядка над $\mathbb{Q}$ доказано, что других элементов вида $\sqrt{f}$, $f \in \mathbb{Q}[x]$, $\deg f = 3$, имеющих периодическое разложение в непрерывную дробь в $\mathbb{Q}((x))$, нет. Также показано, что не существует элементов вида $x\sqrt{f}$, $f \in \mathbb{Q}[x]$, $\deg f = 3$, для которых разложение в непрерывную дробь в $\mathbb{Q}((x))$ периодическое.

Результаты этого раздела опубликованы в статьях [17; 18].

4.1.1. Поиск примеров периодических непрерывных дробей $\sqrt{f}$

Неоднократно отмечалось (см. [18; 19; 140; 166]), что для полей алгебраических чисел K поиск многочленов $f \in K[x]$ с периодическим разложением $\sqrt{f}$ в непрерывную дробь в $K((x))$ является трудной задачей. Если многочлен $f \in K[x]$ обладает периодическим разложением $\sqrt{f(x)}$ в непрерывную дробь, $a, b \in \mathbb{Q}^*$, $n \in \mathbb{N}$, то и разложение $\sqrt{a^2 f(bx^n)}$ в непрерывную дробь также периодическое. Поэтому мы можем искать многочлены $f \in K[x]$ с точностью до указанной замены. Будем называть примеры многочленов $f \in K[x]$ с периодическим разложением $\sqrt{f}$ в непрерывную дробь *неэквивалентными*, если соответствующие им поля $K(x)(\sqrt{f})$ не являются изоморфными. Для фиксированного $n \in \mathbb{N}$ многочлены вида $cx^n + 1$, $c \in K^*$, дают бесконечную серию не изоморфных полей $K(x)(\sqrt{cx^n + 1})$ (см. [19]). Мы будем называть пример многочлена f с периодическим разложением $\sqrt{f}$ в непрерывную дробь *тривиальным*, если поле $K(x)(\sqrt{f})$ изоморфно некоторому полю вида $K(x)(\sqrt{cx^n + 1})$, где $c \in \mathbb{Q}^*$, $n \in \mathbb{N}$.

В этом разделе используются обозначения и результаты §3.2.2. Основной результат этого параграфа заключается в том, что для каждого $n \geq 3$ найдены 3 неэквивалентных нетривиальных примера $f_n \in \mathbb{Q}[x]$, $\deg f = n$, обладающих периодическим разложением $\sqrt{f_n}$ в непрерывную дробь.

Основные результаты этого раздела опубликованы в статье [19]. Отметим, что приведенные ниже примеры важны, поскольку в них найдены семейства многочленов f_n, для которых разложение $\sqrt{f_n}$ в непрерывную дробь в $\mathbb{Q}((x))$ периодическое. Ранее было известно лишь одно такое семейство вида $f_n = 1 + cx^n$, $c \in K^*$, $n \in \mathbb{N}$.

Перейдем к построению примеров свободных от квадратов многочленов $f \in \mathbb{Q}[x]$ и соответствующих полей $L = \mathbb{Q}(x)(\sqrt{f})$, для которых непрерывная дробь $\sqrt{f}$ периодическая. Такие

поля L встречаются довольно редко, они представляют особый интерес, а их поиск является достаточно трудной задачей. Мы получаем в каждом из примеров 4.1.1.1-4.1.1.4 различные периодические непрерывные дроби элементов вида $\sqrt{f}$ для любого $\deg f \geq 3$. Для краткости изложения численные примеры приведены только для $\deg f = 4$. Численные примеры для $\deg f = 5$ приведены в статье [19]. Примечательно, что все эти примеры найдены с помощью предложения 3.2.2.1 и без компьютерного перебора.

Пример 4.1.1.1. *Простейшим примером является многочлен* $f = bx^n + 1$, $b \in \mathbb{Q}^*$, $n \in \mathbb{N}$ *(для* $n = 2g + 1$ *этот пример рассмотрен в [166]) с разложением* $\sqrt{f}$ *в непрерывную дробь*

$$\sqrt{f} = \left[1; \frac{1}{2} + \frac{2}{bx^n}, \overline{-4 - \frac{8}{bx^n}, 1 + \frac{2}{bx^n}}\right].$$

Длина квазипериода равна 1, *коэффициент квазипериода* $c = -1/4$, *длина периода равна* 2, *степень фундаментальной* S_x*-единицы в поле* $L = \mathbb{Q}(x)(\sqrt{f})$ *равна* n, *если* n *нечетное, и* $n/2$, *если* n *четное.*

Если многочлен $f \in \mathbb{Q}[x]$ обладает периодическим разложением $\sqrt{f(x)}$ в непрерывную дробь, $a, b \in \mathbb{Q}^*$, $n \in \mathbb{N}$, то и разложение $\sqrt{a^2 f(bx^n)}$ в непрерывную дробь также периодическое. Мы будем искать многочлены $f \in \mathbb{Q}[x]$, обладающих периодическим разложением $\sqrt{f}$, с точностью до указанной замены.

Пример 4.1.1.2. *Пусть*

$$s_0 = 0,\ r = \deg f,\ \deg \mu_4 = \deg \mu_3 = 1,\ m_1 = \deg f + 2,\ \deg f_2 = \deg f,$$
$$f_2 = x^r + b_1 x^{r-1} + \ldots + b_r,\ f_1 = b,\ \mu_3 = x + e,\ \mu_4 = x + 1,\ b, e \in K^*,$$

тогда (3.2.2.3) *дает следующие рекуррентные условия на коэффициенты* b, e *и* b_j*:*

$$b_0 = 1, \quad b_1 + 2b_0 = 0, \quad b_j + 2b_{j-1} + b_{j-2} = 0, \quad j = 2, 3, \ldots, r-1, \tag{4.1.1.1}$$
$$b_r + 2b_{r-1} + b_{r-2} = b, \quad 2b_r + b_{r-1} = 2be, \quad b_r = be^2. \tag{4.1.1.2}$$

Коэффициенты $b_0, b_1, \ldots, b_{r-1}$ *определяем из* (4.1.1.1), *а из* (4.1.1.2) *имеем*

$$b_r = \frac{b_{r-1}^2}{4(b_{r-1} + b_{r-2})}, \quad b = \frac{(3b_{r-1} + 2b_{r-2})^2}{4(b_{r-1} + b_{r-2})}, \quad e = \frac{b_{r-1}}{3b_{r-1} + 2b_{r-2}}.$$

Произведя вычисления для $\deg f = 4$, *получаем* $f = -x^4 + 2x^3 - 3x^2 + 4x + 4$. *Сделаем замену* $f := (1/2)^2 f(2x)$, *тогда*

$$f = -4x^4 + 4x^3 - 3x^2 + 2x + 1,$$

и разложение $\sqrt{f}$ *в непрерывную дробь имеет вид*

$$\sqrt{f} = \Big[1; 2 + \tfrac{1}{x}, \overline{-1 + \tfrac{1}{2x} - \tfrac{1}{4x^2} + \tfrac{1}{8x^3} + \tfrac{1}{8x^4}, \tfrac{5}{2} + \tfrac{1}{x}},$$
$$\overline{-10 - \tfrac{4}{x}, \tfrac{1}{4} - \tfrac{1}{8x} + \tfrac{1}{16x^2} - \tfrac{1}{32x^3} - \tfrac{1}{32x^4}, -10 - \tfrac{4}{x}, \tfrac{5}{2} + \tfrac{1}{x}}\Big].$$

Длина квазипериода равна 3, *коэффициент квазипериода* $c = -1/4$, *длина периода равна* 6. *Непрерывная дробь* $\sqrt{f}/x^2$ *имеет вид*

$$\frac{\sqrt{f}}{x^2} = \left[-2 + \frac{1}{x} + \frac{1}{x^2};\ \overline{\frac{1}{2} + \frac{1}{4x}, -4 + \frac{2}{x} + \frac{2}{x^2}}\right].$$

Длина квазипериода совпадает с длиной периода и равна 2. *Фундаментальная* S_x*-единица и имеет вид*

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

$u \cdot \overline{u} = 1$, *степень фундаментальной* S_x*-единицы и равна* 3.

Пример 4.1.1.3. *Пусть* $s_0 = 0$, $r = \deg f$, $\deg f_2 = \deg d_0 - 1$, $\deg \mu_4 = 1$, $\mu_3 = 1$, $m_1 = \deg d_0 + 1$, $\deg f_1 = 1$. *Положим* $f_1 = b_0 + b_1 x$, *тогда многочлен* $x^{m_1} + b_1 x + b_0$ *должен иметь кратный корень. При* $b_1 = -m_1$, $b_0 = m_1 - 1$ *данное требование достигается:*

$$x^{m_1} - m_1 x + m_1 - 1 = (x^{m_1-2} + 2x^{m_1-3} + \ldots + (m_1 - 1))(x-1)^2,$$

$$f_1 = m_1 - 1 - m_1 x, \quad f_2 = x^{m_1-2} + 2x^{m_1-3} + \ldots + (m_1 - 1), \quad \mu_4 = x - 1.$$

Искомое решение имеет вид:

$$\mu_1 = x^{m_1} - 2m_1 x + 2(m_1 - 1), \quad \mu_2 = x - 1,$$
$$f = 4(m_1 - 1)^2 - 4\sum_{j=1}^{m_1-1}(2m_1 - (j+1))x^j.$$

Для $\deg f = 4$ *получаем* $f = -5x^4 - 6x^3 - 7x^2 - 8x + 16$. *Сделаем замену* $f := (1/4)^2 f(-4x)$, *тогда*

$$f = -80x^4 + 24x^3 - 7x^2 + 2x + 1,$$

и разложение $\sqrt{f}$ *в непрерывную дробь имеет вид*

$$\sqrt{f} = \left[1; 4 + \frac{1}{x},\ \overline{-\frac{1}{2} + \frac{1}{8x} - \frac{1}{32x^2} + \frac{1}{128x^3}, \frac{9}{2} + \frac{1}{x}},\right.$$
$$\left.\overline{-18 - \frac{4}{x}, \frac{1}{8} - \frac{1}{32x} + \frac{1}{128x^2} - \frac{1}{512x^3}, -18 - \frac{4}{x}, \frac{9}{2} + \frac{1}{x}}\right].$$

Длина квазипериода равна 3, *коэффициент квазипериода* $c = -1/4$, *длина периода равна* 6. *Непрерывная дробь* $\sqrt{f}/x^2$ *имеет вид*

$$\frac{\sqrt{f}}{x^2} = \left[-4 + \frac{1}{x} + \frac{1}{x^2};\ \overline{\frac{1}{4} + \frac{1}{16x}, -8 + \frac{2}{x}, \frac{1}{4} + \frac{1}{16x}, -8 + \frac{2}{x} + \frac{2}{x^2}}\right].$$

Длина квазипериода совпадает с длиной периода и равна 4. *Фундаментальная* S_x*-единица и имеет вид*

$$u = \frac{1}{x^5}\left(-x^5 + \frac{5x}{128} + \frac{1}{128} + \left(\frac{x}{32} + \frac{1}{128}\right)\sqrt{f}\right),$$

$u \cdot \overline{u} = 1$, *степень фундаментальной* S_x*-единицы и равна* 5.

Пример 4.1.1.4. *Пусть* $s_0 = 0$, $r = \deg f$, $\deg f_2 = 1$, $\deg \mu_4 = \deg f - 1$, $\mu_3 = 1$, $m_1 =$

$2\deg f-1$, $\deg f_1=\deg f-1$. *Положим*

$$f_1=b_0x^{r-1}+b_1x^{r-2}+\ldots+b_{r-1},\ \ f_2=x+1,\ \ \mu_4=c_0x^{r-1}+c_1x^{r-2}+\ldots+c_{r-1},$$

тогда (3.2.2.3) *дает следующие рекуррентные условия на коэффициенты* c_j *и* b_j*:*

$$c_0=1,\quad 2c_j+S'_j(\overline{c})+S_{j-1}(\overline{c})=0,\quad j=1,2,\ldots,r-1,$$

$$S_j(\overline{c})+S_{j-1}(\overline{c})=b_{j-r},\quad c_j=0,\quad j=r,r+1,\ldots,m_1,$$

$$\text{где}\quad S_n(\overline{c})=\sum_{j=0}^{n}c_jc_{n-j},\quad S'_n(\overline{c})=\sum_{j=1}^{n-1}c_jc_{n-j}.$$

Произведя вычисления для $\deg f=4$, *получаем* $f=-140x^4-168x^3+84x^2-80x+400$. *Сделаем замену* $f:=(1/20)^2f(-10x)$, *тогда*

$$f=-3500x^4+420x^3+21x^2+2x+1,$$

и разложение $\sqrt{f}$ *в непрерывную дробь имеет вид*

$$\sqrt{f}=\Big[1;-10+\tfrac{1}{x},\overline{-\tfrac{1}{2}-\tfrac{1}{100x},\tfrac{17}{10}-\tfrac{1}{20x},-60+\tfrac{10}{x},\tfrac{17}{10}-\tfrac{1}{20x},-\tfrac{1}{2}-\tfrac{1}{100x},-\tfrac{19}{2}+\tfrac{1}{x},}$$
$$\overline{38-\tfrac{4}{x},\tfrac{1}{8}+\tfrac{1}{400x},-\tfrac{34}{5}+\tfrac{1}{5x},15-\tfrac{5}{2x},-\tfrac{34}{5}+\tfrac{1}{5x},\tfrac{1}{8}+\tfrac{1}{400x},38-\tfrac{4}{x},-\tfrac{19}{2}+\tfrac{1}{x}}\Big].$$

Длина квазипериода равна 7, *коэффициент квазипериода* $c=-1/4$, *длина периода равна* 14. *Непрерывная дробь* $\sqrt{f}/x^2$ *имеет вид*

$$\tfrac{\sqrt{f}}{x^2}=\Big[10+\tfrac{1}{x}+\tfrac{1}{x^2};\overline{\tfrac{1}{20}+\tfrac{1}{200x},-20+\tfrac{2}{x},\tfrac{3}{20}+\tfrac{1}{40x},-20+\tfrac{2}{x},\tfrac{1}{20}+\tfrac{1}{200x},20+\tfrac{2}{x}+\tfrac{2}{x^2}}\Big].$$

Длина квазипериода совпадает с длиной периода и равна 6. *Фундаментальная* S_x*-единица и имеет вид*

$$u=\tfrac{1}{x^7}\left(-x^7+\tfrac{7x^3}{4000}+\tfrac{7x^2}{50000}+\tfrac{7x}{400000}+\tfrac{1}{400000}+\left(\tfrac{x^3}{1000}+\tfrac{x^2}{10000}+\tfrac{3x}{200000}+\tfrac{1}{400000}\right)\sqrt{f}\right),$$

$u\cdot\overline{u}=1$, *степень фундаментальной* S_x*-единицы и равна* 7.

Отметим, что гиперэллиптические поля $\mathbb{Q}(x)(\sqrt{f})$ для многочленов $f\in\mathbb{Q}[x]$, $\deg f=4$, построенных в примерах 4.1.1.1 - 4.1.1.4, не являются изоморфными.

4.1.2. Примеры многочленов f степени 2, обладающих периодическим разложением $\sqrt{f}$ в непрерывную дробь

Пусть K — поле характеристики отличной от 2. Пусть $f=c_2x^2+2c_1x+c_0\in K[x]$, причем $c_2\neq0$, $c_1^2-c_0c_2\neq0$ и c_2 является полным квадратом в K^*, $c_2=\gamma^2$. Поле $L=K(x)(\sqrt{f})$ изоморфно $K(x)(\sqrt{1-dx^2})$, где $d=c_1^2-c_0c_2\neq0$. Элемент $\sqrt{1-dx^2}$ имеет периодическое разложение в непрерывную дробь в $K((x))$, откуда следует разрешимость норменного уравнения $\omega_1^2-\omega_2^2f=bx^2$:

$$\omega_1=\gamma+\frac{c_1}{\gamma}x,\quad \omega_2=1,\quad b=\frac{c_1^2}{\gamma^2}-c_2.$$

В силу замен вида $a^2 f(bx)$ для многочлена $f(x)$, не влияющих на периодичность разложения в непрерывную дробь, мы можем без ограничения общности считать $c_1 = c_0 = 1$ или $c_1 = 0$, $c_0 = 1$.

По теореме 3.2.1.3 непрерывная дробь $\sqrt{f}/x$ периодическая, она имеет вид

$$\sqrt{f}/x = \left[\frac{1}{2} + \frac{1}{x};\ \overline{\frac{4x+8}{4c_0x - x}, 1 + \frac{2}{x}}\right].$$

Однако, в отличие от случая $\deg f = 1$, для $\deg f = 2$ не для каждого многочлена $f(x)$, для которого нормирование v_x поля $\mathbb{Q}(x)$ имеет два продолжения на $L = \mathbb{Q}(x)(\sqrt{f})$, непрерывная дробь $\sqrt{f}$ периодическая. Далее приведены примеры многочленов $f = c_0x^2 + 2x + 1$ с периодическим разложением $\sqrt{f}$ в непрерывную дробь.

Пример 4.1.2.1. *При* $c_0 = -3$ *имеем* $f = -3x^2 + 2x + 1$,

$$\sqrt{f} = \left[1; 2 + \tfrac{1}{x},\ \overline{-1 + \tfrac{1}{2x}, \tfrac{5}{2} + \tfrac{1}{x}, -10 - \tfrac{4}{x}, \tfrac{1}{4} - \tfrac{1}{8x}, -10 - \tfrac{4}{x}, \tfrac{5}{2} + \tfrac{1}{x}}\right].$$

При $c_0 = -1$ *имеем* $f = -x^2 + 2x + 1$,

$$\sqrt{f} = \left[1; 1 + \tfrac{1}{x},\ \overline{-2 + \tfrac{2}{x} + \tfrac{2}{x^2}, \tfrac{3}{2} + \tfrac{1}{x}, -6 - \tfrac{4}{x}, \tfrac{1}{2} - \tfrac{1}{2x} - \tfrac{1}{2x^2}, -6 - \tfrac{4}{x}, \tfrac{3}{2} + \tfrac{1}{x}}\right].$$

При $c_0 = -1/3$ *имеем* $f = -x^2/3 + 2x + 1$,

$$\sqrt{f} = \left[1; \tfrac{2}{3} + \tfrac{1}{x},\ \overline{-6 - \tfrac{9}{2x}, \tfrac{4}{9} - \tfrac{2}{3x} - \tfrac{2}{3x^2}, -6 - \tfrac{9}{2x}, \tfrac{7}{6} + \tfrac{1}{x}, \\ -\tfrac{14}{3} - \tfrac{4}{x}, \tfrac{3}{2} + \tfrac{9}{8x}, -\tfrac{16}{9} + \tfrac{8}{3x} + \tfrac{8}{3x^2}, \tfrac{3}{2} + \tfrac{9}{8x}, -\tfrac{14}{3} - \tfrac{4}{x}, \tfrac{7}{6} + \tfrac{1}{x}}\right].$$

4.1.3. Описание многочленов f степени 3, обладающих периодическим разложением $\sqrt{f}$ в непрерывную дробь

Основным результатом этого параграфа является следующая теорема.

Теорема 4.1.3.1. *1. Количество нетривиальных неэквивалентных свободных от квадратов многочленов* $f \in \mathbb{Q}[x]$, $\deg f = 3$, *имеющих периодическое разложение* $\sqrt{f}$ *в непрерывную дробь, не превосходит* 3.

2. Следующие нетривиальные неэквивалентные примеры свободных от квадратов многочленов $f \in \mathbb{Q}[x]$, $\deg f = 3$, *имеют периодическое разложение* $\sqrt{f}$ *в непрерывную дробь:*

$$f = 12x^3 - 8x^2 + 4x + 1, \quad f = 12x^3 - 5x^2 + 2x + 1, \quad f = -120x^3 + 25x^2 + 2x + 1.$$

Доказательство. Мы сперва кратко опишем общую структуру доказательства теоремы 4.1.3.1, а затем отдельно рассмотрим все возникающие случаи.

Для доказательства теоремы 4.1.3.1 мы сначала выписываем в параметрическом виде все многочлены $f(x)$, $\deg f = 3$, такие, что в группе классов дивизоров степени ноль $\Delta^\circ(L)$

гиперэллиптического поля $L = \mathbb{Q}(x)(\sqrt{f})$ порядок класса дивизора $P_x^- - P_x^+$ равен n, где точки $P_x^\pm$ соответствуют нормированиям $v_x^\pm$. Последнее условие равносильно тому, что точки P_x^- и P_x^+ имеют порядок n на эллиптической кривой $C_n(\mathbb{Q})$, заданной уравнением $C_n:\ y^2 = f(x)$. Согласно теореме Мазура [33] достаточно рассматривать $2 \le n \le 10$, $n = 12$.

Для $n > 4$ мы воспользуемся известной параметризацией [35]. Напомним, что *нормальная форма Тейта* уравнения неособой плоской кубической кривой имеет вид $Y^2 + (1-c)XY - bY = X^3 - bX^2$ с дискриминантом $\Delta = b^3(16b^2 - 8bc^2 - 20bc + b + c^4 - 3c^3 + 3c^2 - c)$. В статье [35] для $n \in \{4, 5, 6, 7, 8, 9, 10, 12\}$ приведена явная параметризация $b = b(t)$, $c = c(t)$ всех эллиптических кривых $C_n = C_{n,t}$, заданных в нормальной форме Тейта с точкой $(0, 0)$ порядка n. С помощью замены $y = Y + \frac{(1-c)X-b}{2}$, $x = X$ мы можем для кривой C_n получить параметрическое уравнение вида $y^2 = f(x)$ с точкой $P = (x_1, y_1) = (0, \sqrt{f(0)})$ порядка n. Если $n \in \{8, 10, 12\}$, то мы также должны рассмотреть точку $[2]P$ порядка $n/2$, и если $n \in \{9, 12\}$, то еще мы должны рассмотреть точку $[3]P$. Для того, что найти координаты точек $[2]P$ и $[3]P$, мы должны привести уравнение эллиптической кривой $y^2 = f(x)$ к короткой форме Вейерштрасса $y^2 = x^3 + ax + b$ и воспользоваться известными формулами для $P = (x_1,\ y_1)$ и $Q = (x_2,\ y_2)$:

$$P \ne \pm P,\ [2]P = (x_3,\ y_3):\ x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1,\ y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1, \quad (4.1.3.1)$$

$$P \ne \pm Q,\ P \oplus Q = (x_3,\ y_3):\ x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2,\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1. \quad (4.1.3.2)$$

Итак, для каждого n такого, что $2 \le n \le 10$, $n = 12$, мы имеем однопараметрическое семейство многочленов $f(x) = f_{n,t}(x)$ с параметром $t \in \mathbb{Q}$. Далее мы хотим найти все подходящие значения параметра t такие, что непрерывная дробь $\sqrt{f}$ периодическая. Для этого можно воспользоваться предложением 3.2.3.4 (см. также [17], предложение 4). Но за счет того, что степень многочлена f нечетная, нам удобнее по аналогии с предложением 3.2.3.4 воспользоваться исследованием периодической непрерывной дроби $\sqrt{f}/x$ и соответствующих подходящих дробей p_j/q_j. Оказывается, что в этом случае $v_{x^{-1}}(p_j) = 0$ и $v_{x^{-1}}(q_j) \ge 1$, где номер j соответствует концу периода непрерывной дроби $\sqrt{f}/x$. Поэтому для перечисления примеров многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь, согласно теореме 3.2.1.3, нужно найти все значения параметра $t \in \mathbb{Q}$ такие, что $v_{x^{-1}}(q_j) \ge 2$.

Вычисления, связанные с поиском параметризации многочленов f для $n \le 4$, а также непосредственное рассмотрение каждого из случаев $2 \le n \le 10$, $n = 12$, см. в статье [17].

Теорема 4.1.3.1 доказана. □

Отметим, что в случае четной степени многочлена f мы не можем рассуждать точно также, как мы рассуждали при доказательстве теоремы 4.1.3.1. Основная проблема заклю-

чается в том, что мы существенным образом использовали на теорему 3.2.1.3, опирающуюся на лемму 3.2.1.2. Для четной степени f лемма 3.2.1.2 не позволяет получить аналогичный результат. По этой причине пункт 2 теоремы 3.2.1.3 верен только для нечетной степени f (см. пример 3.2.1.4). В следующем параграфе мы преодолеваем эти трудности и решаем проблему классификации для случая $\deg f = 4$, $K = \mathbb{Q}$.

4.2. Классификация эллиптических полей, заданных многочленом четвертой степени над полем рациональных чисел

Классическая проблема периодичности непрерывных дробей элементов гиперэллиптических полей имеет большую и глубокую историю. До сих пор эта проблема была далека от полного решения. В разделе 4.1 для квадратичных расширений, определяемых кубическими многочленами с коэффициентами из поля рациональных чисел $\mathbb{Q}$, доказано, что за исключением тривиальных случаев с точностью до эквивалентности существует только три кубических многочлена над $\mathbb{Q}$, квадратный корень из которых разлагается в периодическую непрерывную дробь в поле формальных степенных рядов $\mathbb{Q}((x))$.

В.П. Платонов в [19] поставил вопрос о классификации полей $L = K(x)(\sqrt{f})$ по признаку периодичности ключевых элементов $\sqrt{f}$ для непрерывных дробей, построенных в поле $K((x))$, где K — поле алгебраических чисел. В этом разделе представлено полное решение проблемы классификации многочленов f, с периодическим разложением $\sqrt{f}$ в непрерывную дробь для эллиптических полей L, заданных многочленом f четвертой степени, с полем рациональных чисел в качестве поля констант.

Результаты этого раздела опубликованы в статьях [8; 12].

4.2.1. Формулировка основных результатов

Важную роль в разделе 4.1 играет теорема 3.2.1.3, в которой по данному элементу $\alpha \in L$ с квазипериодическим разложением в непрерывную дробь найден промежуток таких значений s, что элемент $\alpha \cdot x^s$ имеет квазипериодическое разложение в непрерывную дробь. Для случая, когда степень многочлена f нечетная в той же теореме доказано, что этот промежуток точный, а случай четной степени многочлена f оказался более сложным: в некоторых особых случаях могут существовать значения s, не принадлежащие найденному промежутку, такие, что непрерывная дробь элемента $\alpha \cdot x^s$ квазипериодическая. В теореме 3.3.3.3 найдены необходимые и достаточные условия периодичности непрерывных дробей ключевых элементов для случая четной степени многочлена f.

Далее мы покажем, что в поле L могут существовать элементы, имеющие периодическую непрерывную дробь, построенную в поле $K((1/X))$, с длиной квазипериода существенно боль-

ше, чем порядок класса дивизора $(\infty^- - \infty^+)$ в группе классов дивизоров степени ноль $\Delta^\circ(L)$ поля L. Этот эффект возникает только в случае гиперэллиптических полей L, заданных многочленами f четной степени и объясняется результатом теоремы 3.3.3.3. Частные примеры непрерывных дробей, построенных по конечному нормированию в поле $\mathbb{Q}((x))$, для которых длина квазипериода существенно больше степени соответствующего дивизора кручения, были приведены в статьях [14; 17].

Приведем основной результат этого раздела.

Теорема 4.2.1.1. *С точностью до отношения эквивалентности, определенного допустимыми заменами многочлена $f(x)$ на $a^2 f(bx)$ для $a, b \in \mathbb{Q}^*$, множество свободных от квадратов многочленов $f \in \mathbb{Q}[x]$, $\deg f = 4$, для которых разложение $\sqrt{f}$ в непрерывную дробь в поле $\mathbb{Q}((x))$ периодично, описывается семью многочленами*

$$(1-2x)(1+6x+32x^3),$$
$$(1-2x)(1+6x+96x^3),$$
$$(1-2x)(1+6x+32x^3/3),$$
$$1-2x-2x^2-3x^3-3x^4/4,$$
$$(1+10x)(1-6x+32x^2-128x^3),$$
$$(27+144x+320x^2)(9-72x+400x^2)/243,$$
$$(1-10x)(1+14x+224x^2+5600x^3),$$

и четырьмя семействами многочленов:

$$c_1x^4+1,$$
$$-c_2^2x^4+2c_2x^2+1,$$
$$(-c_3x^2+1)(3c_3x^2+1),$$
$$-c_4^2x^4/3+2c_4x^2+1,$$

где параметр $c_1 \in \mathbb{Z} \setminus \{0\}$ свободен от четвертых степеней, параметры $c_2, c_3, c_4 \in \mathbb{Z} \setminus \{0\}$ свободны от квадратов.

Теорема 4.2.1.1 была анонсирована в статье [12], а полное доказательство приведено в статье [8].

Доказательство теоремы 4.2.1.1 существенным образом опирается на большие символьные компьютерные вычисления. Схема доказательства приведена в §4.2.5. Подробный разбор каждого случая, возникающего в схеме доказательства см. в [8].

Периодичность непрерывной дроби элемента $\sqrt{f}/x^s$ влечет периодичность непрерывной дроби элемента $\sqrt{f}/x^{\deg f - s}$ (см. теорему 3.3.3.3), поэтому для решения проблемы описания периодических ключевых элементов достаточно рассматривать только элементы вида $\sqrt{f}/x^s$,

$s \le g+1$.

Для $\deg f = 2g+2$ в проблеме описания периодических ключевых элементов в $\mathbb{Q}((x))$ путем преобразований $X = 1/x$, $F = X^4 f(1/X)$ получаем, что случай $s = g+1$ эквивалентен описанию свободных от квадратов многочленов $F \in \mathbb{Q}[X]$, $\deg F = 2g+2$, для которых разложение в поле $\mathbb{Q}((1/X))$ элемента $\sqrt{F}$ в непрерывную дробь периодично. Параметрическое описание многочленов $F \in \mathbb{Q}[X]$ четвертой степени с периодическим разложением $\sqrt{F}$ в непрерывную дробь в поле $\mathbb{Q}((1/X))$ приведено, например, в [69]. В случае $s = 1$ найденные в теореме 4.2.4.1 условия связывают два параметра, задающих коэффициенты многочлена F, в одно полиномиальное уравнение над полем $\mathbb{Q}$. Поэтому множество многочленов $F \in \mathbb{Q}[X]$ четвертой степени с периодическим разложением $X\sqrt{F}$ в непрерывную дробь в поле $\mathbb{Q}((1/X))$ описывается рациональными точками на специальных кривых для каждого порядка m, $2 \le m \le 12$, $m \ne 11$, класса дивизора $(\infty^- - \infty^+)$ в группе классов дивизоров степени ноль $\Delta^\circ(\mathcal{L})$ поля $\mathcal{L} = \mathbb{Q}(X)(\sqrt{F})$. В случае $s = 0$ два параметра, задающих коэффициенты многочлена F, становятся связаны системой двух полиномиальных соотношений, которую удается решить с применением компьютерной алгебры (подробности см. в пункте 4.2.5). Таким образом, получается множество многочленов $F \in \mathbb{Q}[X]$ четвертой степени с периодическим разложением $X^2\sqrt{F}$ в непрерывную дробь в поле $\mathbb{Q}((1/X))$, откуда следует результат теоремы 4.2.1.1 с помощью преобразования $f = x^4 F(1/x)$.

Для каждого многочлена f (или семейства многочленов), найденных в теореме 4.2.1.1, вычисления показывают, что непрерывная дробь элемента $x\sqrt{f}$ не является периодической, поскольку в случае периодичности длина квазипериода не должна превосходить степень фундаментальной S-единицы, умноженную на 6 (см. таблицу 3.1).

Теорема 4.2.1.2. *В случае $s < 0$ или $s > 4$ не существует многочленов $f \in \mathbb{Q}[x]$, $\deg f = 4$, для которых разложение $\sqrt{f}/x^s$ в непрерывную дробь в поле $\mathbb{Q}((x))$ периодично.*

4.2.2. Слабый критерий периодичности ключевых элементов

Пусть β является корнем неприводимого многочлена

$$\Lambda_2 Z^2 + 2\Lambda_1 Z + \Lambda_0 \in K[X][Z], \quad \text{где } \Lambda_0, \Lambda_1, \Lambda_2 \in K[X], \quad (\Lambda_0,\ \Lambda_1,\ \Lambda_2) \in K^*. \tag{4.2.2.1}$$

Пусть $D(\beta) = \Lambda_1^2 - \Lambda_2\Lambda_0 = \Theta^2 F$, где $F \in K[X]$ — свободная от квадратов часть $D(\beta)$. Если $D(\beta) \ne 0$, то величину $D(\beta)$ будем называть *дискриминантом* квадратичной иррациональности β.

Согласно теореме 2 [118] элемент β имеет квазипериодическую непрерывную дробь в поле $K((1/X))$ тогда и только тогда, когда для дискриминанта $D(\beta)$ справедливо соотношение

$$\Omega_1^2 - \Omega_2^2 \cdot D(\beta) \in K^* \tag{4.2.2.2}$$

для некоторых ненулевых многочленов $\Omega_1, \Omega_2 \in K[X]$. Заметим, что из (4.2.2.2) следует равенство

$$\left(\Omega_1^2 + \Omega_2^2 D(\beta)\right)^2 - (2\Omega_1\Omega_2)^2 \cdot D(\beta) \in K^*,$$

причем, если $v_X(\Omega_1\Omega_2) = \max\{v_X(\Omega_1),\ v_X(\Omega_2)\} > 0$, то $v_X(\Omega_1^2 + D(\beta)\Omega_2^2) = 0$. Следовательно, без ограничения общности в соотношении (4.2.2.2) можно требовать дополнительное условие $v_X(\Omega_1) = 0$.

Результаты следующей теоремы аналогичны объединению результатов теоремы 2 статьи [17] и в теоремы 1 статьи [14], в которых рассматриваются непрерывные дроби, построенные по конечному нормированию.

Теорема 4.2.2.1. *Пусть для элемента $\beta \in \mathcal{L} = K(X)(\sqrt{F})$ с дискриминантом $D(\beta) = \Theta^2 F$ непрерывная дробь, построенная в поле $K((1/X))$, квазипериодическая, причем справедливо соотношение (4.2.2.2) для некоторых многочленов $\Omega_1, \Omega_2 \in K[X]$ таких, что $v_X(\Omega_1) = 0$, $\Omega_2 \neq 0$. Тогда справедливы следующие утверждения:*

1. *если $s \in \mathbb{Z}$ удовлетворяет неравенствам*

$$-v_X(\Lambda_0) - v_X(\Omega_2) \leq s \leq v_X(\Omega_2) + v_X(\Lambda_2), \tag{4.2.2.3}$$

   то непрерывная дробь элемента $\beta \cdot X^s$ квазипериодическая;

2. *если $v_X(F) > 0$ и s не удовлетворяет неравенствам (4.2.2.3), то непрерывная дробь элемента $\beta \cdot X^s$ не квазипериодическая;*

3. *если $v_X(F) = 0$ и фундаментальная единица $\Psi_1 + \Psi_2\sqrt{F}$, где $\Psi_1, \Psi_2 \in K[X]$, в поле $\mathcal{L}$ такая, что $v_X(\Psi_1) > 0$ или $v_X(\Psi_2) > 0$, то для s, не удовлетворяющим неравенствам (4.2.2.3), непрерывная дробь элемента $\beta \cdot X^s$ не квазипериодическая.*

Доказательство. Предположим, что $s \in \mathbb{Z}$ удовлетворяет неравенствам (4.2.2.3). Положим

$$q = \min\left(v_X(\Lambda_2) - s,\ v_X(\Lambda_1),\ v_X(\Lambda_0) + s\right), \tag{4.2.2.4}$$

тогда элемент $\beta \cdot X^s$ является корнем квадратного уравнения

$$\Lambda_2 X^{-s-q} Z^2 + 2\Lambda_1 X^{-q} Z + \Lambda_0 X^{s-q} = 0, \tag{4.2.2.5}$$

с дискриминантом $D(\beta \cdot X^s) = D/X^{2q}$, причем $\Lambda_2 X^{-s-q}, \Lambda_1 X^{-q}, \Lambda_0 X^{s-q} \in K[X]$ и $(\Lambda_2 X^{-s-q},\ \Lambda_1 X^{-q}, K^*$. Из (4.2.2.3) и (4.2.2.4) имеем

$$\min\Big(v_X(\Lambda_2) - \big(v_X(\Omega_2) + v_X(\Lambda_2)\big),\ v_X(\Lambda_1),\ v_X(\Lambda_0) + \big(-v_X(\Lambda_0) - v_X(\Omega_2)\big)\Big) \leq q, \tag{4.2.2.6}$$

то есть $-q \leq v_X(\Omega_2)$. Отсюда получаем, что $D(\beta \cdot X^s) \mid \Omega_2^2 \cdot D(\beta)$, и, следовательно, непрерывная дробь элемента $\beta \cdot X^s$ квазипериодическая.

Пусть $\Psi_1 + \Psi_2\sqrt{F}$ фундаментальная единица кольца целых $\mathcal{O}_F$ поля $\mathcal{L}$. Для произвольной нетривиальной единицы $\omega_1 + \omega_2\sqrt{F}$ кольца $\mathcal{O}_F$ для некоторых $c \in K^*$ и $n \in \mathbb{Z}$ справедливо

равенство $\omega_1+\omega_2\sqrt{F}=c(\Psi_1+\Psi_2\sqrt{F})^n$. Домножая при необходимости ω_2 на -1 и изменяя константу c, без ограничения общности можно считать, что $n\in\mathbb{N}$ и выполнены равенства

$$\omega_1+\omega_2\sqrt{F}=c(\Psi_1+\Psi_2\sqrt{F})^n=$$
$$=\sum_{0\le j\le n/2}\binom{n}{2j}c\Psi_1^{n-2j}\Psi_2^{2j}F^j+\left(\sum_{0\le j<n/2}\binom{n}{2j+1}c\Psi_1^{n-2j-1}\Psi_2^{2j+1}F^j\right)\sqrt{F}=$$
$$=\left(c\Psi_1^n+\binom{n}{2}c\Psi_1^{n-2}\Psi_2^2F+\dots\right)+\left(nc\Psi_1^{n-1}\Psi_2+\binom{n}{3}c\Psi_1^{n-3}\Psi_2^3F+\dots\right)\sqrt{F}. \qquad (4.2.2.7)$$

Кроме того, можно считать, что постоянная c и $n\in\mathbb{N}$ подобраны так, что $\omega_1=\Omega_1$, $\omega_2=\Theta\cdot\Omega_2$. Если выполнено условие $v_X(F)>0$ или $v_X(\Psi_2)>0$, то в силу $\Psi_1^2-\Psi_2^2F\in\mathbb{K}^*$ имеем $v_X(\Psi_1)=0$, следовательно, из (4.2.2.7) получаем $v_X(\omega_1)=0$, $v_X(\omega_2)=v_X(\Psi_2)$. Если $v_X(F)=0$ и $v_X(\Psi_1)>0$, то $v_X(\Psi_2)=0$, и при четном n имеем $v_X(\omega_1)=0$, $v_X(\omega_2)=v_X(\Psi_1)$, а при нечетном n имеем $v_X(\omega_1)=v_X(\Psi_1)$, $v_X(\omega_2)=0$. В последнем случае при нечетном n можно рассмотреть $\omega_1^{(2n)}+\omega_2^{(2n)}\sqrt{F}=\left(\omega_1+\omega_2\sqrt{F}\right)^2$, тогда $v_X\left(\omega_1^{(2n)}\right)=0$, $v_X\left(\omega_2^{(2n)}\right)=v_X(\Psi_1)$.

Тем самым, если $v_X(F)>0$ или $v_X(\Psi_1)>0$ или $v_X(\Psi_2)>0$, то $v_X\left(\omega_1^{(2n)}\right)=0$, $v_X\left(\omega_2^{(2n)}\right)=\max\{v_X(\Psi_1),\ v_X(\Psi_2)\}$. Значит, при таких условиях непрерывная дробь элемента $\beta\cdot X^s$ квазипериодическая тогда и только тогда, когда $D(\beta\cdot X^s)\mid\Omega_2^2\cdot D(\beta)$, что равносильно неравенству $v_X(\Omega_2)+q\ge 0$. Таким образом, для s, не удовлетворяющих неравенствам (4.2.2.3), из (4.2.2.4) имеем $v_X(\Omega_2)+q<0$, и непрерывная дробь элемента $\beta\cdot X^s$ не квазипериодическая. □

4.2.3. Рациональные корни двух последовательностей многочленов с биномиальными коэффициентами

Результаты этого параграфа следуют из результатов §3.3.1. Здесь рассуждения проведены в частном случае, когда $K=\mathbb{Q}$.

Пусть $v_X(F)=0$, и в поле $\mathcal{L}=K(X)(\sqrt{F})$ есть фундаментальная единица $\Psi_1+\Psi_2\sqrt{F}$, где $\Psi_1,\Psi_2\in K[X]$. Пусть элемент β имеет квазипериодическое разложение в непрерывную дробь в поле $K((1/X))$. В теореме 4.2.2.1 остается не рассмотренным вопрос о квазипериодичности непрерывных дробей элементов вида $\beta\cdot X^s$ в случае, когда $v_X(\Psi_1)=v_X(\Psi_2)=0$ и $s\in\mathbb{Z}$ не удовлетворяет неравенствам (4.2.2.3). Оказывается, этот случай наиболее интересен с точки зрения строения квазипериодов непрерывных дробей элементов вида $\beta\cdot X^s$, а также разрешимости норменных уравнений (функциональных уравнений типа Пелля) с дискриминантом $D(\beta\cdot X^s)$.

Из существования фундаментальной единицы в поле $\mathcal{L}$ следует периодичность непрерывной дроби элемента $\sqrt{F}$, построенной в поле $K((1/X))$. Дальнейшая наша цель заключается в поиске необходимых и достаточных условий периодичности непрерывных дробей ключевых

элементов $X^s\sqrt{F}$, $s \in \mathbb{Z}$, над полем $K = \mathbb{Q}$ рациональных чисел. Для этого нам необходимо изучить рациональные корни двух последовательностей многочленов с биномиальными коэффициентами.

Для $n \in \mathbb{N}$ определим многочлены T_n, Q_n как в (3.3.1.1). По лемме 3.3.1.6 из условия, что многочлен $T_{nm}(z)$ имеет рациональный корень, следует, что хотя бы один из многочленов $T_n(z)$ или $T_m(z)$ имеет рациональный корень, а из условия, что многочлен $Q_{nm}(z)$ имеет рациональный корень, следует, что хотя бы один из многочленов $T_n(z)$, $Q_n(z)$ или $Q_m(z)$ имеет рациональный корень.

Лемма 4.2.3.1. *Если число n простое, то многочлены $T_n(z), Q_n(z) \in \mathbb{Q}[z]$ неприводимы над $\mathbb{Q}$.*

Доказательство. Пусть $n = p$ — простое, тогда $p \mid \binom{p}{j}$ для $1 \le j \le p-1$. Следовательно, по признаку Эйзенштейна многочлены $T_p(z), Q_p(z) \in \mathbb{Q}[z]$ неприводимы над $\mathbb{Q}$. □

Лемма 4.2.3.2. *Если $z_0 \in \mathbb{Q}$ является корнем уравнения $T_n(z) = 0$, то $T_{nm}(z_0) = 0$ и $Q_{nm}(z_0) \neq 0$, если $m \in \mathbb{N}$ нечетно, и $T_{nm}(z_0) \neq 0$ и $Q_{nm}(z_0) = 0$, если $m \in \mathbb{N}$ четно. Если $z_0 \in \mathbb{Q}$ является корнем уравнения $Q_n(z) = 0$, то $Q_{nm}(z_0) = 0$ и $T_{nm}(z_0) \neq 0$ для любого $m \in \mathbb{N}$.*

Доказательство. Утверждение леммы следует из соотношений (3.3.1.9), а также из леммы 3.3.1.1. □

Таблица 4.1: Рациональные корни многочленов $T_n(z), Q_n(z)$

$n \pmod{12}$	0	1	2	3	4	5	6	7	8	9	10	11
рац. корни T_n			-1	-1/3			-1			-1/3	-1	
рац. корни Q_n	-1/3; -1; -3			-3	-1		-1/3; -3		-1	-3		

Предложение 4.2.3.3. *Все рациональные корни многочленов $T_n(z), Q_n(z)$, $n \in \mathbb{N}$, описаны в таблице 4.1 и имеют кратность один.*

Доказательство. Найдем описание рациональных корней многочленов $T_n(z), Q_n(z)$.

Сначала докажем, что при $n \in \mathbb{N}$, $n \not\equiv 0 \pmod 2$, $n \not\equiv 0 \pmod 3$, многочлены $T_n(z), Q_n(z)$ рациональных корней не имеют. Будем рассуждать по индукции по количеству простых делителей числа n с учетом их кратностей. База индукции для простых $n > 3$ справедлива по лемме 4.2.3.1. Рассмотрим $n = p \cdot m$, где p — простое, $p > 3$, $m \in \mathbb{N}$, $m \not\equiv 0 \pmod 2$, $m \not\equiv 0 \pmod 3$. Так как $T_p(z)$ и $Q_p(z)$ неприводимы и $\deg T_p \ge 2$, $\deg Q_p \ge 2$, то по лемме 3.3.1.6

получаем, что множество рациональных корней многочлена $T_{pm}(z)\cdot Q_{pm}(z)$ совпадает с множеством рациональных корней многочлена $T_m(z)\cdot Q_m(z)$, которое пусто по индукционному предположению.

Имеем $T_2(-1)=0$, $T_3(-1/3)=0$, $Q_3(-3)=0$. По лемме 4.2.3.2 набор корней многочленов $T_n(z)$ и $Q_n(z)$ содержит корни, указанные в таблице 4.1 при соответствующих значениях n. Покажем, что при $n\equiv 0 \pmod 2$ или $n\equiv 0 \pmod 3$ других рациональных корней у многочленов $T_n(z)$ и $Q_n(z)$ нет. Предположим, что z_0 — рациональный корень многочлена $T_n(z)$ или $Q_n(z)$ с наименьшим номером n, причем пара (n,z_0) не совпадает ни с одной парой из таблицы 4.1. Такую пару (n,z_0) назовем *минимальной*, не совпадающей ни с одной парой из таблицы 4.1.

Пусть $T_n(z_0)=0$, $n=2m$ или $n=3m$, где $m\in\mathbb{N}$.

Если $n=2m$, то по (3.3.1.9) имеем $T_m\bigl(4z_0/(z_0+1)^2\bigr)=0$, и, поскольку по предположению z_0 — рациональный корень многочлена T_n с наименьшим номером n, причем пара (n,z_0) не совпадает ни с одной парой из таблицы 4.1, то пара $\bigl(m,4z_0/(z_0+1)^2\bigr)$ совпадает с одной из пар из таблицы 4.1. Если $m\equiv 2 \pmod 4$ и $4z_0/(z_0+1)^2=-1$, то z_0 не может быть рациональным числом. Если $m\equiv 3 \pmod 6$ и $4z_0/(z_0+1)^2=-1/3$, то z_0 также не может быть рациональным числом.

Если $n=3m$, то по (3.3.1.9) имеем $T_m\bigl(z_0(z_0+3)^2/(3z_0+1)^2\bigr)=0$, и, поскольку по предположению z_0 — рациональный корень многочлена T_n с наименьшим номером n, причем пара (n,z_0) не совпадает ни с одной парой из таблицы 4.1, то пара $\bigl(m,z_0(z_0+3)^2/(3z_0+1)^2\bigr)$ совпадает с одной из пар из таблицы 4.1 для многочлена T_n. Если $m\equiv 2 \pmod 4$ и $z_0(z_0+3)^2/(3z_0+1)^2=-1$, то $z_0=-1$. Так как $n=3m$ и $m\equiv 2 \pmod 4$, то $n\equiv 2 \pmod 4$, но это противоречит условию, что пара (n,z_0) не совпадает ни с одной парой из таблицы 4.1. Если $m\equiv 3 \pmod 6$ и $z_0(z_0+3)^2/(3z_0+1)^2=-1/3$, то z_0 не может быть рациональным числом.

Пусть $Q_n(z_0)=0$, $n=2m$ или $n=3m$, где $m\in\mathbb{N}$.

Если $n=2m$, то по (3.3.1.9) имеем $Q_m\bigl(4z_0/(z_0+1)^2\bigr)=0$, и, поскольку по предположению z_0 — рациональный корень многочлена Q_n с наименьшим номером n, причем пара (n,z_0) не совпадает ни с одной парой из таблицы 4.1, то пара $\bigl(m,4z_0/(z_0+1)^2\bigr)$ совпадает с одной из пар из таблицы 4.1. Если $m\equiv 0 \pmod 3$ и $4z_0/(z_0+1)^2=-3$, то $z_0=-1/3$ или $z_0=-3$. Так как $n=2m$ и $m\equiv 0 \pmod 3$, то $n\equiv 0 \pmod 6$, но это противоречит условию, что пара (n,z_0) не совпадает ни с одной парой из таблицы 4.1. Если $m\equiv 0 \pmod 4$ и $4z_0/(z_0+1)^2=-1$, то z_0 не может быть рациональным числом. Если $m\equiv 0 \pmod 6$ и $4z_0/(z_0+1)^2=-1/3$, то z_0 также не может быть рациональным числом.

Если $n=3m$, то по (3.3.1.9) имеем $Q_m\bigl(z_0(z_0+3)^2/(3z_0+1)^2\bigr)=0$, и, поскольку по предположению z_0 — рациональный корень многочлена Q_n с наименьшим номером n, причем пара (n,z_0) не совпадает ни с одной парой из таблицы 4.1, то пара $\bigl(m,z_0(z_0+3)^2/(3z_0+1)^2\bigr)$ сов-

падает с одной из пар из таблицы 4.1. Если $m \equiv 0 \pmod 3$ и $z_0(z_0+3)^2/(3z_0+1)^2 = -3$, то z_0 не может быть рациональным числом. Если $m \equiv 0 \pmod 4$ и $z_0(z_0+3)^2/(3z_0+1)^2 = -1$, то $z_0 = -1$. Так как $n = 3m$ и $m \equiv 0 \pmod 4$, то $n \equiv 0 \pmod 4$, но это противоречит условию, что пара (n, z_0) не совпадает ни с одной парой из таблицы 4.1. Если $m \equiv 0 \pmod 6$ и $z_0(z_0+3)^2/(3z_0+1)^2 = -1/3$, то z_0 не может быть рациональным числом.

Теперь покажем, что все рациональные корни, описанные в таблице 4.1, имеют кратность один. Если бы какой-то из описанных рациональных корней T_n или Q_n имел бы кратность больше одного, то по следствию 3.3.1.5 этот же корень имел бы соответственно многочлен Q_{n-1} или T_{n-1}, что невозможно, так как все рациональные корни описаны в таблице 4.1. □

Пусть в поле $\mathcal{L} = K(X)(\sqrt{F})$ существует фундаментальная единица $\Psi_1 + \Psi_2\sqrt{F}$, где $\Psi_1, \Psi_2 \in K[X]$. Для $n \in \mathbb{N}$ положим $\Omega_1^{(n)}, \Omega_2^{(n)} \in K[X]$ такие многочлены, что

$$\Omega_1^{(n)} + \Omega_2^{(n)}\sqrt{F} = \left(\Psi_1 + \Psi_2\sqrt{F}\right)^n. \tag{4.2.3.1}$$

Определим $Z = \Psi_2^2 F/\Psi_1^2$, тогда

$$\Omega_1^{(n)} + \Omega_2^{(n)}\sqrt{F} = \Psi_1^n\left(T_n(Z) + Q_n(Z)\sqrt{Z}\right), \tag{4.2.3.2}$$

где многочлены $T_n(z), Q_n(z) \in \mathbb{Z}[z]$ определены в (3.3.1.1).

4.2.4. Сильный критерий периодичности ключевых элементов

В следующей теореме для поля $K = \mathbb{Q}$ рациональных чисел доказаны необходимые и достаточные условия периодичности непрерывных дробей ключевых элементов $X^s\sqrt{F}$, $s \in \mathbb{Z}$, построенных в поле $\mathbb{Q}((1/X))$. Для непрерывных дробей, построенных по конечному нормированию, аналогичные результаты, как в следующей теореме, получены в теореме 2 статьи [14].

Теорема 4.2.4.1. *Пусть $F \in \mathbb{Q}[X]$ — свободный от квадратов многочлен, и в поле $\mathcal{L} = \mathbb{Q}(X)(\sqrt{F})$ есть фундаментальная единица $u = \Psi_1 + \Psi_2\sqrt{F}$, где $\Psi_1, \Psi_2 \in \mathbb{Q}[X]$. Пусть для $n \in \mathbb{N}$ многочлены $\Omega_1^{(n)}, \Omega_2^{(n)} \in \mathbb{Q}[X]$ определены соотношениями (4.2.3.1).*

1. *Если хотя бы одно из значений $v_X(F), v_X(\Psi_1), v_X(\Psi_2)$ отлично от нуля, то непрерывная дробь элемента $X^s\sqrt{F}$ периодическая тогда и только тогда, когда*

$$|s| \le v_X(\Psi_1) + v_X(\Psi_2).$$

2. *Если $v_X(F) = v_X(\Psi_1) = v_X(\Psi_2) = 0$, то непрерывная дробь элемента $X^s\sqrt{F}$ периодическая тогда и только тогда, когда*

$$|s| \le v_X\left(\Omega_1^{(2)}\right) + v_X\left(\Omega_1^{(3)}\right) + v_X\left(\Omega_2^{(3)}\right) = v_X\left(\Omega_2^{(12)}\right). \tag{4.2.4.1}$$

Доказательство. Пункт 1 следует из теоремы 4.2.2.1.

Докажем пункт 2, когда $v_X(F) = v_X(\Psi_1) = v_X(\Psi_2) = 0$. Положим $Z = Z(X) = \Psi_2^2 F/\Psi_1^2$, тогда для $n \in \mathbb{N}$ имеем (4.2.3.2). Согласно предложению 3.3.3.1 для периодичности элемента $X^s\sqrt{F}$, $s \neq 0$, необходимо, чтобы $Q_n(Z)|_{X=0} = 0$, поскольку $v_X(\Psi_1) = 0$, то есть $\Psi_1(0) \neq 0$. Из предложения 4.2.3.3, дающего полное описание всех рациональных корней многочленов T_n и Q_n, следует, что если $Z(0) \notin \{-3, -1, -1/3\}$, то $Q_n(Z)|_{X=0} \neq 0$ для любого $n \in \mathbb{N}$, и из тождества (4.2.3.2) имеем $v_X\left(\Omega_2^{(n)}\right) = 0$ для любого $n \in \mathbb{N}$. С другой стороны, если $Z(0) \in \{-3, -1, -1/3\}$, то возможен один из трех случаев:

- $Z(0) = -3$, тогда из предложения 4.2.3.3 и тождества (4.2.3.2) имеем $v_X\left(\Omega_2^{(3)}\right) > 0$, причем $v_X\left(\Omega_2^{(j)}\right) = 0$ при $1 \leq j \leq 2$;
- $Z(0) = -1$, тогда из предложения 4.2.3.3 и тождества (4.2.3.2) имеем $v_X\left(\Omega_1^{(2)}\right) > 0$ и, следовательно, $v_X\left(\Omega_2^{(4)}\right) > 0$, причем $v_X\left(\Omega_2^{(j)}\right) = 0$ при $1 \leq j \leq 3$;
- $Z(0) = -1/3$, тогда из предложения 4.2.3.3 и тождества (4.2.3.2) имеем $v_X\left(\Omega_1^{(3)}\right) > 0$ и, следовательно, $v_X\left(\Omega_2^{(6)}\right) > 0$, причем $v_X\left(\Omega_2^{(j)}\right) = 0$ при $1 \leq j \leq 5$.

Объединяя эти три случая, получаем, что для $s \in \mathbb{Z}$, удовлетворяющих неравенствам (4.2.4.1), имеем $X^{|s|} \mid \Omega_2^{(12)}$, откуда следует периодичность непрерывной дроби элемента $X^s\sqrt{F}$ с дискриминантом $D(X^{|s|}\sqrt{F}) = X^{2|s|}F$.

Далее остается показать, что для $s \in \mathbb{Z}$, не удовлетворяющих неравенствам (4.2.4.1), непрерывная дробь элемента $X^s\sqrt{F}$ не является периодической, и даже квазипериодической. Для этого достаточно показать, что справедливы утверждения:

- если $v_X\left(\Omega_2^{(3)}\right) > 0$ и $v_X\left(\Omega_2^{(j)}\right) = 0$ при $1 \leq j \leq 2$, то $v_X\left(\Omega_2^{(3k)}\right) = v_X\left(\Omega_2^{(3)}\right)$ для $k \in \mathbb{N}$;
- если $v_X\left(\Omega_2^{(4)}\right) > 0$ и $v_X\left(\Omega_2^{(j)}\right) = 0$ при $1 \leq j \leq 3$, то $v_X\left(\Omega_2^{(4k)}\right) = v_X\left(\Omega_2^{(4)}\right)$ для $k \in \mathbb{N}$;
- если $v_X\left(\Omega_2^{(6)}\right) > 0$ и $v_X\left(\Omega_2^{(j)}\right) = 0$ при $1 \leq j \leq 5$, то $v_X\left(\Omega_2^{(6k)}\right) = v_X\left(\Omega_2^{(6)}\right)$ для $k \in \mathbb{N}$.

Для каждого многочлена $\Omega_i^{(n)}(X)$, $1 \leq i \leq 2$, $n \in \mathbb{N}$, обозначим $\Omega_{i,j}^{(n)}(X)$ соответствующий коэффициент при X^j. Пусть

$$\Psi_1(X) \equiv \Psi_{1,0} + \Psi_{1,1}X \pmod{X^2},$$
$$\Psi_2(X) \equiv \Psi_{2,0} + \Psi_{2,1}X \pmod{X^2},$$
$$F(X) \equiv F_0 + F_1X \pmod{X^2},$$

причем $\Psi_{1,0} \neq 0$, $\Psi_{2,0} \neq 0$ и $F_0 \neq 0$.

Предположим, что $Z(0) = -1$, тогда $v_X\left(\Omega_1^{(2)}\right) > 0$ и $v_X\left(\Omega_2^{(4)}\right) > 0$, причем $v_X\left(\Omega_2^{(j)}\right) = 0$ при $1 \leq j \leq 3$. По определению величины Z, условие $Z(0) = -1$ равносильно условию

$\Psi_{1,0}^2 + \Psi_{2,0}^2 F_0 = 0$. В силу предложения 4.2.3.3 справедливы соотношения $v_X\left(\Omega_1^{(n)}\right) = 0$ при $n \not\equiv 2 \pmod 4$, и $v_X\left(\Omega_2^{(n)}\right) = 0$ при $n \not\equiv 0 \pmod 4$. Покажем, что для $k \in \mathbb{N}$ выполнены равенства $v_X\left(\Omega_1^{(4k+2)}\right) = v_X\left(\Omega_1^{(2)}\right) = v_X\left(\Omega_2^{(4k)}\right) = v_X\left(\Omega_2^{(4)}\right)$.

Для начала рассмотрим $\Omega_1^{(2)}(X) \equiv \Omega_{1,0}^{(2)} + \Omega_{1,1}^{(2)} X \pmod{X^2}$, где

$$\Omega_{1,0}^{(2)} = \Psi_{1,0}^2 + \Psi_{2,0}^2 F_0 = 0,$$
$$\Omega_{1,1}^{(2)} = 2\Psi_{1,0}\Psi_{1,1} + 2\Psi_{2,0}\Psi_{2,1}F_0 + \Psi_{2,0}^2 F_1.$$

Имеем

$$\Omega_1^{(4k+2)} = \Psi_1^{4k+2} T_{4k+2}\left(\frac{\Psi_2^2 F}{\Psi_1^2}\right) =$$
$$= \left(\Psi_1^2 + \Psi_2^2 F\right) \cdot T_{2k+1}\left(\frac{4\Psi_1^2\Psi_2^2 F}{\left(\Psi_1^2 + \Psi_2^2 F\right)^2}\right)\left(\Psi_1^2 + \Psi_2^2 F\right)^{2k} \equiv$$
$$\equiv \Omega_{1,1}^{(2)} \cdot \binom{2k+1}{2k} \cdot \left(4\Psi_{1,0}^2\Psi_{2,0}^2 F_0\right)^k \cdot X \pmod{X^2}.$$

Таким образом, $\Omega_{1,1}^{(4k+2)} = 0$ тогда и только тогда, когда $\Omega_{1,1}^{(2)} = 0$. Далее, рассуждая аналогично, при условии, что $\Omega_{1,0}^{(2)} = \Omega_{1,1}^{(2)} = \ldots = \Omega_{1,n-1}^{(2)} = 0$, по индукции имеем

$$\Omega_1^{(4k+2)} \equiv \Omega_{1,n}^{(2)} \cdot \binom{2k+1}{2k} \cdot \left(4\Psi_{1,0}^2\Psi_{2,0}^2 F_0\right)^k \cdot X^n \pmod{X^{n+1}},$$

то есть $\Omega_{1,n}^{(4k+2)} = 0$ тогда и только тогда, когда $\Omega_{1,n}^{(2)} = 0$, что означает $v_X\left(\Omega_1^{(4k+2)}\right) = v_X\left(\Omega_1^{(2)}\right)$.

Аналогично, по формуле (3.3.1.9) получаем

$$\Omega_2^{(4k)} = \Psi_1^{4k-1}\Psi_2 Q_{4k}\left(\frac{\Psi_2^2 F}{\Psi_1^2}\right) =$$
$$= 2\Psi_1\Psi_2 \cdot \left(\Psi_1^2 + \Psi_2^2 F\right) \cdot Q_{2k}\left(\frac{4\Psi_1^2\Psi_2^2 F}{\left(\Psi_1^2 + \Psi_2^2 F\right)^2}\right)\left(\Psi_1^2 + \Psi_2^2 F\right)^{2(k-1)} \equiv$$
$$\equiv 2\Psi_{1,0}\Psi_{2,0} \cdot \Omega_{1,1}^{(2)} \cdot \binom{2k}{2k-1} \cdot \left(4\Psi_{1,0}^2\Psi_{2,0}^2 F_0\right)^{k-1} \cdot X \pmod{X^2}.$$

Следовательно, $\Omega_{2,1}^{(4k)} = 0$ тогда и только тогда, когда $\Omega_{1,1}^{(2)} = 0$. Далее, при условии, что $\Omega_{1,0}^{(2)} = \Omega_{1,1}^{(2)} = \ldots = \Omega_{1,n-1}^{(2)} = 0$, по индукции имеем

$$\Omega_2^{(4k)} \equiv 2\Psi_{1,0}\Psi_{2,0} \cdot \Omega_{1,n}^{(2)} \cdot \binom{2k}{2k-1} \cdot \left(4\Psi_{1,0}^2\Psi_{2,0}^2 F_0\right)^{k-1} \cdot X^n \pmod{X^{n+1}},$$

то есть $\Omega_{2,n}^{(4k)} = 0$ тогда и только тогда, когда $\Omega_{1,n}^{(2)} = 0$, что означает $v_X\left(\Omega_2^{(4k)}\right) = v_X\left(\Omega_1^{(2)}\right)$.

Предположим теперь, что $Z(0) = -1/3$, тогда $v_X\left(\Omega_1^{(3)}\right) > 0$ и $v_X\left(\Omega_2^{(6)}\right) > 0$, причем $v_X\left(\Omega_2^{(j)}\right) = 0$ при $1 \leq j \leq 5$. По определению величины Z, условие $Z(0) = -1/3$ равносильно условию $\Psi_{1,0}^2 + 3\Psi_{2,0}^2 F_0 = 0$. В силу предложения 4.2.3.3 справедливы соотношения $v_X\left(\Omega_1^{(n)}\right) = 0$ при $n \not\equiv 3 \pmod 6$, и $v_X\left(\Omega_2^{(n)}\right) = 0$ при $n \not\equiv 0 \pmod 6$. Покажем, что для $k \in \mathbb{N}$ выполнены

равенства $v_X\left(\Omega_1^{(6k+3)}\right) = v_X\left(\Omega_1^{(3)}\right) = v_X\left(\Omega_2^{(6k)}\right) = v_X\left(\Omega_2^{(6)}\right)$.

Для начала рассмотрим $\Omega_1^{(3)}(X) \equiv \Omega_{1,0}^{(3)} + \Omega_{1,1}^{(3)} X \pmod{X^2}$, где

$$\Omega_{1,0}^{(3)} = \Psi_{1,0}(\Psi_{1,0}^2 + 3\Psi_{2,0}^2 F_0) = 0,$$
$$\Omega_{1,1}^{(3)} = 3(2F_0\Psi_{1,0}\Psi_{2,0}\Psi_{2,1} + F_0\Psi_{1,1}\Psi_{2,0}^2 + F_1\Psi_{1,0}\Psi_{2,0}^2 + \Psi_{1,0}^2\Psi_{1,1}).$$

Имеем

$$\Omega_1^{(6k+3)} = \Psi_1^{6k+3} T_{6k+3}\left(\frac{\Psi_2^2 F}{\Psi_1^2}\right) =$$
$$= \Psi_1^{2k+1}\left(\Psi_1^2 + 3\Psi_2^2 F\right)\cdot T_{2k+1}\left(\frac{\Psi_2^2 F}{\Psi_1^2}\left(\frac{3\Psi_1^2 + \Psi_2^2 F}{\Psi_1^2 + 3\Psi_2^2 F}\right)^2\right)\left(\Psi_1^2 + 3\Psi_2^2 F\right)^{2k} \equiv$$
$$\equiv \Psi_{1,0}\cdot\Omega_{1,1}^{(3)}\cdot\binom{2k+1}{2k}\cdot\left(\Psi_{2,0}^2 F_0\right)^k\cdot\left(\Omega_{2,0}^{(3)}\right)^{2k}\cdot X \pmod{X^2},$$

где $\Omega_{2,0}^{(3)} = 3\Psi_{1,0}^2 + \Psi_{2,0}^2 F_0 \neq 0$. Таким образом, $\Omega_{1,1}^{(6k+3)} = 0$ тогда и только тогда, когда $\Omega_{1,1}^{(3)} = 0$. Далее, рассуждая аналогично, при условии, что $\Omega_{1,0}^{(3)} = \Omega_{1,1}^{(3)} = \ldots = \Omega_{1,n-1}^{(3)} = 0$, по индукции имеем

$$\Omega_1^{(6k+3)} \equiv \Psi_{1,0}\cdot\Omega_{1,n}^{(3)}\cdot\binom{2k+1}{2k}\cdot\left(\Psi_{2,0}^2 F_0\right)^k\cdot\left(\Omega_{2,0}^{(3)}\right)^{2k}\cdot X^n \pmod{X^{n+1}},$$

то есть $\Omega_{1,n}^{(6k+3)} = 0$ тогда и только тогда, когда $\Omega_{1,n}^{(3)} = 0$, что означает $v_X\left(\Omega_1^{(6k+3)}\right) = v_X\left(\Omega_1^{(3)}\right)$.

Аналогично, по формуле (3.3.1.9) получаем

$$\Omega_2^{(6k)} = \Psi_1^{6k-1}\Psi_2 Q_{6k}\left(\frac{\Psi_2^2 F}{\Psi_1^2}\right) =$$
$$= \Psi_1^{2k-1}\Psi_2\left(3\Psi_1^2 + \Psi_2^2 F\right)\left(\Psi_1^2 + 3\Psi_2^2 F\right)Q_{2k}\left(\frac{\Psi_2^2 F}{\Psi_1^2}\left(\frac{3\Psi_1^2 + \Psi_2^2 F}{\Psi_1^2 + 3\Psi_2^2 F}\right)^2\right)\left(\Psi_1^2 + 3\Psi_2^2 F\right)^{2(k-1)} \equiv$$
$$\equiv \Psi_{1,0}\Psi_{2,0}\cdot\Omega_{1,1}^{(3)}\cdot\binom{2k}{2k-1}\cdot\left(\Psi_{2,0}^2 F_0\right)^{k-1}\cdot\left(\Omega_{2,0}^{(3)}\right)^{2k-1}\cdot X \pmod{X^2}.$$

Следовательно, если $\Omega_{1,1}^{(3)} \neq 0$, то $\Omega_{2,1}^{(6k)} \neq 0$. Следовательно, $\Omega_{2,1}^{(6k)} = 0$ тогда и только тогда, когда $\Omega_{1,1}^{(3)} = 0$. Далее, рассуждая аналогично, при условии, что $\Omega_{1,0}^{(3)} = \Omega_{1,1}^{(3)} = \ldots = \Omega_{1,n-1}^{(3)} = 0$, по индукции имеем

$$\Omega_2^{(6k)} \equiv \Psi_{1,0}\Psi_{2,0}\cdot\Omega_{1,n}^{(3)}\cdot\binom{2k}{2k-1}\cdot\left(\Psi_{2,0}^2 F_0\right)^{k-1}\cdot\left(\Omega_{2,0}^{(3)}\right)^{2k-1}\cdot X^n \pmod{X^{n+1}},$$

то есть $\Omega_{1,n}^{(6k)} = 0$ тогда и только тогда, когда $\Omega_{1,n}^{(3)} = 0$, что означает $v_X\left(\Omega_1^{(6k)}\right) = v_X\left(\Omega_1^{(3)}\right)$.

Далее, по индукции получаем $\Omega_{1,n}^{(6k)} = 0$ тогда и только тогда, когда $\Omega_{1,n}^{(3)} = 0$, что означает $v_X\left(\Omega_2^{(6k)}\right) = v_X\left(\Omega_1^{(3)}\right)$.

Наконец, предположим, что $Z(0) = -3$, тогда $v_X\left(\Omega_2^{(3)}\right) > 0$, причем $v_X\left(\Omega_2^{(j)}\right) = 0$ при $1 \leq j \leq 2$. По определению величины Z, условие $Z(0) = -3$ равносильно условию $3\Psi_{1,0}^2 + \Psi_{2,0}^2 F_0 = 0$. В силу предложения 4.2.3.3 справедливо соотношение $v_X\left(\Omega_2^{(n)}\right) = 0$ при $n \not\equiv 0$

(mod 3). Нам необходимо доказать, что $v_X\left(\Omega_2^{(3k)}\right) = v_X\left(\Omega_2^{(3)}\right)$. Для этого мы покажем, что для $k \in \mathbb{N}$ выполнены равенства $v_X\left(\Omega_2^{(6k)}\right) = v_X\left(\Omega_2^{(6k+3)}\right) = v_X\left(\Omega_2^{(3)}\right)$.

Для начала рассмотрим $\Omega_2^{(3)}(X) \equiv \Omega_{2,0}^{(3)} + \Omega_{2,1}^{(3)} X \pmod{X^2}$, где

$$\Omega_{2,0}^{(3)} = \Psi_{2,0}(3\Psi_{1,0}^2 + \Psi_{2,0}^2 F_0) = 0,$$
$$\Omega_{2,1}^{(3)} = 3F_0\Psi_{2,0}^2\Psi_{2,1} + F_1\Psi_{2,0}^3 + 3\Psi_{1,0}^2\Psi_{2,1} + 6\Psi_{1,0}\Psi_{1,1}\Psi_{2,0}.$$

По формуле (3.3.1.9) имеем

$$\Omega_2^{(6k)} = \Psi_1^{6k-1}\Psi_2 Q_{6k}\left(\frac{\Psi_2^2 F}{\Psi_1^2}\right) =$$
$$= \Psi_1^{2k-1}\Psi_2\big(3\Psi_1^2 + \Psi_2^2 F\big)Q_{2k}\left(\frac{\Psi_2^2 F}{\Psi_1^2}\left(\frac{3\Psi_1^2 + \Psi_2^2 F}{\Psi_1^2 + 3\Psi_2^2 F}\right)^2\right)\big(\Psi_1^2 + 3\Psi_2^2 F\big)^{2k-1} \equiv$$
$$\equiv \Psi_{1,0}^{2k-1}\Psi_{1,0}\cdot\Omega_{2,1}^{(3)}\cdot 2k\cdot\big(\Omega_{1,0}^{(3)}\big)^{2k-1}\cdot X \pmod{X^2}.$$

Следовательно, $\Omega_{2,1}^{(6k)} = 0$ тогда и только тогда, когда $\Omega_{2,1}^{(3)} = 0$. Далее, рассуждая аналогично, при условии, что $\Omega_{2,0}^{(3)} = \Omega_{2,1}^{(3)} = \ldots = \Omega_{2,n-1}^{(3)} = 0$, по индукции имеем

$$\Omega_2^{(6k)} \equiv \Psi_{1,0}^{2k-1}\Psi_{1,0}\cdot\Omega_{2,n}^{(3)}\cdot 2k\cdot\big(\Omega_{1,0}^{(3)}\big)^{2k-1}\cdot X^n \pmod{X^{n+1}},$$

то есть $\Omega_{2,n}^{(6k)} = 0$ тогда и только тогда, когда $\Omega_{2,n}^{(3)} = 0$, что означает $v_X\left(\Omega_2^{(6k)}\right) = v_X\left(\Omega_2^{(3)}\right)$.

Аналогично, по формуле (3.3.1.9) получаем

$$\Omega_2^{(6k+3)} = \Psi_1^{6k+2}\Psi_2 Q_{6k+3}\left(\frac{\Psi_2^2 F}{\Psi_1^2}\right) =$$
$$= \Psi_1^{2k}\Psi_2\big(3\Psi_1^2 + \Psi_2^2 F\big)Q_{2k+1}\left(\frac{\Psi_2^2 F}{\Psi_1^2}\left(\frac{3\Psi_1^2 + \Psi_2^2 F}{\Psi_1^2 + 3\Psi_2^2 F}\right)^2\right)\big(\Psi_1^2 + 3\Psi_2^2 F\big)^{2k} \equiv$$
$$\equiv \Psi_{1,0}^{2k}\Psi_{2,0}\cdot\Omega_{2,1}^{(3)}\cdot(2k+1)\cdot\big(\Omega_{1,0}^{(3)}\big)^{2k}\cdot X \pmod{X^2}.$$

Таким образом, $\Omega_{2,1}^{(6k+3)} = 0$ тогда и только тогда, когда $\Omega_{2,1}^{(3)} = 0$. Далее, рассуждая аналогично, при условии, что $\Omega_{2,0}^{(3)} = \Omega_{2,1}^{(3)} = \ldots = \Omega_{2,n-1}^{(3)} = 0$, по индукции имеем

$$\Omega_2^{(6k+3)} \equiv \Psi_{1,0}^{2k}\Psi_{2,0}\cdot\Omega_{2,n}^{(3)}\cdot(2k+1)\cdot\big(\Omega_{1,0}^{(3)}\big)^{2k}\cdot X^n \pmod{X^{n+1}},$$

то есть $\Omega_{2,n}^{(6k+3)} = 0$ тогда и только тогда, когда $\Omega_{2,n}^{(3)} = 0$, что означает $v_X\left(\Omega_2^{(6k+3)}\right) = v_X\left(\Omega_2^{(3)}\right)$.

Теорема 4.2.4.1 доказана. □

4.2.5. Схема доказательства теорем 4.2.1.1 и 4.2.1.2

Пусть $F \in \mathbb{Q}[X]$ — свободный от квадратов многочлен степени 4, такой, что поле $\mathcal{L} = \mathbb{Q}(X)(\sqrt{F})$ обладает фундаментальной единицей степени m. Тогда в группе классов дивизоров степени ноль $\Delta^\circ(\mathcal{L})$ поля $\mathcal{L}$ класс дивизора $\infty^- - \infty^+$ имеет порядок m. Согласно теореме Мазура [33] порядок m может принимать только следующие значения $2 \le m \le 10$ и $m = 12$. Для каждого $4 \le m \le 12$, $m \ne 11$, в [69; 72] явно выписано полное параметрическое семейство

многочленов $F = F(X, c) \in \mathbb{Q}[X]$ четвертой степени с параметром $c \in \mathbb{Q}$ таких, что в $F(X, c)$ коэффициент при X^3 равен нулю, свободный член равен 1, класс дивизора $\infty^- - \infty^+$ имеет порядок m в группе классов дивизоров степени ноль $\Delta^\circ(\mathcal{L})$ поля $\mathcal{L} = \mathbb{Q}(X)(\sqrt{F(X, c)})$. Для $m = 2$ или $m = 3$ в [69; 72] также явно выписано параметрическое семейство таких многочленов $F = F(X, b, c) \in \mathbb{Q}[X]$, но уже зависящее от двух параметров $b, c \in \mathbb{Q}$. Схема рассуждений остается аналогичной, поэтому представим ее только для $4 \leq m \leq 12$, $m \neq 11$, когда имеется единственный параметр $c \in \mathbb{Q}$.

Описанные выше параметрические семейства многочленов $F(X, c)$ для $4 \leq m \leq 12$, $m \neq 11$, (или $F(X, b, c)$ соответственно для $2 \leq m \leq 3$) содержат все многочлены F четвертой степени над полем рациональных чисел такие, что в многочлене F коэффициент при X^3 равен нулю, свободный член равен 1 и выполнено одно из равносильных условий:

- непрерывная дробь элемента $\sqrt{F}$ в в поле $\mathbb{Q}((1/X))$ периодическая;
- норменное уравнение
$$\Omega_1^2 - \Omega_2^2 F = b \tag{4.2.5.1}$$
имеет решение $\Omega_1, \Omega_2 \in \mathbb{Q}[X]$, $\Omega_2 \neq 0$, для некоторого $b \in \mathbb{Q}^*$.

Если пара многочленов Ω_1, Ω_2 является решением норменного уравнения (4.2.5.1) с минимальной степенью $\deg \Omega_1$, причем $\Omega_2 \neq 0$, то $\deg \Omega_1 = m$ и $\Omega_1 + \Omega_2\sqrt{F}$ является фундаментальной единицей поля $\mathcal{L}$. Периодичность непрерывной дроби элемента $X^s\sqrt{F}$ равносильна разрешимости норменного уравнения вида (4.2.5.1) с дополнительными условиями на значения $v_X(\Omega_1)$ и $v_X(\Omega_2)$, но теперь $\Omega_1 + \Omega_2\sqrt{F}$ может не являться фундаментальной единицей, а быть некоторой степенью k фундаментальной единицы, причем в теореме 4.2.4.1 доказано, что $k \leq 3$.

Обозначим p_j/q_j, $j \in \mathbb{N}_0$, подходящие дроби к $\sqrt{F(X, c)}$, причем $p_j = p_j(X, c)$, $q_j = q_j(X, c) \in \mathbb{Q}[X]$. Тогда фундаментальная единица поля $\mathcal{L} = \mathbb{Q}(X)(\sqrt{F})$ имеет вид $p_n + q_n\sqrt{F}$ для некоторого минимального $n \in \mathbb{N}$ такого, что $p_n^2 - q_n^2 F \in \mathbb{Q}^*$ (см. [92]). Обозначим $\Omega_1^{(j)} + \Omega_2^{(j)}\sqrt{F} = (p_n + q_n\sqrt{F})^j$, где $\Omega_1^{(j)}, \Omega_2^{(j)} \in \mathbb{Q}[X]$, $j \in \mathbb{N}$. Положим $r_j = v_X\left(\Omega_2^{(j)}\right)$, тогда согласно теореме 4.2.4.1 возможны только следующие 6 случаев:

$$r_1 > 0, \qquad r_2 > 0 \text{ и } r_1 = 0,$$
$$r_3 > 0 \text{ и } r_j = 0,\ j < 3, \qquad r_4 > 0 \text{ и } r_j = 0,\ j < 4,$$
$$r_6 > 0 \text{ и } r_j = 0,\ j < 6, \qquad r_j = 0,\ j \in \mathbb{N}.$$

Причем, если для некоторого $j \in \mathbb{N}$ выполнено $r_j > 0$, то непрерывная дробь элемента $\sqrt{F}/X^{r_j}$, построенная в поле $\mathbb{Q}((1/X))$ периодическая.

Замена X на $X+t$ соответствует изоморфизму кривых $C : Y^2 = F(X)$ и $C_t : Y^2 = F(X+t)$. Тем самым, с точностью до отношения эквивалентности, определяемого допустимыми заме-

нами $F(X)$ на $A^2F(BX)$ для некоторых $A, B \in \mathbb{Q}^*$, имеем полное описание всех многочленов $F = F(c,t) \in \mathbb{Q}[X]$, $\deg F = 4$, для которых разложение $\sqrt{F}$ в непрерывную дробь периодично. Наша задача сводится к поиску всех значений параметров $c, t \in \mathbb{Q}$ (или параметров $b, c, t \in \mathbb{Q}$ соответственно для случаев $m = 2$ и $m = 3$) для каждого из случаев $v_X\left(\Omega_2^{(j)}\right) > 0$, $j \in \{1, 2, 3, 4, 6\}$. Необходимым и достаточным условием периодичности непрерывной дроби $\sqrt{F(X+t,c)}/X$ в $\mathbb{Q}((1/X))$ является $\Omega_2^{(j)}(t) = 0$ хотя бы для одно из $j \in \{1, 2, 3, 4, 6\}$. Для того, чтобы непрерывная дробь $\sqrt{F(X+t,c)}/X^2$ была периодической необходимо и достаточно, чтобы $r_j = v_X\left(\Omega_2^{(j)}\right) \geq 2$ для некоторого $j \in \{1, 2, 3, 4, 6\}$, то есть $\Omega_2^{(j)}(t) = 0$ и $\frac{\mathrm{d}}{\mathrm{d}t}\Omega_2^{(j)}(t) = 0$, что возможно только тогда, когда дискриминант $d = d^{(j)}(c)$ (или дискриминант $d = d^{(j)}(b, c)$ соответственно для случаев $m = 2$ и $m = 3$) многочлена $\Omega_2^{(j)}(t) \in \mathbb{Q}[t]$ равен нулю. То есть задача сводится к поиску корней дискриминанта $d^{(j)}(c)$ и соответствующих кратных корней многочлена $\Omega_2^{(j)}(t) \in \mathbb{Q}[t]$ для каждого из $j \in \{1, 2, 3, 4, 6\}$, причем параметры $c, t \in \mathbb{Q}$ должны быть такие, что дискриминант многочлена $F(X+t, c) \in \mathbb{Q}[X]$ был отличен от нуля.

В задаче описания многочленов $F \in \mathbb{Q}[X]$ с периодическим разложением $\sqrt{F}$ в непрерывную дробь в $Q((1/X))$ для упрощения вычислений мы будем искать такие значения параметров c и t (или параметров $b, c, t \in \mathbb{Q}$ соответственно для случаев $m = 2$ и $m = 3$), чтобы был выполнен хотя бы один из следующих случаев

$$v_X\left(q_n(X)\right) \geq 2, \quad v_X\left(p_n(X)\right) \geq 2, \quad v_X\left(p_n(X)^2 + F(X)q_n(X)^2\right) \geq 2,$$
$$v_X\left(p_n(X)^2 + F(X)q_n(X)^2\right) \geq 2, \quad v_X\left(p_n(X)^2 + 3F(X)q_n(X)^2\right) \geq 2,$$

которые соответствуют $v_X\left(\Omega_2^{(j)}\right) \geq 2$ для $j \in \{1, 2, 3, 4, 6\}$. Обозначим

$$\theta_1 = q_n(t), \quad \theta_2 = p_n(t), \quad \theta_3 = 3p_n(t)^2 + F(t)q_n(t)^2,$$
$$\theta_4 = p_n(t)^2 + F(t)q_n(t)^2, \quad \theta_6 = p_n(t)^2 + 3F(t)q_n(t)^2. \tag{4.2.5.2}$$

Найдем подходящие значения параметра $c \in \mathbb{Q}$ (или параметров $b, c \in \mathbb{Q}$ соответственно для случаев $m = 2$ и $m = 3$), чтобы дискриминант многочлена $\theta_j(t) \in \mathbb{Q}[t]$ по очереди для $j \in \{1, 2, 3, 4, 6\}$ был равен нулю. Далее, найдем кратные корни $t \in \mathbb{Q}$ соответствующих многочленов $\theta_j(t)$, и восстановим многочлен $f(x) = x^4F(1/x + t, c) \in \mathbb{Q}[x]$.

Для доказательства теоремы 4.2.1.2 достаточно для каждого из найденных в теореме 4.2.1.1 многочлена (или семейства многочленов) $f(x)$ проверить, что соответствующие величины $r_j = v_X\left(\Omega_2^{(j)}\right) \leq 2$ для $j \in \{1, 2, 3, 4, 6\}$.

Реализация изложенной схемы доказательства существенным образом опирается на большие символьные компьютерные вычисления. Компьютерные вычисления, и в частности, доказательство неприводимости указанных далее многочленов, проводились на языке программирования Python с использованием библиотеки Sympy. Более подробно см. в [8].

4.3. Классификация эллиптических полей над квадратичными расширениями поля рациональных чисел

Классическая проблема периодичности непрерывных дробей элементов гиперэллиптических полей имеет большую и глубокую историю. Она имеет глубокие приложения к проблеме поиска и построения фундаментальных единиц и S-единиц, к проблеме описания точек конечного порядка на эллиптических кривых и проблеме кручения в якобианах гиперэллиптических кривых. Кроме того, изучение функциональных непрерывных дробей имеет интерес с точки зрения арифметических приложений, в том числе к решению норменных уравнений или функциональных уравнений типа Пелля.

До сих пор проблема периодичности непрерывных дробей элементов гиперэллиптических полей была далека от полного решения. В.П. Платонов в [17; 19] поставил вопрос о классификации полей $L = K(x)(\sqrt{f})$ по признаку периодичности ключевых элементов $\sqrt{f}$ для непрерывных дробей, построенных в поле $K((x))$, где K — поле алгебраических чисел. В разделах 4.1, 4.2 для квадратичных расширений, определяемых многочленами степени 3 или 4 с коэффициентами из поля рациональных чисел $\mathbb{Q}$, доказано, что за исключением тривиальных случаев с точностью до эквивалентности существует ограниченное количество многочлена над $\mathbb{Q}$, квадратный корень из которых разлагается в периодическую непрерывную дробь в поле формальных степенных рядов $\mathbb{Q}((x))$. В теоремах 4.1.3.1 и 4.2.1.1 явно выписаны представители таких классов эквивалентности.

В этом разделе для всех квадратичных числовых полей K приведено описание свободных от квадратов многочленов $f(x) \in K[x]$ степени 4 таких, что $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в поле формальных степенных рядов $K((x))$, а эллиптическое поле $L = K(x)(\sqrt{f})$ обладает фундаментальной S-единицей степени m, $2 \leq m \leq 12$, $m \neq 11$, где множество S состоит из двух сопряженных нормирований определенных на поле L и связанных с униформизующей x поля $K(x)$.

Результаты этого раздела опубликованы в статьях [4; 5].

4.3.1. Формулировка основных результатов

Пусть $f(x) \in K[x]$ — свободный от квадратов многочлен, над полем K характеристики отличной от 2. Дополнительно предположим, что свободный член многочлена f является полным квадратом в мультипликативной группе K^* поля K. Тогда гиперэллиптическое поле $L = K(x)(\sqrt{f})$ вкладывается в поле формальных степенных рядов $K((x))$, которое состоит из элементов вида

$$\alpha = \sum_{j=s}^{+\infty} b_j x^j, \qquad s \in \mathbb{Z}, \quad b_j \in K, \ b_s \neq 0.$$

В $K((x))$ определено нормирование $v_x(\alpha) = s$, которое индуцируется на поле L двумя способами v_x^- и v_x^+, зависящими от вложения L в $K((x))$. Зафиксируем одно из вложений поля L в $K((x))$, и для определенности обозначим соответствующее ему нормирование v_x^-. Тогда для элементов $\alpha \in L$ определена соответствующая целая часть $[\alpha]_x^-$ и корректно определено разложение в непрерывную дробь (см. §3.1.1). Будем писать, что разложение элементов поля L в непрерывную дробь построено в поле $K((x))$, когда необходимо подчеркнуть, что соответствующее построение индуцировано из вложения L в $K((x))$.

В статьях [17; 18] сформулирована задача описания эллиптических и гиперэллиптических полей $L = K(x)(\sqrt{f})$, в которых соответствующие элементы $\sqrt{f}$ имеют периодическое разложение в непрерывную дробь, построенную в поле $K((x))$. Интерес к этой задаче объясняется следующими обстоятельствами.

Во-первых, постановка этой задачи по формулировке почти идентична классической проблеме периодичности, впервые появившейся в работах Абеля и Чебышева, и в дальнейшем получившей достаточно широкое внимание в математических работах вплоть до настоящего времени (см. [52; 61; 69; 70; 187]). Классическая проблема периодичности заключается в определении эллиптических и гиперэллиптических полей $L = K(x)(\sqrt{f})$, в которых соответствующие элементы $\sqrt{f}$ имеют периодическое разложение в непрерывную дробь, построенную в поле $K((x^{-1}))$. Эта проблема имеет глубокую связь с такими проблемами как проблема поиска и построения фундаментальных единиц и S-единиц гиперэллиптических полей, проблема поиска рациональных точек кручения в якобиане гиперэллиптической кривой (см. [17; 62; 92; 118]).

Во-вторых, изучение элементов вида $\sqrt{f}$, имеющих периодическое разложение в непрерывную дробь, построенную в поле $K((x))$, важно для решения проблемы описания всех периодических и квазипериодических элементов в эллиптических и гиперэллиптических полях. В статье [8] была высказана гипотеза (Гипотеза №2) о том, что элементы вида $\sqrt{f}$ являются "пограничными" в следующем смысле: для полей алгебраических чисел K не существует элементов вида $x\sqrt{f}$, обладающих периодическим разложением в непрерывную дробь в $K((x))$. Кроме того, известно (см. [14; 141]), что из периодичности непрерывной дроби элемента $\sqrt{f}$ следует периодичность непрерывных дробей всех элементов вида $\sqrt{f}/x^s$, $0 \leq s \leq \deg f$.

В этом разделе найдено полное описание троек $[m, f(x), K]$ соответствующих K-точкам на рациональных модулярных кривых $X_1(m)$, где m — порядок кручения, $2 \leq m \leq 12$, $m \neq 11$, K — квадратичное расширение $\mathbb{Q}$, $f \in K[x]$ — свободный от квадратов многочлен степени 4, для которого элемент $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в поле $K((x))$. В статье [5] при $4 \leq m \leq 12$, $m \neq 11$, было анонсировано описание таких троек без подробных рассуждений. Случаи $2 \leq m \leq 3$ имеют особый интерес над квадратичными числовыми полями K, поскольку в этих случаях возникает половина всех примеров многочленов f, для

которых $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в $K((x))$.

Поиск элементов вида $\sqrt{f}$, обладающих периодическим разложением в непрерывную дробь в поле $K((x))$, имеет смысл осуществлять с точностью до отношения эквивалентности, определенного допустимыми заменами многочлена $f(x)$ на $a^2 f(bx^n)$ для $a, b \in K^*$, $n \in \mathbb{N}$, и заменой $f(x)$ на $f^\sigma(x)$, где σ — автоморфизм группы Галуа $\mathrm{Gal}(K/\mathbb{Q})$. Гипотеза №1 в [8] утверждает, что над числовыми полями K для заданного числа $N \in \mathbb{N}$ с точностью до указанной выше эквивалентности существует лишь конечное число свободных от квадратов многочленов $f(x)$, $\deg f \leq N$, для которых $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в $K((x))$. Мы будем говорить, что многочлен f определен с точностью до указанной эквивалентности с минимальным представлением степени $\deg f = k$, если нельзя сделать замену x^n на x для некоторого $n \in \mathbb{N}$ так, чтобы степень многочлена f стала меньше k.

Обозначим через $\mathcal{U}_0^{(4)}$ множество пар $[f(x),\ K]$, состоящих из числового поля K и свободного от квадратов многочлена $f \in K[x]$ с минимальным представлением степени 4, имеющего периодическое разложение $\sqrt{f}$ в непрерывную дробь в поле $K((x))$, с точностью до *отношения эквивалентности*, определенного допустимыми заменами многочлена $f(x)$ на $a^2 f(bx)$ для $a, b \in K^*$ и заменой $f(x)$ на $f^\sigma(x)$, где $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Для $[f(x),\ K] \in \mathcal{U}_0^{(4)}$ в силу теоремы 3.2.1.1 эллиптическое поле $L = K(x)(\sqrt{f})$ обладает фундаментальной S-единицей некоторой степени m, где множество $S = \{v_x^-,\ v_x^+\}$. Отсюда следует, что класс дивизора $(x)^- - (x)^+$ имеет конечный порядок m в группе классов дивизоров $\Delta^\circ(L)$, причем в случае $K = \mathbb{Q}$ из статьи [33] следует, что $m \leq 12$, $m \neq 11$, а в случае $[K\ :\ \mathbb{Q}] = 2$ из статьи [36] следует, что $m \leq 18$, $m \neq 17$.

Обозначим за $\mathcal{U}^{(4)}$ множество троек $[m,\ f(x),\ K]$, где $[f(x),\ K] \in \mathcal{U}_0^{(4)}$ и m — степень соответствующей фундаментальной S-единицы кольца S-целых элементов поля $L = K(x)(\sqrt{f})$.

Теорема 4.3.1.1. *Множество троек* $[m,\ f(x),\ K] \in \mathcal{U}^{(4)}$, *таких, что* $[K : \mathbb{Q}] \leq 2$, $m \leq 12$,

$m \neq 11$, описывается следующим образом

$$
\begin{aligned}
&m=3, \quad f_1=-4x^4-4x^3-3x^2-2x+1, \quad K=\mathbb{Q},\\
&m=3, \quad f_2=-12x^4-12x^3-3x^2-2x+1, \quad K=\mathbb{Q},\\
&m=3, \quad f_3=-\frac{4x^4}{3}-\frac{4x^3}{3}-3x^2-2x+1, \quad K=\mathbb{Q},\\
&m=3, \quad f_4=-4x^4\left(3-2\sqrt{2}\right)-4x^3\left(3-2\sqrt{2}\right)-3x^2-2x+1, \quad K=\mathbb{Q}(\sqrt{2}),\\
&m=3, \quad f_5=-4x^4\left(7-4\sqrt{3}\right)-4x^3\left(7-4\sqrt{3}\right)-3x^2-2x+1, \quad K=\mathbb{Q}(\sqrt{3}),\\
&m=3, \quad f_6=-4x^4\left(5-2\sqrt{5}\right)-4x^3\left(5-2\sqrt{5}\right)-3x^2-2x+1, \quad K=\mathbb{Q}(\sqrt{5}),\\
&m=3, \quad f_7=-\frac{4x^4\left(5-2\sqrt{5}\right)}{5}-\frac{4x^3\left(5-2\sqrt{5}\right)}{5}-3x^2-2x+1, \quad K=\mathbb{Q}(\sqrt{5}),\\
&m=4, \quad f_8=-\frac{3x^4}{4}-3x^3-2x^2-2x+1, \quad K=\mathbb{Q},\\
&m=4, \quad f_9=\frac{36-21\sqrt{3}}{2}x^4+(15-9\sqrt{3})x^3+(4-3\sqrt{3})x^2-2x+1, \quad K=\mathbb{Q}(\sqrt{3}),\\
&m=5, \quad f_{10}=-5x^4-3x^3-\frac{7x^2}{4}-x+1, \quad K=\mathbb{Q},\\
&m=6, \quad f_{11}=\frac{108x^4}{5}+\frac{324x^3}{25}+\frac{69x^2}{25}-\frac{6x}{5}+1, \quad K=\mathbb{Q},\\
&m=7, \quad f_{12}=-\frac{28x^4}{5}-\frac{84x^3}{25}+\frac{21x^2}{25}-\frac{2x}{5}+1, \quad K=\mathbb{Q},\\
&m=7, \quad f_{13}=\frac{(35-9\sqrt{-7})x^4}{2}+\frac{(33-3\sqrt{-7})x^3}{2}+\\
&\qquad +\frac{(41+5\sqrt{-7})x^2}{8}-\frac{(3+\sqrt{-7})x}{2}+1, \quad K=\mathbb{Q}(\sqrt{-7}),\\
&m=7, \quad f_{14}=-\frac{x^4\left(32\sqrt{21}+147\right)}{15}-\frac{x^3\left(621+136\sqrt{21}\right)}{75}-\\
&\qquad -\frac{x^2\left(304\sqrt{21}+1469\right)}{300}-\frac{x\left(33+8\sqrt{21}\right)}{15}+1, \quad K=\mathbb{Q}(\sqrt{21}).
\end{aligned}
$$

Все многочлены в теореме 4.3.1.1 лежат в разных классах относительно указанного выше отношения эквивалентности и имеют минимальное представление степени 4. Более того, соответствующие эллиптические поля $L=K(x)(\sqrt{f})$ попарно неизоморфны, а эллиптические кривые, определяемые уравнениями $y^2=f(x)$, попарно бирационально неэквивалентны.

Примеры $f_1, f_2, f_3, f_8, f_{10}, f_{11}, f_{12}$, определенные над $\mathbb{Q}$, были найдены в [8]. Примеры f_9, f_{13}, f_{14}, определенные соответственно над полями $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{21})$, были найдены в [5]. Оставшиеся примеры f_4, f_5, f_6, f_7 были найдены в [4].

С помощью теоремы 4.3.1.1 и непосредственной вычислительной проверки получаем следующий результат, который подтверждает Гипотезу №2 из [8] в случае $\deg f=4$, $[K\ :\mathbb{Q}]\leq 2$.

Теорема 4.3.1.2. *В случае $s<0$ или $s>4$ не существует троек $[m, f(x), K]$ таких, что*

K — квадратичное расширение поля $\mathbb{Q}$, многочлен $f \in K[x]$ свободен от квадратов, элемент $\sqrt{f}/x^s$ имеет периодическое разложение в непрерывную дробь в поле $K((x))$, поле $L = K(x)(\sqrt{f})$ содержит фундаментальную S-единицу степени m, $m \leq 12$, $m \neq 11$.

В статьях [8; 17] полностью решена проблема описания эллиптических полей $L = \mathbb{Q}(x)(\sqrt{f})$, в которых соответствующие элементы $\sqrt{f}$ имеют периодическое разложение в непрерывную дробь, построенную в поле $\mathbb{Q}((x))$ над полем $\mathbb{Q}$ рациональных чисел. Тем самым доказана Гипотеза №1 для $K = \mathbb{Q}$ и $N = 4$, а также показано, что в этом случае справедлива Гипотеза №2. В статьях [144; 183; 184] доказана Гипотеза №1 для кубических многочленов $f(x)$, определенных над полями K, $[K : \mathbb{Q}] \leq 6$, а в случае $[K : \mathbb{Q}] \leq 3$ в [144; 182] дано явное описание таких пар $[K, f(x)]$, что $\deg f = 3$ и $\sqrt{f}$ имеет периодическое разложение в непрерывную дробь в поле $K((x))$.

Результаты этого раздела опубликованы в статьях [4; 5].

4.3.2. Вспомогательные утверждения

В §4.2.3 найдены все рациональные корни многочленов $T_n(x)$ и $Q_n(x)$, определенных в (3.3.1.1), при всех натуральных n: для многочленов $T_n(x)$, $n \in \mathbb{N}$, корнями могут быть только $x \in \{-1, -1/3\}$, более точно, $T_{2(2k-1)}(-1) = 0$, $T_{3(2k-1)}(-1/3) = 0$ при всех $k \in \mathbb{N}$, причем указанные корни имеют кратность один и других рациональных корней нет; для многочленов $Q_n(x)$, $n \in \mathbb{N}$, корнями могут быть только $x \in \{-3, -1, -1/3\}$, более точно, $Q_{3k}(-3) = 0$, $Q_{4k}(-1) = 0$, $Q_{6k}(-1/3) = 0$ при всех $k \in \mathbb{N}$, причем указанные корни имеют кратность один и других рациональных корней нет.

Исследуем последовательности многочленов $T_n(x)$ и $Q_n(x)$, на наличие корней в квадратичных полях. По критерию Эйзенштейна (см. лемму 4.2.3.1) при простых n многочлены $T_n(x)$ и $Q_n(x)$ неприводимы, причем при $n \geq 7$ степени многочленов $T_n(x)$ и $Q_n(x)$ больше 3, поэтому при простых n многочлены $T_n(x)$ и $Q_n(x)$ корней в квадратичных полях не имеют. Обозначим множество различных корней многочленов $T_n(x)$ и $Q_n(x)$ при $n \leq 6$ через M. Имеем

$$M = \left\{-1,\ -\frac{1}{3},\ -3,\ -3 \pm 2\sqrt{2},\ \frac{-5 \pm 2\sqrt{5}}{5},\ -5 \pm 2\sqrt{5},\ -7 \pm 4\sqrt{3}\right\}. \tag{4.3.2.1}$$

Обозначим элементы множества M, записанные в том же порядке, как в (4.3.2.1), следующим образом

$$M = \{c_3, c_4, c_5, c_6^{\pm}, c_8^{\pm}, c_{10}^{\pm}, c_{12}^{\pm}\}. \tag{4.3.2.2}$$

Для краткости верхние индексы у $c_n^{\pm}$ опускаем. Нижние индексы в (4.3.2.2) означают соответственно минимальные номера n, для которых $Q_n(c_n) = 0$. Покажем, что других корней в квадратичных полях кроме корней из множества M многочлены $T_n(x)$ и $Q_n(x)$, $n \in \mathbb{N}$, не

имеют.

Рассуждая по индукции по числу простых множителей числа n, аналогично предложению 4.2.3.3 получаем следующее утверждение.

Предложение 4.3.2.1. *При $n \in \mathbb{N}$ таких, что $n \not\equiv 0 \pmod 2$, $n \not\equiv 0 \pmod 3$, $n \not\equiv 0 \pmod 5$, многочлены $T_n(x)$ и $Q_n(x)$ в квадратичных полях корней не имеют.*

Таким образом, корни многочленов $T_n(x)$ и $Q_n(x)$ из квадратичных полей могут быть только при n кратных 2, 3 или 5.

Теорема 4.3.2.2. *Множество корней последовательности многочленов $T_n(x)$ и $Q_n(x)$, принадлежащих квадратичным полям, исчерпывается множеством M, определенном в (4.3.2.1).*

Доказательство. Пусть для некоторого $n \in \mathbb{N}$ имеем $T_n(a) = 0$, причем $a \notin M$ — элемент некоторого квадратичного поля. Представим $n = n_1 \cdot m_1$, где $n_1 = 2^\alpha 3^\beta 5^\gamma$, а число m_1 не имеет простых делителей меньше 7. Предположим, что $T_{n_1}(a) \neq 0$, тогда из (3.3.1.9) следует, что $T_m(b) = 0$, но этого не может быть, так как b, как и a, принадлежит квадратичному полю. Значит, $T_{n_1}(a) = 0$ для $a \notin M$.

Если n_1 четно, то представим $n_1 = 2m_1$. Так как $T_2(a) \neq 0$, ибо $a \notin M$, то из (3.3.1.9) следует, что $T_{m_1}(b_1) = 0$, где $b_1 = a\big(Q_2(a)/T_2(a)\big)^2$. Покажем, что из того, что $a \notin M$ следует, что $b_1 \notin M$. Предположим противное, то есть $b_1 \in M$. Перебрав все возможные значения для $b_1 \in M$, видим, что значения a, удовлетворяющие уравнению $b_1 = a\big(Q_2(a)/T_2(a)\big)^2$, либо принадлежат множеству M, либо не являются элементами квадратичных полей, что противоречит начальному предположению о корне a многочлена $T_n(x)$. Таким образом, $b_1 \notin M$ и $T_{m_1}(b_1) = 0$. Если m_1 четно, то снова представим $m_1 = 2m_2$, и, рассуждая аналогично, придем к тому, что должно существовать число $b_2 \notin M$ такое, что $T_{m_2}(b_2) = 0$. Повторяя эти рассуждения необходимое количество раз, получаем, что должен существовать элемент $b_\alpha \notin M$ некоторого квадратичного поля такой, что $T_{m_\alpha}(b_\alpha) = 0$, причем $m_\alpha = 3^\beta 5^\gamma$. Далее, если $\beta > 0$, то представим $m_\alpha = 3k$. Так как $T_3(b_\alpha) \neq 0$, ибо $b_\alpha \notin M$, то из (3.3.1.9) следует, что $T_k(c) = 0$, где $c = b_\alpha\big(Q_3(b_\alpha)/T_3(b_\alpha)\big)^2$. Перебирая все возможные значения $c \in M$, приходим к выводу, что либо $b_\alpha \in M$, либо b_α не является элементом квадратичного поля, что противоречит нашему предположению об элементе b_α. Значит, $c \notin M$ — такой элемент квадратичного расширения, что $T_k(c) = 0$. При необходимости рассуждая аналогично, можно считать, что $k = 5^\gamma$. Если $\gamma > 1$, то представим $k = 5k_1$. Так как $T_5(c) \neq 0$, ибо $c \notin M$, то из (3.3.1.9) следует, что $T_{k_1}(c_1) = 0$, где $c_1 = c\big(Q_5(c)/T_5(c)\big)^2$. Перебирая все возможные значения $c_1 \in M$, приходим к выводу, что либо $c \in M$, либо c не является элементом квадратичного поля, что противоречит нашему предположению об элементе c. Значит, $c_1 \notin M$ — такой элемент квадратичного расширения, что $T_{k_1}(c_1) = 0$. При необходимости рассуждая аналогично, можно

считать, что $k_1 = 5$. Но все корни $T_5(x)$ лежат в M, что приводит нас к противоречию. Таким образом, у многочлена $T_n(x)$ не может быть других корней из квадратичного поля, кроме корней, указанных в множестве M.

Для многочлена $Q_n(x)$ рассуждения полностью аналогичны.

Теорема 4.3.2.2 доказана. □

4.3.3. Схема доказательства основных результатов

Обозначим через $X_1(m)$ модулярную кривую, K-точки которой с точностью до изоморфизма отвечают парам (E, P_m), где E — эллиптическая кривая, определенная над K, P_m — K-точка порядка m на E. Ограничение в теореме 4.3.1.1 на степень m фундаментальной S-единицы обусловлено тем фактом, что в случае $m \leq 12$, $m \neq 11$ кривые $X_1(m)$ рациональны, и дают так называемую рациональную параметризацию множества пар (E, P_m) с зависимостью от единственного параметра t (явное представление см., например, в [35]). Для $m = 11$ и $m \geq 13$ кривые $X_1(m)$ перестают быть рациональными, что существенно увеличивает вычислительную сложность используемого нами метода, поскольку возникают дополнительные параметры и нелинейные условия. В связи с этим для дальнейших существенных продвижений нужны кардинально новые идеи.

Доказательство теоремы 4.3.1.1 является обобщением доказательства основных результатов раздела 4.2 (см. дополнительно [8]), проведенных над полем $\mathbb{Q}$, на случай квадратичных полей констант. Отметим, что рассуждения нельзя назвать аналогичными, поскольку при расширениях поля $\mathbb{Q}$ существенным образом изменяется множество M корней многочленов $T_n(x)$ и $Q_n(x)$, определенных в (3.3.1.1). Для квадратичных расширений в теореме 4.3.2.2 явно найдены элементы множества M — их конечное число (см. (4.3.2.1)), что дает конечное число вариантов уравнений, связывающих параметры семейств эллиптических кривых, имеющих точку порядка m, $m \leq 12$, $m \neq 11$. Указанная связь возникает из условия периодичности разложения $\sqrt{f}$ в непрерывную дробь в поле $K((x))$, и явно представлена в теореме 4.2.4.1. Кроме того, ввиду необходимости объемных символьных компьютерных вычислений над квадратичными полями, была значительно изменена программная реализация используемых алгоритмов.

Приведем схему доказательства теоремы 4.3.1.1.

Пусть K — числовое поле. Для каждого $4 \leq m \leq 12$, $m \neq 11$, в [8; 69; 72] явно выписано параметрическое семейство всех приведенных многочленов $F = F(X, c) \in \mathbb{Q}[X]$ четвертой степени с параметром $c \in K$ таких, что класс дивизора $\infty^- - \infty^+$ имеет порядок m в группе классов дивизоров степени ноль $\Delta^\circ(\mathcal{L})$ поля $\mathcal{L} = \mathbb{Q}(X)(\sqrt{F(X, c)})$. Для $2 \leq m \leq 3$ в [8; 72] также выписано параметрическое семейство всех приведенных многочленов $F = F(X, b, c) \in \mathbb{Q}[X]$ четвертой степени с двумя параметрами $b, c \in K$ таких, что класс дивизора $\infty^- - \infty^+$ имеет

порядок m в группе классов дивизоров степени ноль $\Delta^\circ(\mathcal{L})$. Здесь приведенность многочлена F понимается в смысле дополнительных ограничений: коэффициент при X^3 равен нулю, коэффициент при X^4 равен 1. Для $2 \leq m \leq 3$ при всевозможных значениях параметров $b, c \in K$, для которых дискриминант $F(X)$ не обращается в ноль, указанные параметрические семейства содержат все приведенные многочлены $F(X)$ четвертой степени над полем K, такие, что выполнено одно из равносильных условий:

- непрерывная дробь элемента $\sqrt{F}$ в в поле $K((1/X))$ периодическая;
- норменное уравнение
$$\Omega_1^2 - \Omega_2^2 F = \gamma \tag{4.3.3.1}$$
имеет решение $\Omega_1, \Omega_2 \in K[X]$, $\Omega_2 \neq 0$, для некоторого $\gamma \in K^*$.

Если пара многочленов Ω_1, Ω_2 является решением норменного уравнения (4.3.3.1) с минимальной степенью $\deg \Omega_1$, причем $\Omega_2 \neq 0$, то $\deg \Omega_1 = m$ и $\Omega_1 + \Omega_2\sqrt{F}$ является фундаментальной единицей поля $\mathcal{L} = K(X)(\sqrt{F})$. По теореме 3.3.3.3 периодичность непрерывной дроби элемента $X^s\sqrt{F}$ равносильна разрешимости норменного уравнения вида (4.3.3.1) с дополнительными условиями на значения $v_X(\Omega_1)$ и $v_X(\Omega_2)$, но теперь $\Omega_1 + \Omega_2\sqrt{F}$ может не являться фундаментальной единицей, а может быть фундаментальной единицей, возведенной в некоторую степень n, причем из теоремы 4.3.2.2 следует, что в случае $[K : \mathbb{Q}] \leq 2$ число n ограничено 12 (см. Таблицу 3.1).

Опишем схему доказательства теоремы 4.3.1.1 при $4 \leq m \leq 12$, $m \neq 11$, когда параметрическое семейство приведенных многочленов $F(X) = F(X, c)$ зависит от одного параметра c.

Обозначим через p_j/q_j, $j \in \mathbb{N}_0$, подходящие дроби к $\sqrt{F(X,c)}$, причем $p_j = p_j(X,c)$, $q_j = q_j(X,c) \in \mathbb{Q}(c)[X]$. Положим $K = \mathbb{Q}(c)$. Тогда фундаментальная единица поля $\mathcal{L} = K(X)(\sqrt{F})$ имеет вид $p_n + q_n\sqrt{F}$ для некоторого минимального $n \in \mathbb{N}$ такого, что $p_n^2 - q_n^2 F \in K^*$ (см. [92]). Обозначим $\Omega_1^{(j)} + \Omega_2^{(j)}\sqrt{F} = (p_n + q_n\sqrt{F})^j$, где $\Omega_1^{(j)}, \Omega_2^{(j)} \in K[X]$, $j \in \mathbb{N}$, тогда справедливо представление (см. [3], §5)
$$\Omega_1^{(j)} + \Omega_2^{(j)}\sqrt{F} = p_n^j\big(T_j(Z) + Q_j(Z)\sqrt{Z}\big), \quad \text{где} \quad Z = \frac{q_n^2 F}{p_n^2}. \tag{4.3.3.2}$$
Положим $r_j = v_X\left(\Omega_2^{(j)}\right)$, тогда согласно теореме 4.3.2.2 возможны только следующие 9 случаев: $r_k > 0$ при том, что $r_j = 0$, если $1 \leq j < k$, для каждого $k \in \Lambda = \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Отметим, что, если для некоторого $k \in \mathbb{N}$ выполнено $r_k > 0$, то непрерывная дробь элемента $\sqrt{F}/X^{r_k}$, построенная в поле $K((1/X))$ периодическая (см. [8], теорема 4).

Замена X на $X + t$ соответствует изоморфизму ("сдвигу") кривых $C : Y^2 = F(X)$ и $C_t : Y^2 = F(X + t)$, причем непрерывная дробь элемента $\sqrt{F(X+t)}$ периодична тогда и только

тогда, когда непрерывная дробь $\sqrt{F(X)}$ периодична, поскольку указанная замена не меняет структуру норменного уравнения (4.3.3.1). Однако для элементов вида $X^s\sqrt{F(X+t)}$, $s \neq 0$, свойство периодичности вообще говоря не сохраняется при различных значениях параметра t, поэтому в дальнейшем мы будем искать те значения t, для которых разложение $X^s\sqrt{F(X+t)}$ в непрерывную дробь периодично.

Заметим, что опять в силу структуры норменного уравнения (4.3.3.1) для $a, b \in K^*$ непрерывная дробь вида $(bX)^s\sqrt{a^2F(bX)}$ периодична тогда и только тогда, когда непрерывная дробь $X^s\sqrt{F(X)}$ периодична. Поэтому дальнейшие рассуждения о поиске периодических непрерывных дробей элементов вида $X^s\sqrt{F(X)}$, $s \in \mathbb{N}$, будут проводиться с точностью до указанной замены для некоторых $a, b \in K^*$.

Как было отмечено, в [69; 72] выписаны параметрические семейства всех приведенных многочленов $F = F(X, c) \in \mathbb{Q}[X]$, которые задают соответствующие эллиптические кривые с точками конечного порядка. Замена вида $F(X)$ на $F(X+t)$ из указанных параметрических семейств приведенных многочленов позволяет получить описание всех многочленов $F = F(c, t) \in \mathbb{Q}[X]$, $\deg F = 4$, со старшим коэффициентом 1, для которых разложение $\sqrt{F}$ в непрерывную дробь в поле $\mathbb{Q}(c, t)((1/X))$ периодично. Наша задача сводится к поиску всех значений параметров $c, t \in K$ для каждого из случаев $v_X\left(\Omega_2^{(k)}\right) > 0$, $k \in \Lambda$, причем по постановке задачи мы ограничиваемся квадратичными расширениями, $K = \mathbb{Q}(c, t)$, $[K : \mathbb{Q}] \leq 2$.

Необходимым и достаточным условием периодичности непрерывной дроби $\sqrt{F(X+t, c)}/X$ в $K((1/X))$ является $\Omega_2^{(k)}(t) = 0$ хотя бы для одно из $k \in \Lambda$. Для того, чтобы непрерывная дробь $\sqrt{F(X+t, c)}/X^2$ была периодической, необходимо и достаточно, чтобы $r_k = v_X\left(\Omega_2^{(k)}\right) \geq 2$ для некоторого $k \in \Lambda$.

Будем вычислять последовательно значения $r_k = v_X\left(\Omega_2^{(k)}\right)$, $k \in \Lambda$, причем вычисляя очередное r_k считаем, что $r_j = 0$ при $j \in \Lambda$, $j < k$, поскольку нас интересует минимальный номер $k \in \Lambda$, для которого $r_k > 0$. Согласно (4.3.3.2) значения r_k можно вычислить следующим образом:

$$\begin{gathered} r_1 = v_X\left(q_n\right), \\ r_2 = v_X\left(p_n\right), \quad \text{при условии, что} \quad r_1 = 0, \\ r_k = v_X\left(q_n^2F/p_n^2 - c_k\right), \quad c_k \in M, \text{ при условии, что } r_j = 0 \text{ при } j \in \Lambda, j < k, \end{gathered} \tag{4.3.3.3}$$

причем в случае сопряженных квадратичных иррациональностей, входящих в множество M, в качестве c_k нужно рассматривать каждое значение $c_k^{\pm}$. Таким образом, мы приходим к необходимости изучения значений v_X на следующем множестве:

$$\begin{aligned} \Theta = \big\{&q_n,\ p_n,\ 3p_n^2 + q_n^2F,\ p_n^2 + q_n^2F,\ p_n^2 + 3q_n^2F,\ p_n^4 + 6p_n^2q_n^2F + q_n^4F^2, \\ &5p_n^4 + 10p_n^2q_n^2F + q_n^4F^2, p_n^4 + 10p_n^2q_n^2F + 5q_n^4F^2, p_n^4 + 14p_n^2q_n^2F + q_n^4F^2\big\}. \end{aligned}$$

Для краткости обозначим элементы множества Θ за θ_k, $k \in \Lambda$, в указанном порядке следования.

Итак, наша задача состоит в поиске всех значений параметров t, c, определенных в некотором квадратичном поле K, для которых $r_k = v_X(\theta_k) \geq 2$, где k — минимальный номер из Λ (см. [5]). Так как $X = 0$ должен быть корнем θ_k кратности не менее 2, то дискриминант D_k многочлена $\theta_k(X)$ должен обращаться в 0. Дискриминант $D_k = D_k(c)$ многочлена $\theta_k(X) = \theta_k(X, c, t)$ зависит только от параметра c, поскольку "сдвиг" t на дискриминант не влияет. По корням дискриминанта $D_k(c)$ находим значения параметра t такие, что $r_k \geq 2$. Если найдены все подходящие значения параметров c, t, то для доказательства теоремы 4.3.1.1 достаточно положить $f(x) = x^4 F(1/x + t, c) \in K[x]$ и отобрать представителей с точностью до указанного в определении множества $\mathcal{U}_0^{(4)}$ отношения эквивалентности.

В случаях $2 \leq m \leq 3$ параметрическое семейство многочленов $F(X)$ зависит от двух параметров b, c, а также от параметра "сдвига" t. Тогда дискриминанты $D_k = D_k(b, c)$ многочленов $\theta_k(X)$ также зависит от двух параметров b, c, поскольку "сдвиг" t на дискриминант не влияет. По корням дискриминанта D_k относительно переменных b, c находим значения параметра t такие, что $r_k \geq 2$.

Изложенная схема доказательства существенным образом опирается на большие символьные компьютерные вычисления. Отметим, что схема доказательства позволяет проводить все операции над полем $\mathbb{Q}$, за исключением финального поиска корней над квадратичными расширениями. С вычислительной точки зрения это обстоятельство существенно оптимизирует работу алгоритмов. Программный код был реализован на языке программирования Python с использованием библиотеки Sympy [185; 186]. В частности, использовались базовые арифметические функции над кольцом многочленов $\mathbb{Q}[X]$, а также встроенные алгоритмы символьного вычисления дискриминанта многочлена относительно переменной X и с параметрами b, c, разложения многочлена на множители, анализ и решение систем алгебраических уравнений с помощью базисов Гребнера. Без подобных вычислений получить заявленные результаты не представляется возможным.

Далее необходимо рассмотреть все возможные степени m фундаментальных единиц эллиптических полей $\mathcal{L}$ и соответствующие параметрические семейства многочленов $F(X)$. Подробнее см. в статьях [4; 5].

Глава 5. Функциональные непрерывные дроби обобщенного типа

В этой главе построена новая теория обобщенных функциональных непрерывных дробей, а также рассмотрено применение этой теории к проблеме поиска фундаментальных S-единиц в гиперэллиптических полях и к проблеме кручения в якобианах гиперэллиптических кривых. Теория функциональных непрерывных дробей, рассмотренная в Главе 3, оказывается менее эффективной для случаев, когда нормирование v_h, по которому строится непрерывная дробь, имеет степень выше 1. В частности, при $\deg h \geq 2$ не выполнено свойство наилучшего приближения у подходящих дробей (см. [130], пример 5.7).

В серии статей 2015-2024 гг. в соавторстве с В.П. Платоновым был развит теоретико-числовой подход к проблеме поиска и построения фундаментальных S-единиц гиперэллиптических полей, основанный на теории функциональных непрерывных дробей в поле формальных степенных рядов $K((x))$. В частности, было показано, что теория функциональных непрерывных дробей позволяет существенно продвинуться в поиске нетривиальных S-единиц и в изучении их строения в гиперэллиптических полях над произвольным числовым полем в качестве поля констант для множества S состоящего из двух нормирований. В Главах 3 и 5 рассмотрены следующие случаи:

- множество S состоит из двух сопряженных (относительно гиперэллиптической инволюции) нормирований первой степени (Глава 3);
- классический случай, когда множество S состоит из единственного бесконечного нормирования (когда $v_\infty^- = v_\infty^+$) и конечного нормирования первой степени, не связанного с точками Вейерштрасса (см. нетрадиционный подход в разделе 5.2);
- множество S состоит из двух несопряженных нормирований первой степени (раздел 5.3);
- множество S состоит из двух сопряженных нормирований второй степени (раздел 5.4).

В частности, из решения проблемы поиска и построения S-единиц в указанных случаях следует полное алгоритмическое решение проблемы кручения в якобианах гиперэллиптических кривых рода 2.

В разделе 5.2 теория функциональных непрерывных дробей обобщенного типа (h-дробей) была применена для традиционного случая, когда непрерывная дробь строится по нормированию v_h, $\deg h = 1$ (см. [15]). В теореме 5.2.2.1 доказан критерий периодичности (квазипериодичности) функциональных непрерывных дробей обобщенного типа, дающий эффективный алгоритм поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях (см. §5.2.3).

В разделе 5.3 построена теория функциональных непрерывных дробей обобщенного типа для двух несопряженных линейных нормирований (см. [7]). Особенность таких обобщенных непрерывных дробей в том, что они сходятся к элементу как по первому, так и по второму линейному нормированию (см. предложение 5.3.3.3). В теореме 5.3.4.1 для функциональных непрерывных дробей обобщенного типа, построенным по двум несопряженным линейным нормированиям, доказан критерий периодичности для ключевых элементов гиперэллиптических полей.

В качестве следствия сформулирован эффективный алгоритм поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях (см. §5.4.6). В §5.3.6 в качестве иллюстрации построенного метода найдены новые примеры S-единиц для множеств S, состоящих из двух несопряженных линейных нормирований.

В разделе 5.3 построена теория непрерывных h-дробей — функциональных непрерывных дробей обобщенного типа, построенных по нормированию v_h, $\deg h = 2$ (см. [11; 16]). Ранее теория непрерывных дробей не применялась для поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях, когда в множестве S содержалось нормирование второй степени. В теореме 5.4.4.1 для непрерывных h-дробей, $\deg h = 2$, доказан критерий периодичности для ключевых элементов гиперэллиптических полей.

В качестве следствия сформулирован эффективный алгоритм поиска и построения соответствующих фундаментальных S-единиц в гиперэллиптических полях (см. §5.4.6). В §5.4.7 в качестве иллюстрации построенного метода найдены новые примеры S-единиц для множеств S, состоящих из двух сопряженных нормирований второй степени.

Результаты Главы 5 опубликованы в статьях [7; 11; 15; 16].

5.1. Общий подход к построению непрерывных дробей обобщенного типа

В Главе 3 показано, что теория функциональных дробей является мощным инструментом для поиска и построения фундаментальных единиц и S-единиц гиперэллиптического поля L. В этой главе рассматривается конструкция построения функциональных непрерывных дробей обобщенного типа, найденная с помощью анализа дивизоров. Основная идея заключается в том, чтобы проинтерпретировать на языке рациональных функций кратное увеличение

заданного дивизора так, чтобы на каждом шаге явно видеть, какой точке в якобиане этот кратный дивизор соответствует. Оказывается, что обобщенные непрерывные дроби специального вида в точности отвечают на этот вопрос. Кроме того, теория обобщенных непрерывных дробей позволяет сформулировать алгоритмы, которые используют только арифметические операции на многочленах, заданных над полем K. С вычислительной точки зрения такие алгоритмы крайне важны для изучения групповой структуры K-точек якобиана J гиперэллиптической кривой C.

В этом разделе мы рассмотрим общий подход к построению непрерывных дробей обобщенного типа с помощью представления Мамфорда. Важность этого подхода заключается в том, что построение непрерывной дроби оказывается проассоциировано с последовательностью приведенных дивизоров $\{E_j\}$, образами которых являются K-точки на якобиане J. Сам же процесс построения непрерывной дроби обобщенного типа можно интерпретировать на языке дивизоров как построение последовательности приведенных дивизоров $\{E_j\}$ эквивалентной (в группе классов дивизоров) возрастающей последовательности эффективных дивизоров, вида $n\,(h)_\infty^-$, $n \in \mathbb{N}$.

После общего подхода в следующих разделах отдельно рассмотрены случаи, когда эффективный дивизор $(h)_\infty^-$ соответствует одному из следующих вариантов:

- конечный дивизор первой степени, определенный над полем K (см. раздел 5.2);
- конечный дивизор второй степени, распадающийся на два простых плейса, определенные над полем K (см. раздел 5.3);
- конечный дивизор второй степени, определенный над полем K, но не распадающийся на два простых плейса над K (см. раздел 5.4).

В каждом из этих случаев нами доказаны критерии квазипериодичности, которые в некотором смысле являются аналогами критерия, рассмотренного в §3.2.1. Наши рассуждения опираются на анализ дивизоров полных частных непрерывной дроби (см. 2.4) и представление Мамфорда (см. 2.4.5), которое мы заново вводим в каждом случае отдельно учитывая соответствующие особенности.

5.1.1. Определение обобщенной непрерывной дроби

Обобщенной непрерывной дробью над полем $\mathcal{K}$ называется конечное или бесконечное формальное выражение вида

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cdots}}}, \tag{5.1.1.1}$$

где $a_j \in \mathcal{K}^*$ — *неполные частные*, $b_j \in \mathcal{K}^*$ — *неполные числители*, a_0 — *целая часть* непрерывной дроби (5.1.1.1), где $\mathcal{K}^*$ — мультипликативная группа поля $\mathcal{K}$. Обобщенную непрерывную дробь (5.1.1.1) будем обозначать $\alpha = [a_0; b_1|a_1, b_2|a_2, \ldots]$ и для краткости, когда это не приводит к путанице, будем называть ее просто *непрерывной дробью*. Далее нам хотелось бы установить некоторые свойства таких непрерывных дробей и связанных с ними элементов. Без ограничения общности, если не оговорено противное, мы будем предполагать, что непрерывная дробь α бесконечная, и ее "хвосты" вида $[a_j; b_{j+1}|a_{j+1}, \ldots] \neq 0$, $j \in \mathbb{N}_0$. Выражения $\alpha_j = [a_j; b_{j+1}|a_{j+1}, \ldots]$ называются *полными частными*. По виду непрерывной дроби (5.1.1.1) ясно, что при $j \in \mathbb{N}_0$ справедливы соотношения

$$\alpha = [a_0; b_1|a_1, \ldots, b_j|a_j, b_{j+1}|\alpha_{j+1}], \quad \alpha_{j+1} = \frac{b_{j+1}}{\alpha_j - a_j}. \tag{5.1.1.2}$$

Пусть дана непрерывная дробь $[a_0; b_1|a_1, b_2|a_2, \ldots]$ над полем $\mathcal{K}$. Положим $p_{-1} = 1, \quad p_0 = a_0, \quad q_{-1} = 0, \quad q_0 = 1$, и рекуррентным образом для $j \in \mathbb{N}$ продолжим

$$p_{j+1} = a_{j+1}p_j + b_{j+1}p_{j-1}, \quad q_{j+1} = a_{j+1}q_j + b_{j+1}q_{j-1}. \tag{5.1.1.3}$$

Скажем, что непрерывная дробь (5.1.1.1) *невырожденная*, если $q_j \neq 0$ при $j \in \mathbb{N}_0$. В дальнейшем будем по умолчанию предполагать, что рассматриваемые непрерывные дроби невырожденные. Например, для функциональной непрерывной дроби, построенной по нормированию v_h^-, условие $q_j \neq 0$ выполнено автоматически (см. Главу 3).

Далее приведем некоторые свойства обобщенных непрерывных дробей, которые полностью аналогичны соответствующим свойствам функциональных непрерывных дробей, рассмотренные в §3.1.4.

Предложение 5.1.1.1. *При $j \in \mathbb{N}_0$ справедливы равенства*

$$\frac{p_j}{q_j} = [a_0; b_1|a_1, \ldots, b_j|a_j], \tag{5.1.1.4}$$

$$p_{j-1}q_j - p_jq_{j-1} = (-1)^j b_1 \cdot \ldots \cdot b_j, \tag{5.1.1.5}$$

$$\frac{q_j}{q_{j-1}} = [a_j; b_j|a_{j-1}, \ldots, b_2|a_1], \tag{5.1.1.6}$$

$$\frac{p_j}{p_{j-1}} = [a_j; b_j|a_{j-1}, \ldots, b_1|a_0]. \tag{5.1.1.7}$$

Доказательство. Соотношения (5.1.1.4)-(5.1.1.7) могут быть проверены по индукции. Покажем шаг индукции, например, для (5.1.1.6):

$$\frac{q_j}{q_{j-1}} = \frac{a_jq_{j-1} + b_jq_{j-2}}{q_{j-1}} = a_j + \frac{b_j}{q_{j-1}/q_{j-2}}.$$

□

Выражение $p_n/q_n = [a_0; b_1|a_1, \ldots, b_n|a_n] \in \mathcal{K}$ называется *подходящей дробью* с номером $n \in \mathbb{N}_0$. Формулы (5.1.1.3) называются *формулами Эйлера* для обобщенных непрерывных

дробей. Как и в случае обычных непрерывных дробей с $b_j = 1$, $j \in \mathbb{N}$, элементы p_n и q_n мы будем называть *континуантами* n-ой подходящей дроби (хотя формально рекуррентные формулы (5.1.1.3) обобщают традиционное понятие континуанты).

Предложение 5.1.1.2. *При $j \in \mathbb{N}_0$ справедливы тождества*

$$\alpha = \frac{\alpha_{j+1}p_j + b_{j+1}p_{j-1}}{\alpha_{j+1}q_j + b_{j+1}q_{j-1}}, \tag{5.1.1.8}$$

$$\alpha - \frac{p_j}{q_j} = \frac{(-1)^j b_1 \cdot \ldots \cdot b_{j+1}}{q_j(\alpha_{j+1}q_j + b_{j+1}q_{j-1})}. \tag{5.1.1.9}$$

Доказательство. Доказательство проводится по индукции и аналогично традиционному числовому случаю. □

Предположим, что элемент α, заданный выражением (5.1.1.2), является корнем многочлена $H(X) \in \mathcal{K}[X]$, где

$$H(X) = \lambda_2 X^2 + 2\lambda_1 X + \lambda_0, \quad \lambda_2, \lambda_1, \lambda_0 \in \mathcal{K}. \tag{5.1.1.10}$$

Обозначим сокращенный дискриминант $d = \lambda_1^2 - \lambda_2\lambda_0$ уравнения (5.1.1.10). Так как $b_j \neq 0$, то при $j \in \mathbb{N}_0$ положим

$$A_j = \left(\lambda_2 p_j^2 + 2\lambda_1 p_j q_j + \lambda_0 q_j^2\right) \cdot \prod_{i=1}^{j+1}(-b_i)^{-1}, \tag{5.1.1.11}$$

$$B_j = (\lambda_2 p_j p_{j-1} + 2\lambda_1 p_{j-1} q_j + \lambda_0 q_{j-1} q_j) \cdot \prod_{i=1}^{j}(-b_i)^{-1}. \tag{5.1.1.12}$$

Если $\alpha \neq p_j/q_j$, то $H(p_j/q_j) \neq 0$, следовательно, и $A_j \neq 0$ при $j \in \mathbb{N}_0$. Дополнительно определим $A_{-1} = \lambda_2 \neq 0$, $B_{-1} = 0$. При $j = 0$ имеем

$$A_0 = -\frac{1}{b_1}(\lambda_2 a_0^2 + 2\lambda_1 a_0 + \lambda_0), \quad B_0 - \lambda_1 = \lambda_2 a_0 + \lambda_1. \tag{5.1.1.13}$$

Предложение 5.1.1.3. *Для $j \in \mathbb{N}$ справедливо тождество*

$$\alpha_{j+1} = \frac{B_j + \lambda_2\alpha}{A_j}. \tag{5.1.1.14}$$

Доказательство. По определению мы имеем $\alpha_0 = \alpha$. Далее, из (5.1.1.8) получаем

$$\alpha_{j+1} = -\frac{b_{j+1}p_{j-1} - \alpha b_{j+1}q_{j-1}}{p_j - \alpha q_j} = -\frac{b_{j+1}(p_{j-1} - \alpha q_{j-1})(p_j - \overline{\alpha}q_j)}{(p_j - \alpha q_j)(p_j - \overline{\alpha}q_j)},$$

тогда с обозначением (5.1.1.11) имеем

$$\alpha_{j+1} = \prod_{i=1}^{j}(-b_i)^{-1}\frac{\lambda_2\left(p_j p_{j-1} - (\alpha + \overline{\alpha})q_j p_{j-1} + \alpha\overline{\alpha}q_j q_{j-1} + \alpha(q_j p_{j-1} - p_j q_{j-1})\right)}{A_j},$$

откуда, учитывая (5.1.1.5) и (5.1.1.12), получаем (5.1.1.14). □

Предложение 5.1.1.4. *Для $j \in \mathbb{N}$ справедливы тождества*

$$B_{j+1} + B_j - a_{j+1}A_j = 2\lambda_1, \tag{5.1.1.15}$$

$$d - (B_{j+1} - \lambda_1)^2 = A_j b_{j+1} A_{j+1}. \tag{5.1.1.16}$$

Доказательство. В силу (5.1.1.2) справедливо соотношение

$$\alpha_j = a_j + \frac{b_{j+1}}{\alpha_{j+1}}. \tag{5.1.1.17}$$

Подставим вместо α_j и α_{j+1} в (5.1.1.17) выражение (5.1.1.14) и приведем к общему знаменателю

$$A_j b_{j+1} A_{j-1} = (B_j + \lambda_2\alpha)(B_{j-1} - a_j A_{j-1} + \lambda_2\alpha), \tag{5.1.1.18}$$

раскрывая скобки, имеем

$$A_j b_{j+1} A_{j-1} = B_j B_{j-1} - a_j A_{j-1} B_j + \lambda_2\alpha(B_j + B_{j-1} - a_j A_{j-1}) + \lambda_2^2\alpha^2. \tag{5.1.1.19}$$

Подставим выражения для корней $H(X)$

$$\alpha,\ \overline{\alpha} = \frac{-\lambda_1 \pm \sqrt{d}}{\lambda_2}, \qquad d = \lambda_1^2 - \lambda_0\lambda_2, \tag{5.1.1.20}$$

в равенство (5.1.1.19) и приравняем коэффициенты при $\sqrt{d}$, тогда получим рекуррентное соотношение (5.1.1.15) для B_j. Подставим выражение (5.1.1.15) во вторую скобку (5.1.1.18) и воспользуемся тождеством $\lambda_2\alpha^2 + 2\lambda_1\alpha + \lambda_0 = 0$, тогда

$$B_j^2 - 2\lambda_1 B_j + A_j b_{j+1} A_{j-1} + \lambda_0\lambda_2 = 0, \tag{5.1.1.21}$$

откуда следует (5.1.1.16). □

Предложение 5.1.1.5. *При $j \in \mathbb{N}_0$ элементы α_{j+1} и $\iota\alpha_{j+1} = \overline{\alpha_{j+1}}$ являются корнями квадратного уравнения*

$$A_j X^2 - 2(B_j - \lambda_1)X - A_{j-1}b_{j+1} = 0, \tag{5.1.1.22}$$

причем справедливо тождество

$$\alpha_{j+1} = -\frac{b_{j+1}A_{j-1}}{B_j + \lambda_2\overline{\alpha}}. \tag{5.1.1.23}$$

Доказательство. В силу (5.1.1.14) и теоремы Виета для корней квадратного уравнения имеем соотношения

$$\alpha_{j+1} = \frac{B_j + \lambda_2\alpha}{A_j}, \qquad \overline{\alpha_{j+1}} = \frac{B_j + \lambda_2\overline{\alpha}}{A_j},$$

$$\alpha_{j+1} + \overline{\alpha_{j+1}} = \frac{2B_j - 2\lambda_1}{A_j}, \qquad \alpha_{j+1}\cdot\overline{\alpha_{j+1}} = \frac{B_j^2 - 2\lambda_1 B_j + \lambda_0\lambda_2}{A_j^2} = -\frac{A_{j-1}}{A_j}b_{j+1}.$$

Отсюда снова по теореме Виета заключаем, что α_{j+1} и $\overline{\alpha_{j+1}}$ являются корнями уравнения (5.1.1.22).

Из (5.1.1.21) и (5.1.1.16) имеем рекуррентные соотношения на A_j

$$A_j = \frac{2\lambda_1 B_j - B_j^2 - \lambda_0\lambda_2}{b_{j+1}A_{j-1}} = \frac{d - (B_j - \lambda_1)^2}{b_{j+1}A_{j-1}}. \tag{5.1.1.24}$$

Подставляя (5.1.1.24) в (5.1.1.14), получаем еще одно выражение для α_{j+1}

$$\alpha_{j+1} = \frac{b_{j+1}A_{j-1}(B_j + \lambda_2\alpha)}{d - (B_j - \lambda_1)^2} = -\frac{b_{j+1}A_{j-1}}{B_j + \lambda_2\overline{\alpha}}. \tag{5.1.1.25}$$

□

Предложение 5.1.1.6. *При $j \in \mathbb{N}_0$ справедливо тождество*

$$b_{j+1}A_j = b_jA_{j-2} + a_j(B_{j-1} - B_j). \tag{5.1.1.26}$$

Доказательство. Запишем (5.1.1.16) для двух последовательных номеров $j-1$ и j, а затем вычтем их:

$$0 = (B_j - \lambda_1)^2 - (B_{j-1} - \lambda_1)^2 + A_jb_{j+1}A_{j-1} - A_{j-1}b_jA_{j-2},$$

преобразуем

$$(B_j + B_{j-1} - 2\lambda_1)(B_j - B_{j-1}) = A_{j-1}(b_jA_{j-2} - b_{j+1}A_j),$$

и, подставив в первую скобку выражение (5.1.1.15), получим (5.1.1.26). □

Предложение 5.1.1.7. *Неполные частные a_j непрерывной дроби элемента α удовлетворяют квадратному уравнению*

$$A_{j-1}X^2 - 2(B_{j-1} - \lambda_1)X + b_{j+1}A_j - b_jA_{j-2} = 0, \tag{5.1.1.27}$$

причем корни этого уравнения имеют вид

$$a_j = \frac{B_{j-1} + B_j - 2\lambda_1}{A_{j-1}}, \qquad a_j' = \frac{B_{j-1} - B_j}{A_{j-1}}. \tag{5.1.1.28}$$

Доказательство. Подставим выражение (5.1.1.15) в (5.1.1.26), тогда получим аналог соотношения (5.1.1.22), а именно,

$$A_{j-1}a_j^2 - 2(B_{j-1} - \lambda_1)a_j + b_{j+1}A_j - b_jA_{j-2} = 0$$

с сокращенным дискриминантом

$$(B_{j-1} - \lambda_1)^2 - A_{j-1}(b_{j+1}A_j - b_jA_{j-2}) = d - A_{j-1}b_{j+1}A_j = (B_j - \lambda_1)^2,$$

причем корни имеют вид (5.1.1.28). □

5.1.2. Идея представления кратного дивизора

Пусть K — алгебраически замкнутое поле характеричтики, отличной от 2, и L — гиперэллиптическое поле, являющееся полем функций гиперэллиптической кривой $C : y^2 = f(x)$

рода g (см. §2.4.1). Пусть $D \in \mathrm{Div}_0(L/K)$ и $B \in \mathrm{Div}(L/K)$, $\deg B = g$. По теореме Римана-Роха (см. §2.4.2)

$$\ell(D+B) = \ell(W-D-B) + \deg(D+B) + 1 - g.$$

Имеем $\ell(D+B) \geq 1$, поскольку $\deg(D+B) = g$ и $\ell(W-D-B) \geq 0$. Следовательно, существует функция $\alpha \in \mathscr{L}(D+B)$, $\alpha \neq 0$, такая, что $(\alpha)+D+B \geq 0$, и корректно определен эффективный дивизор $E = (\alpha) + D + B$, $\deg E = g$. Если B — такой эффективный дивизор, то $D \sim E - B$, причем $[E-B] \in J(L/K)$ — *канонический представитель* в якобиане $J(L/K)$ гиперэллиптической кривой C.

Для дивизора $D \in \mathrm{Div}_0(L/K)$ предъявим конструктивное построение канонического представителя $[E-B]$ в якобиане $J(L/K)$ и явно предъявим функцию α, для которой $E - B = (\alpha)+D$. Далее построим последовательность функций α_j и последовательность эффективных дивизоров E_j степени g, для которых будут справедливы соотношения

$$E_0 = B, \quad D + B - E_j + (\alpha_j) = B - E_{j+1}, \quad jD \sim B - E_j.$$

Пусть $D = D_0 - D_\infty \in \mathrm{Div}_0(L/K)$, где D_0 и D_∞ — полуприведенные дивизоры степени $d \in \mathbb{N}$ такие, что $\mathrm{gcdiv}\,(D_0,\ D_\infty) = 0$ (см. §2.4.5). Пусть $E_0 \in \mathrm{Div}(L/K)$ — любой приведенный дивизор такой, что $D_0 + \iota D_\infty + E_0$ — полуприведенный дивизор. Запишем функцию $\alpha_1 \in L/K$ с неопределенными коэффициентами в следующем виде

$$\alpha_1 = \frac{V_1 + W_1\sqrt{f}}{U_1}, \quad V_1, W_1, U_1 \in K[x],\ \deg V_1 = d+g,\ \deg W_1 = d-1,\ \deg U_1 = d+g, \quad (5.1.2.1)$$

причем для определенности считаем $\mathrm{lc}\,(W_1) = 1$. Если

$$D_0 + \iota D_\infty + \iota E_0 = \sum_{i=1}^{2d+g} P_i, \quad (5.1.2.2)$$

где $P_i \in \mathcal{C}$ — точки на кривой $\mathcal{C}$, $P_i = (x_i, y_i)$, то имеем систему линейных уравнений на неопределенные коэффициенты многочленов V_1, W_1, U_1 следующего вида

$$V_1(x_i) + W_1(x_i)y_i = 0, \quad i = 1, 2, \ldots, 2d+g, \quad (5.1.2.3)$$

состоящую из $2d+g$ уравнений на $2d+g$ неопределенных коэффициентов: $d+g+1$ неопределенный коэффициент у многочлена V_1 и $d-1$ неопределенный коэффициент у многочлена W_1, так как $\mathrm{lc}\,(W_1) = 1$. В случае наличия в дивизоре $D_0 + \iota D_\infty + \iota E_0$ точек P_i кратности $m > 1$, вместо одинаковых условий (5.1.2.3) запишем условия

$$\frac{\mathrm{d}^k}{\mathrm{d}x^k}\left(V_1 + W_1\sqrt{f}\right)\Big|_{(x_i,y_i)} = 0, \quad k = 0, 1, \ldots, m-1, \quad (5.1.2.4)$$

при этом количество уравнений и переменных не изменяется, а система уравнений по-прежнему остается линейной. Положим $U_1 = \mathrm{Pol}\,(D_\infty + E_0)$, то есть $U_1 \in K[x]$ такой многочлен, что

$(U_1)_\circ = D_\infty + \iota D_\infty + E_0 + \iota E_0$, $\deg U_1 = d + g$. По построению справедливы соотношения

$$\left(V_1 + W_1\sqrt{f}\right)_\circ = D_0 + \iota D_\infty + \iota E_0 + E_1, \tag{5.1.2.5}$$

$$(U_1)_\circ = D_\infty + \iota D_\infty + E_0 + \iota E_0, \tag{5.1.2.6}$$

где E_1 — некоторый эффективный дивизор степени g. Если $\operatorname{gcdiv}(E_0,\ E_1) \neq 0$, то обозначим $R \in K[x]$ такой многочлен, что $(R)_\circ = \operatorname{gcdiv}(E_0,\ E_1) + \iota \operatorname{gcdiv}(E_0,\ E_1)$. Тогда $R \mid \gcd(V_1, W_1, U_1)$ (см. лемму 2.4.5.1), и в качестве V_1, W_1, U_1 будем рассматривать многочлены $V_1/R, W_1/R, U_1/R$. Поэтому далее можно считать, что $\operatorname{gcdiv}(E_0,\ E_1) = 0$.

Имеем явное выражение для дивизора функции α_1:

$$(\alpha_1) = D_0 - D_\infty + E_1 - E_0, \tag{5.1.2.7}$$

откуда

$$D_0 - D_\infty \sim E_0 - E_1. \tag{5.1.2.8}$$

Если E_1 — приведенный дивизор, то дивизор $D \in \operatorname{Div}_0(L/K)$ принадлежит классу $[E_0 - E_1] \in \Delta^\circ(L)$ с каноническим представителем $E_0 - E_1$.

Если дивизор E_1 не является приведенным, то существует представление $E_1 = T_1 + \iota T_1 + \tilde{E}_1$, где $T_1, \iota T_1, \tilde{E}_1$ — полуприведенные дивизоры. Тогда в качестве канонического представителя для дивизора D будем рассматривать $(E_0 - T_0) - (\tilde{E}_1 + \iota T_0)$, где T_0 — любой эффективный дивизор такой, что $T_0 \leq E_0$, $\deg T_0 = \deg T_1$, $\tilde{E}_1 + \iota T_0$ — полуприведенный дивизор. Необходимо проверить корректность, а именно, существование такого эффективного дивизора T_0 и независимость класса $[(E_0 - T_0) - (\tilde{E}_1 + \iota T_0)] \in \Delta^\circ(L)$ от выбора T_0. Существование T_0 следует из условия $\operatorname{gcdiv}(E_0,\ E_1) = 0$, а единственность класса $[(E_0 - T_0) - (\tilde{E}_1 + \iota T_0)] \in \Delta^\circ(L)$ следует из $(T_0 + \iota T_0) \sim \tilde{T}_0 + \iota \tilde{T}_0$ при разных выборах $T_0, \tilde{T}_0$. Итак, в этом случае вместо α_1 рассматриваем функцию $\alpha_1 T_0/T_1$, а вместо класса $[E_0 - E_1] \in \Delta^\circ(L)$ рассматриваем класс $[(E_0 - T_0) - (\tilde{E}_1 + \iota T_0)] \in \Delta^\circ(L)$.

Таким образом, по набору дивизоров (D_0, D_∞, E_0) построена функция $\alpha_1 \in L$ и эффективный дивизор $E_1 \in \operatorname{Div}_0(L/K)$, $\deg E_1 = g$, для которых справедливы соотношения (5.1.2.7)-(5.1.2.8), причем α_1 имеет вид (5.1.2.1) и выполнены соотношения (5.1.2.5)-(5.1.2.6) (и аналогичные соотношения в случае, когда E_1 не является приведенным). Аналогичным образом по индукции по набору (D_0, D_∞, E_j) построим функцию $\alpha_{j+1} \in L$ и эффективный дивизор $E_{j+1} \in \operatorname{Div}_0(L/K)$, $\deg E_{j+1} = g$, для которых выполнены аналоги соотношений (5.1.2.1)-(5.1.2.8), с заменой соответствующих индексов. Складывая соотношения $D \sim E_j - E_{j+1}$ при $j = 1, \ldots, n$, получаем $nD \sim E_0 - E_n$.

В этом параграфе мы кратко изложили основную идею построения интересующей нас обобщенной непрерывной дроби. Более подробно к этой идее мы вернемся в следующих разделах этой главы.

5.1.3. Редукция к дивизорам меньшего порядка

Пусть теперь K — поле алгебраических чисел и дивизоры D_0, D_∞, E_0 определены над K. Представленные построения (5.1.2.3)-(5.1.2.4) многочленов V_1, W_1 не очень эффективны с вычислительной точки зрения в связи с тем, что в (5.1.2.2) точки $P_i(x_i, y_i)$ вообще говоря определены над алгебраическим замыканием $\overline{K}$. Для дальнейшего построения V_{j+1}, W_{j+1}, $j \in \mathbb{N}$ мы бы хотели найти явные рекуррентные формулы, которые будут определены над полем K.

Положим $B_0 = \mathrm{Pol}\,(D_0)$, $B_\infty = \mathrm{Pol}\,(D_\infty)$ и $\mu_j = \mathrm{Pol}\,(E_j)$, $j \in \mathbb{N}_0$. Запишем

$$\left(V_{j-1} + W_{j-1}\sqrt{f}\right)_\circ + \left(V_j - W_j\sqrt{f}\right)_\circ = D_0 + \iota D_0 + D_\infty + \iota D_\infty + \iota E_{j-1} + 2E_j + \iota E_{j+1},$$

откуда

$$(V_{j-1} + W_{j-1}\sqrt{f})(V_j - W_j\sqrt{f}) = B_0 B_\infty\big(\lambda_j - \tau_j\sqrt{f}\big), \tag{5.1.3.1}$$

$$V_{j-1}^2 - W_{j-1}^2 f = B_0 B_\infty \mu_{j-1}\mu_j, \tag{5.1.3.2}$$

где $\lambda_j, \tau_j \in K[x]$ и из сравнения степеней $\deg\lambda_j \le 2g$, $\deg\tau_j \le g-1$, причем

$$\left(\lambda_j + \tau_j\sqrt{f}\right)_\circ = E_{j-1} + 2\iota E_j + E_{j+1}. \tag{5.1.3.3}$$

Заметим, что при построении V_1, W_1 в (5.1.2.1)-(5.1.2.8) если вместо набора дивизоров (D_0, D_∞, E_0) рассмотреть набор (E_{j-1}, E_j, E_j), то с точностью до умножения на константу мы получим многочлены λ_j, τ_j. Это означает, что по набору из двух многочленов (E_0, E_1) можно построить последовательность дивизоров $\{E_j\}$ и последовательность пар многочленов $\{(\lambda_j, \tau_j)\}$, для которых справедливы соотношения (5.1.3.3). Из (5.1.3.1) имеем систему

$$\begin{cases} V_{j-1}V_j - W_{j-1}W_j f = B_0 B_\infty \lambda_j, \\ W_{j-1}V_j - V_{j-1}W_j = B_0 B_\infty \tau_j, \end{cases}$$

откуда с учетом (5.1.3.2) получаем искомые рекуррентные формулы

$$V_j = \frac{\lambda_j V_{j-1} - \tau_j W_{j-1} f}{\mu_{j-1}\mu_j}, \quad W_j = \frac{\lambda_j W_{j-1} - \tau_j V_{j-1}}{\mu_{j-1}\mu_j}. \tag{5.1.3.4}$$

Остается найти эффективный способ над полем K строить последовательность пар многочленов $\{(\lambda_j, \tau_j)\}$.

5.1.4. Построение непрерывной дроби обобщенного типа

Мы хотим найти представление

$$h(\lambda_j + \tau_j\sqrt{f}) = (a_{j-1} + b_{j-1}\sqrt{f})(a_j - b_j\sqrt{f}),$$

где $h, a_{j-1}, b_{j-1}, a_j, b_j \in K[x]$ и справедливы ограничения на степени

$$\deg b_{j-1}, \deg b_j \le [(g-1)/2], \quad \deg a_{j-1}, \deg a_j \le g + [(g+1)/2], \quad \deg h \le 2[(g+1)/2], \tag{5.1.4.1}$$

причем

$$\left(a_{j-1}+b_{j-1}\sqrt{f}\right)_\infty = E_{j-1}+\iota E_j+(h)_\infty^+, \tag{5.1.4.2}$$

$$\left(a_j-b_j\sqrt{f}\right)_\infty = \iota E_j+E_{j+1}+(h)_\infty^-. \tag{5.1.4.3}$$

Уравнение (5.1.4.2) при $j=1$ и при данных эффективных дивизорах E_0, E_1 степени g дает систему из $2g$ линейных условий на $\deg a_0+\deg b_0+1$ переменную. Так как $\deg a_0+\deg b_0+1\geq 2g$, то эта система разрешима. Тем самым, по дивизорам E_0, E_1 восстанавливаются многочлены $a_0, b_0\in K[x]$ и

$$h=\frac{a_0^2-b_0^2 f}{\mu_0\mu_1}\in K[x],\quad (h)_{[2[(g+1)/2]]}=(h)_\infty^-+(h)_\infty^+.$$

Отметим, что степень многочлена h меньше $2[(g+1)/2]$ тогда и только тогда, когда носитель дивизора $(h)_\infty^-$ содержит бесконечное нормирование. Если $v_\infty^-\neq v_\infty^+$, то без ограничения общности предполагаем $v_\infty^+\left((h)_\infty^-\right)=0$.

Рассмотрим случай, когда $v_\infty^-\left((h)_\infty^-\right)=v_\infty^+\left((h)_\infty^-\right)=0$ и $\operatorname{gcdiv}\left(E_0,\ (h)_\infty^+\right)=0, \operatorname{gcdiv}\left(E_1,\ (h)_\infty^+\right)=0$.

Лемма 5.1.4.1. *Пусть E — полуприведенный конечный дивизор, то есть $E\in\operatorname{Div}(L/K)$ такой эффективный дивизор, что $2\operatorname{gcdiv}(E,\ \iota E)\leq(f)_\infty$, $v_\infty^-(E)=v_\infty^+(E)=0$. Пусть функция $\beta\in L$ такая, что для любого $v\in\operatorname{Supp}(E)$ справедливы равенства $v(\beta)=v(E)$, $v(\iota\beta)=0$. Тогда существует и единственный многочлен $\xi\in K[x]$, $\deg\xi<\deg E$, удовлетворяющий соотношению $(\beta-\xi)_\infty\geq\iota E$.*

Доказательство. Пусть $\beta=\frac{a+b\sqrt{f}}{\mu}$, тогда для любого $v\in\operatorname{Supp}(E)$ имеем $v\left(a+b\sqrt{f}\right)=v(E)$, $v\left(a-b\sqrt{f}\right)=0$, $v(\mu)=0$. Для $v\in\operatorname{Supp}(E)$ обозначим $h_v=\operatorname{Pol}(v)$ и κ_v — образ $\sqrt{f}$ в $K_v^{v(E)}=\mathcal{O}_v/\rho_v^{v(E)}$ (см. §2.3.2). С помощью алгоритма Евклида найдем $\xi_v\in K[x]$, $\deg\xi\leq v(E)\deg v$, такой, что

$$a_0+b_0\kappa_v\equiv\xi_v\mu_1\pmod{h_v^{v(E)}}.$$

Далее остается определить искомый многочлен ξ с помощью Китайской теоремы об остатках. □

Положим $a_1=\xi_0\mu_1-a_0$, где $\xi_0\in K[x]$ многочлен, определенный по лемме 5.1.4.1 для $\alpha=(a_0+b_0\sqrt{f})/\mu_1$ и $E=(h)_\infty^+$. Тогда

$$\left(a_1-b_0\sqrt{f}\right)_\infty=\left(a_0-\xi_0\mu_1+b_0\sqrt{f}\right)_\infty\geq\iota E_1+(h)_\infty^-$$

и корректно определен приведенный дивизор $E_2=\left(a_1-b_0\sqrt{f}\right)_\infty-\iota E_1-(h)_\infty^-$ — эффективный полуприведенный дивизор степени g. Следовательно, $\left(a_1+b_0\sqrt{f}\right)_\infty=E_1+\iota E_2+(h)_\infty^+$ и справедливы равенства

$$\beta_1=\frac{h}{\xi_0-\beta_0},\quad \beta_0=\frac{a_0-b_0\sqrt{f}}{\mu_1},\quad \beta_1=\frac{a_1-b_0\sqrt{f}}{\mu_2}. \tag{5.1.4.4}$$

Продолжая указанные построения, мы приходим к понятию обобщенной дроби $\beta_0 = [\xi_0; h|\xi_1, \ldots]$ (см. §5.1.1), которая *проассоциирована* с последовательностью приведенных дивизоров $\{E_j\}$:

$$(\beta_j)_\circ = \iota(E_j - E_{j+1}) + \big((h)_\circ^- - [(g+1)/2](\infty^- + \infty^+)\big). \tag{5.1.4.5}$$

Суммируя 5.1.4.5 по $j = 0, 1, \ldots, n$, получаем

$$E_n - E_0 \sim n\big((h)_\circ^+ - [(g+1)/2](\infty^- + \infty^+)\big). \tag{5.1.4.6}$$

Заметим, что многочлен b_0 входит в качестве коэффициента при $\sqrt{f}$ во все полные частные α_j. Это означает, что соответствующие классы дивизоров $[E_n - E_0]$ будут принадлежать одному и тому же обобщенному якобиану (см. подробнее о непрерывных дробях и обобщенных якобианах в [52; 154]).

Таким образом, по данным двум дивизорам E_0, E_1 сначала построена функция $\alpha_0 \in L$ и дивизор $(h)_\circ^-$ степени $[(g+1)/2]$, а потом построена непрерывная дробь обобщенного типа и соответствующая ей последовательность приведенных дивизоров $\{E_j\}$. Если учитывать выбранные ограничения на степени многочленов a_j, b_0 и степень дивизора $(h)_\circ^-$, то последовательность приведенных дивизоров $\{E_j\}$ восстанавливается однозначно. Следовательно, и многочлены λ_j, τ_j также восстанавливаются однозначно (возможно, с точностью до умножения на константу), а далее с учетом дивизоров D_0, D_∞ рекуррентным образом (5.1.3.4) восстанавливаются многочлены V_j, W_j. Из построений видно, что в случае периодичности последовательности дивизоров $\{E_j\}$ (которая может случиться, если повториться пара последовательных дивизоров), полные частные α_j и β_j будут образовывать квазипериодические последовательности.

Отметим, что по данным двум дивизорам E_0, E_1 можно восстановить целый класс многочленов V_1, W_1 и соответствующих им эффективных дивизоров D_0, D_∞ степени $d \geq g/2$, удовлетворяющих (5.1.2.5).

Можно также рассматривать и другую постановку задачи. Пусть в качестве начальных условий даны приведенный дивизор E_0 и полуприведенный дивизор $(h)_\circ^+$ степени $2k$, $1 \leq k \leq g$, носители которых не пересекаются. Тогда однозначно (с точностью до умножения на константу) восстанавливаются многочлены $a_0, b_0 \in K[x]$, $\deg a_0 = k+g$, $\deg b_0 = k-1$, которые в свою очередь определяют приведенный дивизор E_1. Далее однозначно восстанавливается последовательность полных частных β_j и последовательность приведенных дивизоров $\{E_j\}$, для которых классы дивизоров $[E_n - E_0]$ будут принадлежать одному и тому же якобиану (возможно, обобщенному якобиану).

5.2. Функциональные непрерывные дроби обобщенного типа для одного линейного нормирования

Пусть K — поле характеристики отличной от 2. В классическом случае гиперэллиптического поля $\mathcal{L} = K(X)(\sqrt{F})$, определенного свободным от квадратов многочленом $F \in K(X)$ четной степени, еще по работам Абеля и Чебышева известна связь между наличием единиц кольца $D_F = K[X](\sqrt{F}) = \{\omega_1 + \omega_2\sqrt{F} \mid \omega_1, \omega_2 \in K[X]\}$ и периодичностью разложения $\sqrt{F}$ в непрерывную дробь (подробнее см. [92]).

Рассмотрим $f \in K[x]$ — свободный от квадратов многочлен. Для поиска и построения нетривиальных S-единиц в гиперэллиптическом поле $L = K(x)(\sqrt{f})$ в главе 3 был предложен метод функциональных непрерывных дробей, причем было показано, что этот метод имеет эффективное применение для множеств S, состоящих из двух нормирований первой степени: самосопряженного бесконечного нормирования и нормирования первой степени, или двух сопряженных бесконечных нормирований, или двух сопряженных линейных нормирований.

Пусть v_h — одно из двух неэквивалентных сопряженных нормирований поля L, связанных с линейным многочленом $h \in K[x]$, $\deg h = 1$. Далее будем предполагать, что многочлен f нечетной степени $2g+1$, $g \geq 1$, и $S = \{v_h, v_\infty\}$.

В отличие от числовых непрерывных дробей, в случае функциональных непрерывных дробей возникает новое понятие квазипериодичности — периодичности с точностью до умножения на постоянную величину. Кроме того, даже при наличии в поле L нетривиальных S-единиц, не каждая квадратичная иррациональность имеет периодическое или квазипериодическое разложение в непрерывную дробь. В то же время, из наличия элементов в поле L с периодическим разложением в непрерывную дробь следует, что в поле L есть нетривиальные S-единицы, а значит, непрерывные дроби элементов $\sqrt{f}/h^g$ и $\sqrt{f}/h^{g+1}$ периодические. Тем самым, элементы $\sqrt{f}/h^g$ и $\sqrt{f}/h^{g+1}$ можно считать *ключевыми* для определения существования нетривиальных S-единиц в поле L.

Пусть $\mathcal{V}$ — множество нормирований поля L, определенных над полем K. Обозначим $\mathrm{Div}(L)$ — группу K-дивизоров поля L. Группу классов дивизоров степени ноль поля L обозначим $\Delta^\circ(L) = \mathrm{Div}^\circ(L)/\mathrm{Princ}(L)$. Все дивизоры, о которых далее пойдет речь, лежат в $\mathrm{Div}(L)$. Инволюция ι поля L, действующая $\iota : \sqrt{f} \to -\sqrt{f}$, $\iota^2 = \mathrm{id}$, может быть естественным образом определена на группе дивизоров $\mathrm{Div}(L)$ поля L.

В данном параграфе рассматриваются непрерывные дроби обобщенного типа и их связь с проблемой существования и построения фундаментальных S-единиц и S_h-единиц в гиперэллиптическом поле L, где $S_h = \{v_h, \iota v_h\}$, а также с проблемой кручения в якобиане J_f гиперэллиптической кривой C, заданной уравнением $y^2 = f(x)$.

Для традиционных функциональных непрерывных дробей в статьях [154; 156] был пред-

ставлен геометрический метод, основанный на последовательном построении специальных дивизоров для заданного элемента гиперэллиптического поля. Многочлены Мамфорда этой последовательности дивизоров оказываются тесно связанными с непрерывной дробью рассматриваемого элемента. Основные результаты данного параграфа представлены в статье [15] и были получены путем обобщения и продолжения идей [156] на случай непрерывных дробей обобщенного типа и анализа связанных с ними дивизоров в комбинации с нашими результатами [17] о фундаментальных S_h-единицах поля L.

Результаты этого раздела опубликованы в статье [15].

5.2.1. Вспомогательные построения и утверждения

Перед тем, как перейти к изложению основных результатов данного параграфа, покажем, как может быть построена непрерывная дробь обобщенного типа в поле формальных степенных рядов $K((h))$ и в гиперэллиптическом поле L, а также проведем необходимый для дальнейшего изложения анализ арифметики дивизоров для функций, связанных с построенной непрерывной дробью обобщенного типа.

Элемент $\alpha \in K((h))$ имеет вид $\alpha = \sum_{j=s}^{\infty} b_j h^j$, где $v_h(\alpha) = s \in \mathbb{Z}$, $b_s \neq 0$, $b_j \in K$ для $j \geq s$. Положим $\alpha_0 = \alpha$ и определим $a_0 = \sum_{j=s}^{0} b_j h^j = [\alpha_0]_h$, если $s < 0$, а иначе $a_0 = 0$. Множество целых неотрицательных чисел обозначим $\mathbb{N}_0$. Для каждого $j \in \mathbb{N}_0$, если $\alpha_j - a_j \neq 0$, то определим *полное частное* $\alpha_{j+1} = h/(\alpha_j - a_j) \in K((h))$ и *неполное частное* $a_{j+1} = [\alpha_{j+1}]_h$. В итоге для элемента α мы получим конечное или бесконечное выражение вида

$$a_0 + \cfrac{h}{a_1 + \cfrac{h}{a_2 + \cdots}}, \tag{5.2.1.1}$$

которое называется *непрерывной дробью обобщенного типа*. Для краткости выражение (5.2.1.1) будем записывать так $[a_0; a_1, a_2, \ldots]$, и называть *непрерывной дробью*, так как далее в этом параграфе мы будем рассматривать только непрерывные дроби вида (5.2.1.1). Если на некотором n-ом шаге $\alpha_n - a_n = 0$, то непрерывная дробь для элемента α конечная, и справедливо равенство $\alpha = [a_0; a_1, \ldots, a_n]$. Не сложно заметить, что

- непрерывная дробь (5.2.1.1) элемента α конечная тогда и только тогда, когда $\alpha \in K(x) \subset K((h))$;
- если непрерывная дробь (5.2.1.1) для элемента α бесконечная, то соответствующие подходящие дроби $[a_0; a_1, \ldots, a_j]$, $j \in \mathbb{N}_0$, сходятся к α по нормированию v_h.

Так как по предположению в $\mathcal{V}$ есть два неэквивалентных сопряженных нормирования, связанных с линейным многочленом h, то $\sqrt{f}$ представляется в виде формального степенного ряда в $K((h))$, и тем самым понятие непрерывной дроби индуцируется на элементы $\alpha \in L$,

причем вид непрерывной дроби зависит от вложения $L \subset K((h))$. Зафиксируем вложение $L \subset K((h))$, соответствующее выбранному нормированию v_h (см. §2.3.2).

Эффективный дивизор, соответствующий единственному бесконечному нормированию v_∞ поля L, обозначим $\infty \in \mathrm{Div}(L)$, тогда главный дивизор многочлена h можно записать в следующем виде $(h) = v_h + \iota v_h - 2\infty$, причем $v_h \neq \iota v_h$.

Пусть элемент $\alpha \in L$ имеет вид

$$\alpha = \frac{\sqrt{f} + V}{U}, \tag{5.2.1.2}$$

где

$$U, V \in K[x], \quad U \cdot h \mid f - V^2, \quad \deg U = g, \quad \deg V \leq g. \tag{5.2.1.3}$$

Определим

$$R = \frac{f - V^2}{U \cdot h}, \quad a = [\alpha]_h, \quad W = aU - V, \quad T = \frac{f - W^2}{U \cdot h}, \quad \beta = \frac{\sqrt{f} + W}{T}. \tag{5.2.1.4}$$

Предложение 5.2.1.1. *Справедливы следующие утверждения*

- $R, W, T \in K[x]$ — *многочлены, причем* $\deg R = \deg T = g$, $\deg W \leq g$;
- *существуют и однозначно определены эффективные дивизоры* $D_R, D_U, D_T \in \mathrm{Div}(L)$ *такие, что главные дивизоры многочленов* $R, U, T \in K[x]$ *и функций* $\sqrt{f} - V, \sqrt{f} - W \in L$ *имеют вид*

$$(R) = D_R + \iota D_R + r\big(v_h + \iota v_h\big) - 2g \cdot \infty, \quad v_h(R) = r, \tag{5.2.1.5}$$

$$(U) = D_U + \iota D_U + s\big(v_h + \iota v_h\big) - 2g \cdot \infty, \quad v_h(U) = s, \tag{5.2.1.6}$$

$$(T) = D_T + \iota D_T + t\big(v_h + \iota v_h\big) - 2g \cdot \infty, \quad v_h(T) = t, \tag{5.2.1.7}$$

$$\Big(\sqrt{f} - V\Big) = D_R + (r + s + 1)v_h + \iota D_U - (2g + 1) \cdot \infty, \tag{5.2.1.8}$$

$$\Big(\sqrt{f} - W\Big) = D_U + (s + t + 1)v_h + \iota D_T - (2g + 1) \cdot \infty; \tag{5.2.1.9}$$

- *справедливо тождество* $\beta(\alpha - a) = h$.

Доказательство. Из условий (5.2.1.3) следует, что R — многочлен степени g. Так как элемент $a = [\alpha]_h$ имеет вид $a = \tilde{a} \cdot h^{-s}$, где $\tilde{a} \in K[x]$, $\deg \tilde{a} \leq s \in \mathbb{N}_0$, $v_h(U) = s$, то W — многочлен степени не превосходящей g. Положим $v_h(R) = r$. Определим дивизоры $D_R = \mathrm{gcdiv}\left(R \cdot h^{-r},\ \sqrt{f} - V\right)$ и $D_U = \mathrm{gcdiv}\left(U \cdot h^{-s},\ \sqrt{f} - V\right)$. В силу того, что по построению (5.2.1.3) справедливо равенство $f - V^2 = R \cdot h \cdot U$, то выполнены соотношения (5.2.1.5), (5.2.1.6), (5.2.1.8).

Далее покажем, что $D_U + (s + 1)v_h \leq \left(\sqrt{f} - W\right)_\circ$. Рассмотрим тождество

$$\frac{\sqrt{f} - W}{U} = \frac{\sqrt{f} + V}{U} - a. \tag{5.2.1.10}$$

Поскольку полюса главного дивизора функции a имеют вид $s(v_h + \iota v_h)$ и $D_U \le \left(\sqrt{f} + V\right)_\circ$, то

$$\iota D_U \le \left(\frac{\sqrt{f} + V}{U} - a\right)_\infty,$$

следовательно, $D_U \le \left(\sqrt{f} - W\right)_\circ$. С другой стороны, по построению $v_h(a) = -s$ и

$$v_h\left(\frac{\sqrt{f} + V}{U} - a\right) = v_h(\alpha - a) \ge 0,$$

следовательно, $(s+1)v_h \le \left(\sqrt{f} - W\right)_\circ$. Таким образом, $D_U + (s+1)v_h \le \left(\sqrt{f} - W\right)_\circ$, следовательно, $U \cdot h \mid f - W^2$, откуда получаем, что T — многочлен степени g.

Определим $t = v_h(T)$ и D_T — такой максимальный эффективный дивизор из $\mathrm{Div}(L)$, что $D_T \le (T \cdot h^{-t})_\circ$, $\iota D_T \le \left(\sqrt{f} - W\right)_\circ$. Так как $f - W^2 = U \cdot h \cdot T$, то справедливы соотношения (5.2.1.7) и (5.2.1.9).

Единственность главных дивизоров $D_R, D_U, D_T \in \mathrm{Div}(L)$ следует из соотношений (5.2.1.4) и (5.2.1.5)-(5.2.1.9).

Соотношение $\beta(\alpha - a) = h$ следует из (5.2.1.10) и равенства $f - W^2 = U \cdot h \cdot T$. □

Предложение 5.2.1.1 позволяет с помощью формул (5.2.1.4) для элемента α, определенного в (5.2.1.2), эффективно строить непрерывную дробь вида (5.2.1.1) и ее полные частные α_n.

Предложение 5.2.1.2. *Пусть дан элемент $\alpha_0 = \alpha \in L$ вида (5.2.1.2)-(5.2.1.3). Тогда для $j \in \mathbb{Z}$, $j \ge -1$, существуют и однозначно определены многочлены $U_j, V_j \in K[x]$, $\deg U_j = g$, $\deg V_j \le g$, и эффективные дивизоры $D_j \in \mathrm{Div}(L)$, для которых при $j \ge -1$ справедливы следующие формулы:*

$$\alpha_{j+1} = \frac{V_j + \sqrt{f}}{U_{j+1}}, \quad f - V_j^2 = U_j \cdot h \cdot U_{j+1}, \tag{5.2.1.11}$$

$$a_{j+1} = [\alpha_{j+1}]_h, \quad V_{j+1} = a_{j+1}U_{j+1} - V_j, \tag{5.2.1.12}$$

$$s_{j+1} = v_h(U_{j+1}) = -v_h(a_{j+1}) = -v_h(\alpha_{j+1}), \tag{5.2.1.13}$$

$$(U_j) = D_j + \iota D_j + s_j\big(v_h + \iota v_h\big) - 2g \cdot \infty, \tag{5.2.1.14}$$

$$\left(V_j - \sqrt{f}\right) = D_j + (s_j + s_{j+1} + 1)v_h + \iota D_{j+1} - (2g+1) \cdot \infty. \tag{5.2.1.15}$$

Доказательство. По элементу α с помощью формул (5.2.1.4) строим элемент β. По построению непрерывной дроби имеем $\alpha_1(\alpha_0 - a_0) = h$, а с другой стороны по предложению 5.2.1.1 имеем $\beta(\alpha - a) = h$. Из того, что $a = a_0$ следует, что $\alpha_1 = \beta$, то есть элементы α_0 и α_1 имеют вид:

$$\alpha_j = \frac{\sqrt{f} + V_{j-1}}{U_j}, \ j = \overline{0,1}, \tag{5.2.1.16}$$

где

$$V_{-1} = V, \ U_{-1} = R, \ U_0 = U, \ V_0 = W, \ U_1 = T. \tag{5.2.1.17}$$

Положим

$$D_{-1} = D_R,\ D_0 = D_U,\ D_1 = D_T,\ s_{-1} = r,\ s_0 = s,\ s_1 = t. \tag{5.2.1.18}$$

Продолжая рассуждать аналогично и далее, с помощью предложения 5.2.1.1 завершаем доказательство предложения 5.2.1.2. □

Из предложения 5.2.1.2 следует, что данному элементу $\alpha \in L$ вида (5.2.1.2)-(5.2.1.3) соответствует корректно определенная последовательность эффективных дивизоров D_j, $j \in \mathbb{N}_0$. Следующее важное предложение играет ключевую роль в доказательстве основных результатов этого параграфа, сформулированных ниже в теореме 5.2.2.1.

Предложение 5.2.1.3. *Для $n \in \mathbb{N}$ справедливы соотношения*

$$D_n + s_n \cdot \iota v_h - D_0 - s_0 \cdot \iota v_h \sim \sum_{j=0}^{n-1} (2s_j + 1)\big(v_h - \infty\big). \tag{5.2.1.19}$$

Доказательство. Просуммируем (5.2.1.15) по $j = 0, \dots, n-1$, получим

$$\sum_{j=0}^{n-1} (2s_j + 1)v_h + \sum_{j=0}^{n-1} (D_j + \iota D_j) - \iota D_0 + \iota D_n + (s_n - s_0) \cdot v_h \sim n(2g+1) \cdot \infty. \tag{5.2.1.20}$$

Так как $\deg(D_j + s_j \cdot v_h) = g$, то в силу (5.2.1.14) из (5.2.1.20) следует (5.2.1.19). □

5.2.2. Критерий периодичности

Основные результаты этого раздела представлены в следующей теореме.

Теорема 5.2.2.1. *Пусть элемент $\alpha \in L$ имеет вид (5.2.1.2), где $U = h^g$, $V = h^g \cdot \big[\sqrt{f}h^{-g}\big]_h$. Пусть справедливы построения (5.2.1.4), (5.2.1.16)-(5.2.1.18) и (5.2.1.11)-(5.2.1.15) для $j \in \mathbb{N}_0$. Тогда следующие условия эквивалентны*

1. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $D_n = 0$;*
2. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $V_n = V_0$ и $U_n = ch^g$ для некоторой постоянной $c \in K^*$;*
3. *класс дивизора $\big(v_h - \infty\big)$ имеет конечный порядок m в группе классов дивизоров $\Delta^\circ(L)$;*
4. *класс дивизора $\big(v_h - \iota v_h\big)$ имеет конечный порядок m_h в группе классов дивизоров $\Delta^\circ(L)$;*
5. *непрерывная дробь элемента α типа (5.2.1.1), квазипериодическая с длиной квазипериода n.*

Если существуют $n, m, m_h \in \mathbb{N}$, указанные в эквивалентных условиях 1.-5., то

- *непрерывная дробь α чисто периодическая с длиной периода либо n, если в пункте 2. постоянная $c = 1$, либо с длиной периода $2n$ и коэффициентом квазипериода $1/c$, если $c \neq 1$;*

- *справедливы соотношения*

$$m = \sum_{j=0}^{n-1}(2s_j + 1), \quad \text{где } s_j = -v_h(\alpha_j) = -v_h(a_j) = v_h(U_j),\ j \in \mathbb{N}_0; \tag{5.2.2.1}$$

- *для минимального $t \in \mathbb{N}$, такого, что $D_{2t} = 0$, справедливы соотношения*

$$m_h = t + \sum_{j=0}^{2t-1} s_j; \tag{5.2.2.2}$$

- *если m четно, то $m_h = m/2$, если m нечетно, то $m_h = m$.*

Доказательство. Из вида элемента α следует, что $D_0 = 0$, $s_0 = g$.

Эквивалентность условий 1. и 2. следует из предложения 5.2.1.2.

Докажем, что из условия 3. следует условие 1.

Предположим, что дивизор $\big(v_h - \infty\big)$ имеет порядок $m \in \mathbb{N}$. Тогда найдется такой номер $n \in \mathbb{N}$, что

$$\sum_{j=0}^{n-2}(2s_j + 1) < m \leq \sum_{j=0}^{n-1}(2s_j + 1).$$

Обозначим $\delta = \sum_{j=0}^{n-1}(2s_j + 1) - m$, тогда $0 \leq \delta \leq 2s_{n-1}$. Из предложения 5.2.1.3 следует, что

$$D_n + s_n \cdot \iota v_h - D_0 - s_0 \cdot \iota v_h \sim \delta\big(v_h - \infty\big). \tag{5.2.2.3}$$

Пусть $\delta = 2\delta_0 - \delta_1$, где $\delta_1 \in \{0, 1\}$, $0 \leq \delta_0 \leq s_{n-1}$, $\delta_1 \leq \delta_0$. Так как

$$2\big(v_h - \infty\big) \sim \big(v_h - \iota v_h\big), \tag{5.2.2.4}$$

то из (5.2.2.3) получаем

$$D_n + s_n \cdot \iota v_h \sim D_0 + s_0 \cdot \iota v_h - \delta_0 \cdot \iota v_h + (\delta_0 - \delta_1)v_h + \delta_1 \cdot \infty. \tag{5.2.2.5}$$

Так как по условию теоремы $s_{n-1} \leq s_0$, то в левой и правой частях (5.2.2.5) стоят эффективные дивизоры степени g. Обозначим

$$E = D_n + s_n \cdot \iota v_h - \Big(D_0 + s_0 \cdot \iota v_h - \delta_0 \cdot \iota v_h + (\delta_0 - \delta_1)v_h + \delta_1 \cdot \infty\Big). \tag{5.2.2.6}$$

Поскольку $E \sim 0$ и степень эффективного дивизора полюсов E равна g, то по лемме 2.4.5.4 E — главный дивизор некоторой рациональной функции $\beta \in K(x)$. Для любого конечного нормирования $v \in \mathcal{V}$ такого, что $v \neq v_h$, $v \neq \iota v_h$ и $v \neq \iota v$, имеем $v(E) \cdot v(\iota E) \leq 0$, а так как E — главный дивизор рациональной функции, то получаем $v(E) = v(\iota E) = 0$. Для любого конечного нормирования $v \in \mathcal{V}$ такого, что $v = \iota v$, имеем $|v(E)| \leq 1$, а для главного дивизора рациональной функции E это возможно только, если $v(E) = 0$. Получается, что $\beta = bh^q$ для

некоторых $q \in \mathbb{Z}$ и $b \in K^*$. Из (5.2.2.6) имеем $|v_\infty(E)| \leq 1$, следовательно, $q = 0$. Так как по построению $v_h(D_n) = v_h(\iota D_n) = 0$, то $\delta = 0$ и $D_n = 0$. Отсюда следует условие 1.

Докажем, что из условия 1. следует условие 3.

Предположим, что n — минимальное число такое, что $D_n = 0$, тогда по предложению 5.2.1.3 сразу следует, что класс дивизора $\left(v_h - \infty\right)$ имеет конечный порядок m в $\Delta^\circ(L)$, причем m и n связаны соотношениями (5.2.2.1).

В силу (5.2.2.4) из условия 3. следует конечность порядка класса дивизора $\left(v_h - \iota v_h\right)$ в $\Delta^\circ(L)$, то есть следует условие 4.

Далее, при условии конечности порядка класса дивизора $\left(v_h - \infty\right)$ в $\Delta^\circ(L)$ для некоторого $t \in \mathbb{N}$ соотношение (5.2.2.2) следует из предложения 5.2.1.3.

Если справедливо условие 4, то из (5.2.2.4) имеем условие 3.

Образ дивизора $\left(v_h - \iota v_h\right)$ в группе классов дивизоров $\Delta^\circ(L)$ имеет конечный порядок m_h тогда и только тогда, когда $(U_{2t})^-_\circ = (U_0)^-_\circ$ для некоторого $t \in \mathbb{N}$, причем, если t минимальное такое число, то справедливо равенство (5.2.2.2). Из (5.2.2.1) видно, что n и m одновременно четны или нечетны, следовательно, сравнивая (5.2.2.1) и (5.2.2.2), при нечетном m имеем $n = t$ и $m_h = m$, а при четном m имеем $n = 2t$ и $m_h = m/2$.

Докажем, что условие 2. эквивалентно условию 5.

При заданном нормировании v_h непрерывная дробь полного частного $\alpha_j \in L$, зависит только от значения α_j, поэтому, в силу (5.2.1.11), квазипериодичность α_0 эквивалентна условиям $V_n = V_0$ и $U_n = cU_0$ для некоторого минимального $n \in \mathbb{N}$, то есть квазипериодичность α_0 эквивалентна условию 2.

Далее докажем, что из квазипериодичности непрерывной дроби α следует периодичность. В соответствие с предложением 5.2.1.2 из $\alpha_n = c\alpha_0$ получаем $V_{-1} = V_{n-1}$, $U_0 = cU_n$, поэтому

$$\iota D_0 + s_0 v_h = \operatorname{gcdiv}\left(V_{-1} - \sqrt{f},\ U_0\right) = \operatorname{gcdiv}\left(V_{n-1} - \sqrt{f},\ U_n\right) = \iota D_n + s_n v_h,$$

следовательно, $D_0 = D_n = 0$, $s_0 = s_n = g$. Запишем

$$\left(V_0 - \sqrt{f}\right) - \left(V_{n-1} - \sqrt{f}\right) = (s_1 - s_{n-1})v_h + (\iota D_1 - D_{n-1}).$$

По лемме 2.4.5.4 имеем $V_{n-2} = V_0$, $s_{n-1} = s_1$ и $D_{n-1} = \iota D_1$. Тогда из $\alpha_n = c\alpha_0$ следует $c\alpha_{n-1} = \alpha_1$, $ca_{n-1} = a_1$, $U_{n-1} = cU_1$. Аналогично, рассматривая разность $\left(V_1 - \sqrt{f}\right) - \left(V_{n-2} - \sqrt{f}\right)$, получаем $V_{n-3} = V_1$, $s_{n-2} = s_2$ и $D_{n-2} = \iota D_2$. Продолжая так и далее, будем иметь соотношения $V_{n-j-1} = V_{j-1}$, $s_{n-j} = s_j$, $D_{n-j} = \iota D_j$, а значит и $\alpha_{n-j} = c^{(-1)^j}\alpha_j$, $a_{n-j} = c^{(-1)^j}a_j$, $c^{(-1)^j}U_{n-j} = U_j$ для $j \leq n/2$. Если число n четно, то из последних соотношений при $j = n/2$ получаем $c = 1$. Если число n нечетно, то из $\alpha_n = c\alpha_0$ получаем

$$\alpha_n = [a_n; a_{n+1}, \ldots, a_{2n-1}, \alpha_{2n}] = [ca_0; c^{-1}a_1, \ldots, c^{(-1)^{n-1}}a_{n-1}, c^{(-1)^n}\alpha_n] = c\alpha_0,$$

откуда $\alpha_{2n} = c^{(-1)^n}\alpha_n = c^{-1}\alpha_n = \alpha_0$, то есть при $c \neq 1$ длина периода в два раза больше

длины квазипериода.

Теорема 5.2.2.1 доказана. □

Следствие 5.2.2.2. *Пусть при условиях теоремы 5.2.2.1 при последовательном разложении α в непрерывную дробь нашелся первый номер k такой, что $h^{-s_k}U_k \mid f$, где $s_k = v_h(U_k)$. Тогда длина периода равна k, если $U_k = h^{s_k}$ и k нечетно, а иначе длина периода равна $2k$.*

Доказательство. В доказательстве периодичности квазипериодической непрерывной дроби элемента α в теореме 5.2.2.1 при четном n было получено равенство $D_{n/2} = \iota D_{n/2} \neq 0$, то есть $h^{-s_{n/2}}U_{n/2} \mid f$. Таким образом, если при последовательном разложении α в непрерывную дробь найдется первый номер k такой, что $h^{-s_k}U_k \mid f$, то возможны два случая: $\deg U_k = s_k$ и $\deg U_k > s_k$.

Если $\deg U_k = s_k$, то $U_k = ch^{s_k}$, причем k нечетно, поскольку при четном k было бы справедливо равенство $D_{k/2} = \iota D_{k/2}$, что противоречит минимальности номера k. При $c = 1$ получаем длину периода k, а при $c \neq 1$ получаем длину периода $2k$.

Если $\deg U_k > s_k$, то из условия $h^{-s_k}U_k \mid f$ получаем $D_k = \iota D_k \neq 0$, и

$$\left(V_{k-1} - \sqrt{f}\right) - \left(V_k - \sqrt{f}\right) = (s_{k-1} - s_{k+1})v_h + (\iota D_{k-1} - D_{k+1}),$$

следовательно, по лемме 2.4.5.4 имеем $V_k = V_{k-1}$, $s_{k+1} = s_{k-1}$ и $D_{k+1} = \iota D_{k-1}$. По построению непрерывной дроби справедливы соотношения (см. предложение 5.2.1.2)

$$f - V_{k-1}^2 = U_{k-1}hU_k, \quad f - V_k^2 = U_k hU_{k+1},$$

из которых имеем $U_{k+1} = U_{k-1}$. Рассматривая разность $\left(V_{k-2} - \sqrt{f}\right) - \left(V_{k+1} - \sqrt{f}\right)$, получаем $V_{k+1} = V_{k-2}$, $s_{k+2} = s_{k-2}$, $D_{k+2} = \iota D_{k-2}$ и $U_{k+2} = U_{k-2}$. Продолжая так и далее, в итоге получим $V_{2k-1} = V_0$, $s_{2k} = s_0 = g$, $D_{2k} = \iota D_0 = 0$ и $U_{2k} = U_0 = h^g$, откуда следует периодичность α с длиной периода, равной $2k$. □

5.2.3. Алгоритм поиска S-единиц

Теорема 5.2.2.1, следствие 5.2.2.2 и формулы (5.2.1.11)-(5.2.1.12) позволяют в гиперэллиптическом поле $L = K(x)(\sqrt{f})$ для линейного многочлена h сформулировать эффективный алгоритм поиска S_h-единиц и классов дивизоров конечного порядка в $\Delta^\circ(L)$.

Если алгоритм 5 завершился успешно, то в поле L существует фундаментальные S-единица и S_h-единица, а в $\Delta^\circ(L)$ классы дивизоров $(h)^- - \infty$ и $(h)^- - (h)^+$ имеют конечный порядок. Степень фундаментальных S-единицы и S_h-единицы, порядок классов дивизоров $(h)^- - \infty$ и $(h)^- - (h)^+$ в $\Delta^\circ(L)$, длину квазипериода и длину периода можно найти из теоремы 5.2.2.1 и следствия 5.2.2.2.

Продемонстрируем полученные результаты на примерах, найденных с помощью алгоритма 5 для $g = 3$.

Алгоритм 5. Алгоритм поиска S_h-единиц, $\deg h = 1$.

1: **Дано:** свободный от квадратов многочлен $f \in K[x]$, $\deg f = 2g+1$, $g \geq 1$, линейный многочлен $h \in K[x]$ вида $h = x - h_0$ такой, что $f(h_0)$ является полным квадратом в поле K, $j_0 \in \mathbb{N}$.

2: **Вычислить:**
$$\xi = \sum_{j=0}^{g} f_j h^j \in K[x], \quad \text{где } \sqrt{f} = \sum_{j=0}^{\infty} f_j h^j \in K((h));$$

3: **положить:** $U_0 = h^g$, $V_{-1} = \xi$, $s_0 = g$;

4: **Цикл для** $j \in \mathbb{N}_0$, $j < j_0$, **выполнить:**

5: **вычислить:** $a_j = \left[\frac{V_{j-1}+\xi}{U_j}\right]_h^-$;

6: **вычислить:** $V_j = a_j \cdot U_j - V_{j-1}$;

7: **вычислить:** $U_{j+1} = \frac{f - V_j^2}{U_j \cdot h}$;

8: **вычислить:** $s_{j+1} = v_h(U_{j+1})$;

9: **если** $h^{-s_{j+1}} U_{j+1} \mid f$, **то** успешно завершить цикл.

10: **Конец цикла**

11: **Вернуть**: $k = j+1$, $\{U_i\}_{i=0}^{j+1}$, $\{V_{i-1}\}_{i=0}^{j+1}$, $\{s_i\}_{i=0}^{j+1}$, $\{a_i\}_{i=0}^{j}$.

Пример 5.2.3.1. *Рассмотрим поле* $K = \mathbb{Q}$ *и многочлен*
$$f = h^7 + 2h^6 - 2h^5 - h^4 - 2h^3 - h^2 + 2h + 1 =$$
$$= (h-1)\left(h^6 + 3h^5 + h^4 - 2h^2 - 3h - 1\right).$$
Нормирование v_h *поля* $\mathbb{Q}(h)$ *имеет два неэквивалентных продолжения* v_h^- *и* v_h^+ *на поле* $L = \mathbb{Q}(h)(\sqrt{f})$. *Элемент* $\sqrt{f}$ *имеет следующее разложение в* $\mathbb{Q}((h))$
$$\sqrt{f} = 1 + h - h^2 + \ldots$$
Бесконечное нормирование поля $\mathbb{Q}(x)$ *имеет единственное продолжение на поле* L. *Рассмотрим* $D_0 = g \cdot v_h$, *где* $g = 3$. *Находим*
$$U_0 = h^3, \quad V_0 = 1 + h - h^2.$$
Далее строим непрерывную дробь вида (5.2.1.1) *для элемента* $\sqrt{f}/h^3$ *по нормированию* v_h^-:
$$\frac{\sqrt{f}}{h^3} = \left[-\frac{1}{h^3}\left(h^2 - h - 1\right); \overline{-1, -\frac{2}{h^2}(h+1)^2, -1, -\frac{2}{h^3}\left(h^2 - h - 1\right)}\right].$$
Непрерывная дробь элемента $\sqrt{f}/h^3$ *периодическая, причем период симметричен, длина периода равна длине квазипериода и равна* 4. *Замечаем, что* $U_4 = U_0$ *и* $V_4 = V_0$, *поэтому справедливы условия теоремы* 5.2.2.1 *и, следовательно, в якобиане гиперэллиптического поля* L *класс дивизора* $\left(v_h - \infty\right)$ *имеет порядок* $m = 14$, *а класс дивизора* $\left(v_h - \iota v_h\right)$ *имеет*

порядок $m/2 = 7$. *В поле* L *существует фундаментальная* S*-единица и степени* 14*:*

$$u = \mu_1 - \mu_2\sqrt{f}, \qquad u \cdot \overline{u} = h^{14}$$
$$\mu_1 = h^7 + 2h^6 + 6h^5 + 2h^4 - 4h^2 - 6h - 2,$$
$$\mu_2 = -2\left(h^3 + h^2 + 2h + 1\right).$$

Также в поле L *существует фундаментальная* S_h*-единица* u_h *степени* 7, $u_h = u \cdot h^{-7}$.

Пример 5.2.3.2. *Рассмотрим поле* $K = \mathbb{Q}$ *и многочлен*

$$f = h^7 + h^6 + h^4 - 2h^2 + 1 = (h+1)\left(h^6 + h^3 - h^2 - h + 1\right).$$

Нормирование v_h *поля* $\mathbb{Q}(h)$ *имеет два неэквивалентных продолжения* v_h^- *и* v_h^+ *на поле* $L = \mathbb{Q}(h)(\sqrt{f})$. *Элемент* $\sqrt{f}$ *имеет следующее разложение в* $\mathbb{Q}((h))$

$$\sqrt{f} = 1 - h^2 + \dots$$

Бесконечное нормирование поля $\mathbb{Q}(x)$ *имеет единственное продолжение на поле* L. *Рассмотрим* $D_0 = g \cdot v_h$, *где* $g = 3$. *Находим*

$$U_0 = h^3, \quad V_0 = 1 - h^2.$$

Далее строим непрерывную дробь вида (5.2.1.1) *для элемента* $\sqrt{f}/h^3$ *по нормированию* v_h^-*:*

$$\frac{\sqrt{f}}{h^3} = \left[-\frac{1}{h^3}(h-1)(h+1)\,; \overline{-\frac{2}{h^2}(h-1), -\frac{2}{h^3}(h-1)(h+1)}\right].$$

Непрерывная дробь элемента $\sqrt{f}/h^3$ *периодическая, причем период симметричен, длина периода равна длине квазипериода и равна* 4. *Замечаем, что* $U_2 = U_0$ *и* $V_2 = V_0$, *поэтому справедливы условия теоремы* 5.2.2.1 *и, следовательно, в якобиане гиперэллиптического поля* L *класс дивизора* $\left(v_h - \infty\right)$ *имеет порядок* $m = 12$, *а класс дивизора* $\left(v_h - \iota v_h\right)$ *имеет порядок* $m/2 = 6$. *В поле* L *существует фундаментальная* S*-единица и степени* 12*:*

$$u = \mu_1 - \mu_2\sqrt{f}, \qquad u \cdot \overline{u} = h^{12}$$
$$\mu_1 = h^6 + 2h^3 - 2h^2 - 2h + 2,$$
$$\mu_2 = -2(h-1).$$

Также в поле L *существует фундаментальная* S_h*-единица* u_h *степени* 6, $u_h = u \cdot h^{-6}$.

5.3. Функциональные непрерывные дроби обобщенного типа для двух несопряженных линейных нормирований

За последние несколько десятилетий теория функциональных непрерывных дробей стала мощным инструментом в проблеме поиска фундаментальных единиц (см. [61; 92]) и в проблеме поиска фундаментальных S-единиц (см. [17—19], [20; 130; 166]), хотя истоки применения непрерывных дробей в данном ключе относятся к значительно более раннему периоду, восходящему к работам Абеля [127] и Чебышева [129].

Пусть L — гиперэллиптическое поле. В разделе 5.2 показано, что кроме функциональных непрерывных дробей обыкновенного вида, также можно рассматривать функциональные непрерывные дроби обобщенного типа, у которых в числителе вместо 1 стоит h — многочлен первой степени, связанный с нормированием поля L, по которому строится непрерывная дробь обобщенного типа. Оказывается, что для непрерывных дробей такого вида (h-*дробей*) справедливы аналоги основных утверждений теории функциональных непрерывных дробей, в том числе может быть установлена связь между проблемами периодичности непрерывной дроби, проблемой существования и построения фундаментальных S-единиц и проблемой кручения в якобиане гиперэллиптической кривой (см. теорему 5.2.2.1).

Используя идеи из раздела 5.1 в этом разделе построена теория функциональных непрерывных дробей обобщенного типа со сходимостью сразу по двум различным несопряженным линейным нормированиям в поле L. Обозначим через S множество, состоящее из этих двух линейных нормирований. Нами найдены эквивалентные условия, описывающие взаимосвязь условия квазипериодичности непрерывной дроби обобщенного типа для ключевых элементов поля L, наличия фундаментальной S-единицы, и наличия соответствующего класса дивизоров конечного порядка в группе классов дивизоров гиперэллиптического поля L. Последнее условие эквивалентно наличию точки кручения в якобиане соответствующей гиперэллиптической кривой.

Результаты этого раздела опубликованы в статье [7].

5.3.1. Дивизоры гиперэллиптического поля

Пусть K — произвольное поле характеристики отличной от 2. Пусть $f \in K[x]$ — некоторый свободный от квадратов многочлен, $L = K(x)(\sqrt{f})$ — гиперэллиптическое поле. Обозначим множество нормирований поля L, определенных над полем K, через $\mathcal{V}$ и S — некоторое конечное его подмножество.

Обозначим $v = v_h$ нормирование поля $K(x)$, соответствующее неприводимому многочлену $h \in K[x]$, и $\overline{K(x)_v}$ — пополнение поля $K(x)$ по нормированию v. Предположим, что нормирование v поля $K(x)$ имеет два продолжения v^- и v^+ на поле L. Это означает, что поле L

может быть вложено в $\overline{K(x)_v}$ двумя способами, которые соответствуют нормированиям v^- и v^+, и каждый элемент $\beta \in L$ имеет два разложения в степенные ряды в поле формальных степенных рядов, которые также соответствуют нормированиям v^- и v^+:

$$\beta = \sum_{j=s_0}^{\infty} e_j^{\pm} h_v^j, \quad e_j^{\pm} \in K[x],\ \deg e_j^{\pm} < \deg h,$$

причем для любого $s \geq s_0$ имеем

$$v^{\pm}\left(\beta - \sum_{j=s_0}^{s} e_j^{\pm} h_v^j\right) > s,$$

где в обозначениях $v^{\pm}$ и $e_j^{\pm}$ везде выбирается знак $+$ или знак $-$. Будем полагать, что $\deg v^- = \deg v^+ = \deg h$.

Обозначим $\mathrm{Div}(L)$ — группу K-дивизоров поля L (см. §2.4.1). Там, где ясно, что суммирование берется по $v \in \mathcal{V}$, будем его опускать. Все дивизоры, о которых далее пойдет речь, определены над K и лежат в $\mathrm{Div}(L)$.

Для нормирования v_h поля $K(x)$, заданного с помощью неприводимого многочлена $h \in K[x]$, имеющего два неэквивалентных продолжения v_h^- и v_h^+ на поле L, обозначим эффективные дивизоры соответствующие плейсам v_h^-, v_h^+ в поле L: $(h)_\circ^- = 1 \cdot v_h^-$, $(h)_\circ^+ = 1 \cdot v_h^+$, $(h)_\circ^-, (h)_\circ^+ \in \mathrm{Div}(L)$. Если же продолжения v_h^- и v_h^+ нормирования v_h поля $K(x)$ на поле L эквивалентны, то будем писать $v_h = v_h^- = v_h^+$, $(h)_\circ^- = (h)_\circ^+ \in \mathrm{Div}(L)$. Аналогично, для продолжений v_∞^- и v_∞^+ бесконечного нормирования v_∞ поля $K(x)$, будем использовать обозначения эффективных дивизоров $\infty^- = 1 \cdot v_\infty^-$ и $\infty^+ = 1 \cdot v_\infty^+$, причем $\infty^- \neq \infty^+$, если $v_\infty^- \neq v_\infty^+$, и $\infty^+ = \infty^- = \infty$, если $v_\infty^- = v_\infty^+ = v_\infty$. Таким образом, например, запись $\infty^- + \infty^+$ мы будем использовать, как для случая $\infty^- \neq \infty^+$, так и для случая $\infty^- = \infty^+$, когда $\infty^- + \infty^+ = 2\infty$.

Инволюция ι поля L, действующая $\iota : \sqrt{f} \to -\sqrt{f}$, $\iota^2 = \mathrm{id}$, может быть естественным образом определена на множестве нормирований поля L. Действительно, если нормирование v поля $K(x)$ имеет два продолжения v^- и v^+ (возможно эквивалентных), то для любого $\alpha \in L$ имеем $v^-(\alpha) = v^+(\iota\alpha) = \iota v^+(\alpha)$, поэтому корректно писать $v^- = \iota v^+$ и $v^+ = \iota v^-$. Следовательно, инволюция ι естественным образом продолжается на $\mathrm{Div}(L)$ — группу K-дивизоров поля L. В частности, $\infty^+ = \iota\infty^-$, $(h)_\circ^+ = \iota\,(h)_\circ^-$.

Группу дивизоров степени ноль поля L обозначим $\mathrm{Div}^\circ(L)$, группу главных дивизоров поля L обозначим $\mathrm{Princ}(L)$, *группу классов дивизоров степени ноль* поля L обозначим $\Delta^\circ(L) = \mathrm{Div}^\circ(L)/\mathrm{Princ}(L)$.

Для $t \in \mathbb{N}$ и функции $\alpha \in K[x][\sqrt{f}]$ вида $\alpha = V + W\sqrt{f}$, где $V, W \in K[x]$, обозначим $(\alpha)_{[t]} = (\alpha) + t(\infty^- + \infty^+)$ (см. лемму 2.4.5.2).

Лемма 5.3.1.1. *Если $t \geq \deg(\alpha)_\circ$, то дивизор $(\alpha)_{[t]}$ эффективный.*

Доказательство. Если поле $L = K(x)(\sqrt{f})$ вкладывается в поле формальных степенных

рядов $K((1/x))$, то утверждение следует из предложения 2.3.2.2. В противном случае, если поле $L = K(x)(\sqrt{f})$ не вкладывается в поле формальных степенных рядов $K((1/x))$, то в поле L справедливо $v_\infty^- = v_\infty^+ = v_\infty$, и $(\alpha)_\infty = \deg(\alpha)_\circ \cdot \infty$, причем $\deg(\alpha)_\circ \le t$. □

Пусть $V \in K[x]$, $\deg V \le g+1$, тогда по предложению 2.3.2.2 имеем $v_\infty^\pm\left(V - \sqrt{f}\right) \ge -g-1$. Значит, дивизор $\left(V - \sqrt{f}\right)_{[g+1]}$ эффективный и $\deg\left(V - \sqrt{f}\right)_{[g+1]} = 2(g+1)$, причем

$$\left(V - \sqrt{f}\right)_{[g+1]} = \left(V - \sqrt{f}\right) + (g+1)(\infty^- + \infty^+), \tag{5.3.1.1}$$

где $\left(V - \sqrt{f}\right)$ — главный дивизор функции $V - \sqrt{f} \in L$.

Назовем дивизор $D \in \mathrm{Div}(L)$ *приведенным*, если D эффективный дивизор степени g, такой, что $2\,\mathrm{gcdiv}(D,\ \iota D) \le (f)_{[2g+2]}$. Для приведенного дивизора $D \in \mathrm{Div}(L)$ корректно определен многочлен $U = \mathrm{Pol}(D) \in K[x]$, $\deg U \le g$, главный дивизор которого удовлетворяет соотношению

$$(U) = D + \iota D - g(\infty^- + \infty^+). \tag{5.3.1.2}$$

причем, если справедливо $v_\infty^-(D) = v_\infty^+(D) = 0$, то $\deg U = g$.

В обратную сторону, по данному многочлену $U \in K[x]$, $\deg U \le g$, приведенный дивизор $D \in \mathrm{Div}(L)$, удовлетворяющий (5.3.1.2), восстанавливается не всегда однозначно.

Рассмотрим приведенный дивизор $D \in \mathrm{Div}(L)$ и соответствующий многочлен $U = \mathrm{Pol}(D) \in K[x]$. Определим эффективные дивизоры $(U)_\circ^-, (U)_\circ^+, (U)_{[g]}^-, (U)_{[g]}^+ \in \mathrm{Div}(L)$ следующим образом:

$$\begin{gathered}(U)_\circ^- = \mathrm{gcdiv}(D,\ (U)_\circ), \quad (U)_\circ^+ = \iota(U)_\circ^- = \mathrm{gcdiv}(\iota D,\ (U)_\circ), \\ (U)_{[g]}^- = (U)_\circ^- + (g - \deg U)\infty^-, \quad (U)_{[g]}^+ = (U)_\circ^+ + (g - \deg U)\infty^+.\end{gathered} \tag{5.3.1.3}$$

Отметим, что $(U)_{[g]}^-$ и $(U)_{[g]}^+$ — приведенные дивизоры. Если $v_\infty^+(D) = 0$, то $(U)_{[g]}^- = D$.

Далее мы будем везде использовать сокращенную запись $(U)_\circ^-, (U)_\circ^+$, подразумевая под ней дивизоры $(U)_{[g]}^-$ и $(U)_{[g]}^+$ степени g соответственно. Также под сокращенной записью $\left(V - \sqrt{f}\right)_\circ$ для $V \in K[x]$, $\deg V \le g+1$, мы будем иметь в виду дивизор $\left(V - \sqrt{f}\right)_{[g+1]}$ степени $2(g+1)$.

В случае $K = \mathbb{C}$ следующее утверждение может быть доказано методами гл. IIIa [48] (см. также 2.4.5.3 и [156]). Мы дадим другое конструктивное доказательство, справедливое для произвольного поля K.

Предложение 5.3.1.2. *Пусть $g \ge 1$ и неэквивалентные нормирования v_x, v_h поля $K(x)$ имеют по два неэквивалентных продолжения $v_x^- \ne v_x^+$, $v_h^- \ne v_h^+$ на поле L, которым соответствуют эффективные дивизоры $(x)_\circ^- \ne (x)_\circ^+$, $(h)_\circ^- \ne (h)_\circ^+$ такие, что $\deg(x)_\circ^- = \deg(h)_\circ^- = 1$. Пусть $D \in \mathrm{Div}(L)$ — некоторый приведенный дивизор такой, что $v_x^+(D) = v_h^+(D) = 0$. Тогда*

1. *существует единственный многочлен* $V \in K[x]$, $\deg V \le g+1$, *такой, что* $D + (x)_\circ^- + (h)_\circ^- \le \left(V - \sqrt{f}\right)_{[g+1]}$;

2. *существует единственный с точностью до умножения на постоянную из* K^* *многочлен* $U \in K[x]$, $\deg U \le g$, *такой, что главный дивизор* $(U) = D + \iota D - g(\infty^- + \infty^+)$;

3. *дивизор* $E = \left(V - \sqrt{f}\right)_{[g+1]} - D - (x)_\circ^- - (h)_\circ^-$ *является приведенным;*

4. *если* $\infty^- \ne \infty^+$, *то* $v_\infty^\pm\left(V - \sqrt{f}\right) = \delta^\pm - (g+1)$, *причем* $\delta^\pm \in \mathbb{N}_0$, $\delta^\pm \ge v_\infty^\pm(D)$, $\delta^- \cdot \delta^+ = 0$;

5. *корректно определен многочлен* $T \in K[x]$:
$$T = \frac{f - V^2}{Uxh} \in K[x], \quad \deg T \le g;$$

6. *справедливо равенство* $(T) = E + \iota E - g(\infty^- + \infty^+)$.

Доказательство. Доказательство проведем конструктивным образом.

Представим дивизор $D+(x)_\circ^-+(h)_\circ^-$ в виде суммы дивизоров $D+(x)_\circ^-+(h)_\circ^- = D_1+D_2+D_\infty$, где
$$D_1 = \sum_{v=\iota v \ne v_\infty^\pm} n_v(D)\cdot v, \quad D_2 = \sum_{v\ne\iota v\ne v_\infty^\pm} n_v(D)\cdot v,$$
$$D_\infty = v_\infty^-(D)\cdot\infty^- + v_\infty^+(D)\cdot\infty^+.$$
Ясно, что $\deg D_2 > 0$. Без ограничения общности мы рассмотрим только случай, когда $D_\infty = n_\infty\cdot\infty^-$, $n_\infty \in \mathbb{N}_0$. Так как D — приведенный дивизор, то для $v = \iota v \in \mathcal{V}$ имеем $v(D) = v(D_1) \le 1$. Для $j = 1$ и $j = 2$ положим V_j — многочлен минимальной степени с единичным старшим коэффициентом такой, что $D_j \le (V_j)_\circ$. Тогда $V_j \in K[x]$, и многочлен V_1 делит f. Для каждого нормирования $v \in \operatorname{Supp} D_2$ определим многочлен $V_v \in K[x]$, $\deg V_v < v(D)\cdot\deg v$, так, что $v\left(\sqrt{f} - V_v\right) \ge v(D)$. Мы можем это сделать, например, разложив $\sqrt{f}$ в ряд по нормированию v. По китайской теореме об остатках существует единственный многочлен $V_3 \in K[x]$, $\deg V_3 < \deg D_2$, такой, что для всех нормирований $v \in \operatorname{Supp} D_2$ выполнено сравнение
$$V_1 V_3 \equiv V_v \pmod{h_v^{v(D)}},$$
где многочлены $h_v \in K[x]$ соответствуют нормированиям $v \in \mathcal{V}$. Определим многочлен $V_\infty \in K[x]$, $\deg V_\infty = n_\infty - 1$, так, что
$$v_\infty^-\left(\sqrt{f} - V_\infty\cdot V_2\cdot V_1\right) \le n_\infty - (g+1),$$
причем, если $n_\infty = 0$, то $V_\infty = 0$. Для этого достаточно заметить, что $\deg V_1 + \deg V_2 + n_\infty - 1 = g+1$, и разложить $\sqrt{f}$ в ряд по нормированию v_∞^-. Остается положить
$$V = V_1\left(V_3 + V_2\cdot V_\infty\right).$$

Действительно, для любого $v \in \operatorname{Supp} D_2$ имеем

$$V \equiv V_1 V_3 \equiv V_v \pmod{h_v^{v(D)}},$$

следовательно, $v\left(\sqrt{f} - V\right) \geq n_v(D)$. Также $V_1 \mid \gcd(V,\ f)$, следовательно, для $v \in \operatorname{Supp} D_1$ имеем $v\left(\sqrt{f} - V\right) \geq n_v(D)$. Наконец,

$$\deg\left(V - V_2 V_1 V_\infty\right) = \deg V_1 + \deg V_3 < \deg D_1 + \deg D_2 = g + 2 - n_\infty,$$

следовательно, $v_\infty^-\left(\sqrt{f} - V\right) \geq n_\infty - (g+1)$. Теперь ясно, что $D + (x)_\circ^- + (h)_\circ^- = D_1 + D_2 + D_\infty \leq \left(V - \sqrt{f}\right)_{[g+1]}$.

Если $v_\infty^-(D) = v_\infty^+(D) = 0$, то можно положить $U = \operatorname{Pol}(D)$. В общем случае многочлен $U \in K[x]$ можно определить как произведение неприводимых многочленов, соответствующих ограничению на поле $K(x)$ конечных нормирований, входящих в дивизор D с учетом кратности. Так как D приведенный, то $\deg D = g$ и $v_\infty^-(D) \cdot v_\infty^+(D) = 0$, если $\infty^- \neq \infty^+$, и $0 \leq v_\infty(D) \leq 1$, если $\infty^- = \infty^+ = \infty$. Следовательно, $(U) = D + \iota D - g(\infty^- + \infty^+)$. Ясно, что многочлен U определен однозначно с точностью до умножения на постоянную из K^*.

Докажем, что построенный многочлен V единственный. Предположим, что существует еще один многочлен $V' \in K[x]$ такой, что $V' \neq V$, $\deg V' \leq g+1$ и $D + (x)_\circ^- + (h)_\circ^- \leq \left(V' - \sqrt{f}\right)_{[g+1]}$. Тогда $D + (x)_\circ^- + (h)_\circ^- \leq (V' - V)_\circ$ и $\iota(D + (x)_\circ^- + (h)_\circ^-) \leq (V' - V)_\circ$, следовательно, $Uxh \mid (V' - V)$ и $\deg(V' - V) \leq g + 1 - \deg(D_\infty)$, но $\deg(Uxh) = g + 2 - \deg(D_\infty)$. Противоречие.

По лемме 2.4.5.1 справедливо

$$2\operatorname{gcdiv}\left(V + \sqrt{f},\ V - \sqrt{f}\right) = \operatorname{gcdiv}(V,\ f) \geq (V_1)_\circ.$$

Для $E = \left(V - \sqrt{f}\right)_{[g+1]} - D - (x)_\circ^- - (h)_\circ^-$ имеем $\deg E = g$, и опять по лемме 2.4.5.1 получаем

$$2\operatorname{gcdiv}(E,\ \iota E) = \operatorname{gcdiv}(V,\ f) - (V_1)_\circ \leq (f)_\circ,$$

откуда следует пункт 3 о том, что дивизор E приведенный.

Пункт 4 следует из рассуждений выше и леммы 2.4.5.1.

Пункт 5 следует из определения многочленов V и U в пунктах 1 и 2.

Для доказательства пункта 6 достаточно заметить, что по пунктам 1-5 и обозначению (5.3.1.1) справедливы равенства

$$\begin{gathered}
(T) = \left(f - V^2\right) - (U) - (x) - (h) = \\
= \left(V - \sqrt{f}\right) + \left(V + \sqrt{f}\right) - D - \iota D - \\
- (x)_\circ^- - (x)_\circ^+ - (h)_\circ^- - (h)_\circ^+ + (g+2)(\infty^- + \infty^+) = \\
= \left(V - \sqrt{f}\right)_{[g+1]} - D - (x)_\circ^- - (h)_\circ^- + \left(V + \sqrt{f}\right)_{[g+1]} - \iota D - (x)_\circ^+ - (h)_\circ^+ = \\
= E + \iota E - g(\infty^- + \infty^+).
\end{gathered}$$

Предложение 5.3.1.2 доказано. □

Для данного приведенного дивизора $D \in \mathrm{Div}(L)$, $v_x^+(D) = v_h^+(D) = 0$, и данных дивизоров $(x)_\circ^-$, $(h)_\circ^-$, соответствующих линейным нормированиям v_x^-, v_h^-, назовем *представлением Мамфорда* дивизора $D + (x)_\circ^- + (h)_\circ^-$ набор из двух многочленов (Uxh, V), корректно определенных по предложению 5.3.1.2. Представление Мамфорда данного приведенного дивизора определено однозначно с точностью до умножения многочлена U на постоянную из K^*. Из предложения 5.3.1.2 следует, что представлением Мамфорда дивизора $E + (x)_\circ^- + (h)_\circ^- = \left(V - \sqrt{f}\right)_{[g+1]} - D$ является набор (Txh, V).

Теперь покажем, как по представлению Мамфорда — набору из двух многочленов, удовлетворяющих специальным условиям, — построить соответствующий приведенный дивизор.

Пусть даны многочлены $T, U, V \in K[x]$, удовлетворяющие условиям

$$UxhT = f - V^2, \quad \deg U \le g, \quad \deg T \le g, \quad \deg V \le g+1. \tag{5.3.1.4}$$

Если заранее не определены обозначения продолжений нормирований v_x и v_h поля $K(x)$ на поле $L = K(x)(\sqrt{f})$, то без ограничения общности считаем обозначения нормирований $v_x^- \ne v_x^+$, $v_h^- \ne v_h^+$ такими, что $v_x^-\left(V - \sqrt{f}\right) > 0$ и $v_h^-\left(V - \sqrt{f}\right) > 0$, поскольку $xh \mid f - V^2$. Положим

$$D = \mathrm{gcdiv}\left(\left(V - \sqrt{f}\right)_{[g+1]},\ (U)_{[g]}\right). \tag{5.3.1.5}$$

Тогда D — приведенный дивизор, и представление Мамфорда дивизора $D + (x)_\circ^- + (h)_\circ^-$ имеет вид (Uxh, V). Действительно, по определению D — эффективный дивизор, по лемме 2.4.5.1 справедливо соотношение $2\,\mathrm{gcdiv}\,(D,\ \iota D) \le (f)_{[2(g+1)]}$, и, наконец, в силу

$$(U)_{[g]} \le \left(V - \sqrt{f}\right)_{[g+1]} + \left(V + \sqrt{f}\right)_{[g+1]}$$

имеем $\deg D = g$. Кроме того, по предложению 5.3.1.2 единственным образом определен приведенный дивизор E такой, что набор (Txh, V) является представлением Мамфорда $E + (x)_\circ^- + (h)_\circ^-$.

Отметим, что выполненное построение приведенных дивизоров D и E зависит от выбора обозначений нормирований v_x^- и v_h^-, которые можно зафиксировать с помощью дополнительных условий:

$$v_x^-\left(V - \sqrt{f}\right) > 0, \quad v_h^-\left(V - \sqrt{f}\right) > 0. \tag{5.3.1.6}$$

Таким образом, справедливо следующее предложение.

Предложение 5.3.1.3. *Существуют взаимно однозначные соответствия между следующими множествами*

- *множеством приведенных дивизоров* $D \in \mathrm{Div}(L)$, $v_x^+(D) = v_h^+(D) = 0$;

- *множеством пар многочленов* $U, V \in K[x]$, $\operatorname{lc}(U) = 1$, *удовлетворяющих* (5.3.1.4) *для некоторого* $T \in K[x]$;
- *множеством элементов* $\alpha = \frac{\sqrt{f}+V}{T} \in L$, *где многочлены* $T, V \in K[x]$, $\operatorname{lc}(T) = 1$, *удовлетворяют условиям* (5.3.1.4) *для некоторых* $U \in K[x]$.

Оставляя уже введенные обозначения, в следующем предложении обоснован основной шаг построения последовательности приведенных дивизоров и их представлений Мамфорда, причем каждый следующий приведенный дивизор (и его представление Мамфорда) однозначно определяется по последнему в последовательности приведенному дивизору.

Предложение 5.3.1.4. *Пусть*

$$r = v_x(T), \quad s = v_h(T), \quad B = Tx^{-r}h^{-s}. \tag{5.3.1.7}$$

Тогда существует и единственный ненулевой многочлен $e \in K[x]$, $\deg e \leq r + s + 1$, *такой, что* $(Bx^{s+1}h^{r+1}, eB - V)$ — *представление Мамфорда дивизора* $Q + (x)_\circ^- + (h)_\circ^-$, *где приведенный дивизор* Q *определен следующим образом*

$$Q = \iota E - r((x)_\circ^+ - (h)_\circ^-) - s((h)_\circ^+ - (x)_\circ^-). \tag{5.3.1.8}$$

Доказательство. Сначала убедимся, что дивизор Q, определенный в (5.3.1.8), действительно является приведенным. По предложению 5.3.1.2 дивизор E приведенный, следовательно, и ιE — приведенный, причем по лемме 2.4.5.1 имеем

$$v_x^-(\iota E) = 0, \quad v_x^+(\iota E) = r, \quad v_h^-(\iota E) = 0, \quad v_h^+(\iota E) = s.$$

Значит, дивизор Q также приведенный.

В силу предложения 5.3.1.3, остается только доказать, что представление Мамфорда дивизора $Q + (x)_\circ^- + (h)_\circ^-$ действительно имеет вид $(Bx^{s+1}h^{r+1}, eB - V)$ для некоторого ненулевого многочлена $e \in K[x]$.

Для дальнейших вычислений нам удобно будет доказать существование многочлена e конструктивным образом. Необходимо построить такой многочлен e, чтобы были выполнены условия 1 и 2 предложения 5.3.1.2 для пары многочленов Bx^sh^r и $eB - V$ вместо пары многочленов U и V соответственно. Заметим, что условие 2 предложения 5.3.1.2 выполнено автоматически:

$$(B) + s(x) + r(h) = Q + \iota Q - g(\infty^- + \infty^+).$$

Многочлен e будем строить с помощью Китайской теоремы об остатках, исходя из условия

$$Q + (x)_\circ^- + (h)_\circ^- \leq \left(eB - V - \sqrt{f}\right)_{[g+1]}. \tag{5.3.1.9}$$

С помощью разложений в $K((x))$ и $K((h))$ найдем

$$e_x = \left[\frac{\sqrt{f}+V}{Bx^s}\right]_x^-, \quad e_h = \left[\frac{\sqrt{f}+V}{Bh^r}\right]_h^-. \tag{5.3.1.10}$$

Отметим, что $e_x x^s, e_h h^r \in K[x]$, $\deg(e_x x^s) \le s$, $\deg(e_h h^r) \le r$. С помощью алгоритма Евклида найдем $f_x, f_h \in K[x]$ такие, что

$$f_x x^{s+1} \equiv 1 \pmod{h^{r+1}}, \quad \deg f_x \le r,$$
$$f_h h^{r+1} \equiv 1 \pmod{x^{s+1}}, \quad \deg f_h \le s.$$

Покажем, что многочлен e следующего вида

$$e \equiv (e_x x^s) f_h h^{r+1} + (e_h h^r) f_x x^{s+1} \pmod{x^{s+1} h^{r+1}}, \quad \deg e \le s + r + 1 \le g + 1,$$

удовлетворяет условию (5.3.1.9).

Так как

$$e \equiv e_x x^s \pmod{x^{s+1}}, \quad e \equiv e_h h^r \pmod{h^{r+1}},$$

то

$$v_x^-\left(\frac{\sqrt{f}+V}{B} - e\right) \ge s+1, \quad v_h^-\left(\frac{\sqrt{f}+V}{B} - e\right) \ge r+1. \tag{5.3.1.11}$$

По пунктам 3, 5, 6 предложения 5.3.1.2 с учетом того, что $T = Bx^r h^s$, имеем

$$\operatorname{gcdiv}\left(\left(\sqrt{f}+V\right)_{[g+1]}, \ (Bx^r h^s)_{[g]}\right) = \iota E. \tag{5.3.1.12}$$

Из пункта 6 предложения 5.3.1.2 и (5.3.1.7) корректно определен эффективный дивизор $Q_B = \iota E - r\,(x)_\circ^+ - s\,(h)_\circ^+$, причем $(B)_{[g-r-s]} = Q_B + \iota Q_B$. В силу пункта 3 предложения 5.3.1.2 имеем $Q_B \le \iota E \le \left(\sqrt{f}+V\right)_{[g+1]}$, следовательно,

$$Q_B \le \iota E \le \left(\sqrt{f}+V-eB\right)_{[g+1]}. \tag{5.3.1.13}$$

Условия (5.3.1.11), (5.3.1.12) и (5.3.1.13) влекут (5.3.1.9), причем $\deg(eB) \le \deg T + 1 \le g+1$, следовательно, $\deg(eB - V) \le g+1$ и $Q = Q_B + s\,(x)_\circ^- + r\,(h)_\circ^-$. □

5.3.2. Построение непрерывной дроби с помощью представления Мамфорда

Пусть дан элемент $\alpha = (\sqrt{f}+V)/T \in L$, где многочлены $T, V \in K[x]$ удовлетворяют условиям (5.3.1.4) для некоторого $U \in K[x]$ и справедливы условия (5.3.1.6). Покажем, как построить обобщенную непрерывную дробь для элемента α, которая сходится к α сразу по двум линейным нормированиям v_x^- и v_h^-.

Положим $U_{-1} = U$, $V_{-1} = V$, $T_0 = T$.

Теорема 5.3.2.1. *Существуют и единственные последовательности многочленов $U_j, T_j, V_j, e_j \in K[x]$, $j \in \mathbb{N}_0$, $U_j \ne 0$, $T_j \ne 0$, $e_j \ne 0$, и приведенных дивизоров $D_j, E_j \in \operatorname{Div}(L)$, $j \in \mathbb{N}_0$, удо-*

влетворяющих следующим условиям для $j \in \mathbb{N}_0$

$$U_j = T_j x^{s_j - r_j} h^{r_j - s_j}, \quad V_j = e_j T_j x^{-r_j} h^{-s_j} - V_{j-1}, \tag{5.3.2.1}$$

$$f - V_j^2 = U_j x h T_{j+1}, \quad \deg U_j \leq g, \quad \deg T_{j+1} \leq g, \quad \deg V_j \leq g+1, \tag{5.3.2.2}$$

$$(U_{j-1})_{[g]} = D_j + \iota D_j - g(\infty^- + \infty^+), \tag{5.3.2.3}$$

$$(T_j)_{[g]} = E_j + \iota E_j - g(\infty^- + \infty^+), \tag{5.3.2.4}$$

$$D_j = \operatorname{gcdiv}\left(\left(V_{j-1} - \sqrt{f}\right)_{[g+1]}, \ (U_{j-1})_{[g]}\right), \tag{5.3.2.5}$$

$$E_j = \operatorname{gcdiv}\left(\left(V_{j-1} - \sqrt{f}\right)_{[g+1]}, \ (T_j)_{[g]}\right), \tag{5.3.2.6}$$

$$\left(V_{j-1} - \sqrt{f}\right)_{[g+1]} = D_j + (x)_\circ^- + (h)_\circ^- + E_j, \tag{5.3.2.7}$$

$$D_{j+1} = \iota E_j - r_j((x)_\circ^+ - (h)_\circ^-) - s_j((h)_\circ^+ - (x)_\circ^-), \tag{5.3.2.8}$$

где $r_j = v_x(T_j)$, $s_j = v_h(T_j)$.

Доказательство. По условиям (5.3.1.4) имеем (5.3.2.2) при $j = -1$. Доказательство будем проводить конструктивным образом последовательно для каждого $j \in \mathbb{N}_0$.

Пусть $j = 0$. Определим дивизор D_j как в (5.3.1.5) с помощью (5.3.2.5). Тогда справедливо условие (5.3.2.3) и D_j — приведенный дивизор, причем $v_x^+(D_j) = v_h^+(D_j) = 0$ и $(U_{j-1}xh, V_{j-1})$ — представление Мамфорда дивизора $D_j + (x)_\circ^- + (h)_\circ^-$. По предложению 5.3.1.2 единственным образом определен приведенный дивизор E_j такой, что набор $(T_j xh, V_{j-1})$ является представлением Мамфорда дивизора $E_j + (x)_\circ^- + (h)_\circ^-$, а кроме того выполнены условия (5.3.2.4), (5.3.2.6) и (5.3.2.7). По предложению 5.3.1.4 может быть единственным образом определен многочлен $e_j \in K[x]$ такой, что набор $(U_j xh, V_j)$ является представлением Мамфорда дивизора D_{j+1}, где многочлены $U_j, V_j \in K[x]$ определены в (5.3.2.1), а дивизор D_{j+1} определен в (5.3.2.8).

Положим $j = 1$. Тогда дивизор D_j удовлетворяет (5.3.2.5) и выполнено условие (5.3.2.3). По предложению 5.3.1.2 единственным образом определен многочлен $T_j \in K[x]$, удовлетворяющий (5.3.2.2).

Приведенные рассуждения могут быть проведены по индукции для каждого $j \in \mathbb{N}_0$, причем каждое построение проводится единственным образом. Более того, имея построения при некотором $j = n > 0$, можем единственным образом вернуться с помощью условий (5.3.2.1)-(5.3.2.8) к данным многочленам $U_{-1} = U$, $V_{-1} = V$, $T_0 = T$. Это нам гарантирует единственность искомых последовательностей многочленов $U_j, T_j, V_j, e_j \in K[x]$, $j \in \mathbb{N}_0$, и приведенных дивизоров $D_j, E_j \in \operatorname{Div}(L)$, $j \in \mathbb{N}_0$. □

Следствие 5.3.2.2. *Пусть последовательности многочленов* $U_j, T_j, V_j, e_j \in K[x]$, $j \in \mathbb{N}_0$, *и приведенных дивизоров* $D_j, E_j \in \operatorname{Div}(L)$, $j \in \mathbb{N}_0$, *определены условиями теоремы 5.3.2.1.*

Положим $\alpha_j = (\sqrt{f} + V_{j-1})/T_j \in L$, $a_j = e_j x^{-r_j} h^{-s_j}$, $j \in \mathbb{N}_0$. *Тогда* $\alpha_0 = \alpha$ *и справедливы следующие утверждения*

- $(U_{j-1}xh, V_{j-1})$ — *представление Мамфорда дивизора* $D_j + (x)_\circ^- + (h)_\circ^-$;
- $(T_j xh, V_{j-1})$ — *представление Мамфорда дивизора* $E_j + (x)_\circ^- + (h)_\circ^-$;
- $(x/h)^{r_j - s_j}(\alpha_j - a_j) = xh/\alpha_{j+1}$.

Доказательство. Первые два утверждения сразу следуют из теоремы 5.3.2.1. Для доказательства третьего утверждения запишем

$$\alpha_j - a_j = \frac{\sqrt{f} + V_{j-1} - e_j T_j x^{-r_j} h^{-s_j}}{T_j} = \frac{\sqrt{f} - V_j}{T_j} = \frac{\sqrt{f} - V_j}{U_j x^{r_j - s_j} h^{s_j - r_j}} =$$
$$= \frac{U_j xh T_{j+1} x^{s_j - r_j} h^{r_j - s_j}}{U_j(\sqrt{f} + V_j)} = \frac{x^{1+s_j-r_j} h^{1+r_j-s_j}}{\alpha_{j+1}}.$$

Следствие 5.3.2.2 доказано. □

С помощью предложения 5.3.1.4 может быть единственным образом построен многочлен $e_j \in K[x]$. Его построение зависит только от многочленов T_j и V_{j-1}, поскольку величины r_j, s_j и приведенные дивизоры E_j, D_{j+1} мгновенно восстанавливаются по многочленам T_j и V_{j-1}. Таким образом, многочлен e_j, а следовательно, и *неполное частное* a_j есть функция от элемента α_j. Поэтому корректно ввести обозначение $a_j = [\alpha_j]_{x,h}^-$, причем по теореме 5.3.2.1 и следствию 5.3.2.2 выполнены соотношения

$$v_x^-(\alpha_j - a_j) > 0, \quad v_h^-(\alpha_j - a_j) > 0, \quad v_x(a_{j+1}) = -r_{j+1} \le 0, \quad v_h(a_{j+1}) = -s_{j+1} \le 0. \quad (5.3.2.9)$$

Пусть теперь дан приведенный дивизор $D_0 \in \mathrm{Div}(L)$ такой, что $v_x^+(D_0) = v_h^+(D_0) = 0$. По предложению 5.3.1.2 корректно определены многочлены $U_{-1}, V_{-1} \in K[x]$ такие, что $(U_{-1}xh, V_{-1})$ — представление Мамфорда дивизора $D_0 + (x)_\circ^- + (h)_\circ^-$. Многочлены U_{-1}, V_{-1} определены единственным образом с точностью до умножения многочлена U_{-1} на постоянную из K^*. Справедливы условия (5.3.2.2) при $j = -1$ для некоторого многочлена $T_0 \in K[x]$. Следовательно, единственным образом определены последовательности многочленов $U_j, T_j, V_j, e_j \in K[x]$, $j \in \mathbb{N}_0$, $U_j \neq 0$, $T_j \neq 0$, $e_j \neq 0$, и приведенных дивизоров $D_j, E_j \in \mathrm{Div}(L)$, $j \in \mathbb{N}_0$, удовлетворяющих условиям (5.3.2.1)-(5.3.2.8) для $j \in \mathbb{N}_0$.

Таким образом, понятие *непрерывной дроби* может быть идентифицировано с каждой из трех связанных друг с другом последовательностей:

- последовательность пар многочленов U_j, V_j, удовлетворяющих (5.3.2.2) и (5.3.2.1) для некоторых многочленов e_j, T_j, однозначно восстанавливающихся по паре U_j, V_j;
- последовательность приведенных дивизоров D_j, удовлетворяющих (5.3.2.7)-(5.3.2.8) для некоторого многочлена V_{j-1} и приведенного дивизора E_j такого, что $v_x^-(E_j) = r_j$, $v_h^-(E_j) = s_j$;

- последовательность *полных частных* α_j, удовлетворяющих условиям

$$a_j = [\alpha_j]^-_{x,h}\,,\ r_j = -v^-_x(\alpha_j)\,,\ s_j = -v^-_h(\alpha_j)\,,\ \left(\frac{x}{h}\right)^{r_j-s_j}(\alpha_j - a_j) = \frac{xh}{\alpha_{j+1}}. \tag{5.3.2.10}$$

В итоге получаем *обобщенную непрерывную дробь*

$$\alpha_0 = a_0 + \cfrac{x^{1+s_0-r_0}h^{1+r_0-s_0}}{a_1 + \cfrac{x^{1+s_1-r_1}h^{1+r_1-s_1}}{a_2 + \cdots}}, \tag{5.3.2.11}$$

полные и неполные частные которой удовлетворяют соотношениям (5.3.2.10) для $j \in \mathbb{N}_0$. Мы будем рассматривать только такие обобщенные непрерывные дроби, поэтому далее для краткости будем называть выражение (5.3.2.11) непрерывной дробью и использовать для нее обозначение (см. §5.1.1)

$$[a_0; x^{1+s_0-r_0}h^{1+r_0-s_0} \mid a_1, x^{1+s_1-r_1}h^{1+r_1-s_1} \mid a_2, \ldots].$$

Теорема 5.3.2.3. *Пусть $D_0 \in \mathrm{Div}(L)$ — такой приведенный дивизор, что $v^+_x(D_0) = v^+_h(D_0) = 0$. Пусть $(U_{-1}xh, V_{-1})$ — представление Мамфорда дивизора $D_0 + (x)^-_\circ + (h)^-_\circ$. Пусть D_j — последовательность приведенных дивизоров, построенная в теореме 5.3.2.1. Тогда при $n \in \mathbb{N}$ справедливы соотношения*

$$E_0 - E_n \sim D_n - D_0 \sim \sum_{j=0}^{n-1}(1 + r_j + s_j)\big((x)^-_\circ - (h)^+_\circ\big). \tag{5.3.2.12}$$

Доказательство. Сначала заметим, что из (5.3.2.7) следуют соотношения

$$D_n + (x)^-_\circ + (h)^-_\circ + E_n \sim (g+1)(\infty^- + \infty^+),$$
$$D_0 + (x)^-_\circ + (h)^-_\circ + E_0 \sim (g+1)(\infty^- + \infty^+).$$

Вычитая их, получим $E_0 - E_n \sim D_n - D_0$.

Просуммируем (5.3.2.7) по $j = 0, \ldots, n-1$, и подставим выражения (5.3.2.8), получим

$$\sum_{j=0}^{n-1}\left(V_{j-1} - \sqrt{f}\right)_{[g+1]} = \sum_{j=0}^{n-1}\big(D_j + (x)^-_\circ + (h)^-_\circ\big) +$$
$$+ \sum_{j=0}^{n-1}\big(\iota D_{j+1} + r_j((x)^-_\circ - (h)^+_\circ) + s_j((h)^-_\circ - (x)^+_\circ)\big).$$

Преобразуем это выражение

$$\sum_{j=0}^{n-1}\left(V_{j-1} - \sqrt{f}\right) + n(g+1)(\infty^- + \infty^+) = D_0 - D_n + \sum_{j=0}^{n-1}\big(D_{j+1} + \iota D_{j+1}\big) +$$
$$+ \sum_{j=0}^{n-1}(1 + r_j + s_j)\big((x)^-_\circ + (h)^-_\circ\big) - \sum_{j=0}^{n-1}\big(r_j((h)^-_\circ + (h)^+_\circ) + s_j((x)^-_\circ + (x)^+_\circ)\big),$$

или

$$\sum_{j=0}^{n-1}\left(V_{j-1}-\sqrt{f}\right)=D_0-D_n+\sum_{j=0}^{n-1}(U_j)+$$
$$+\sum_{j=0}^{n-1}(1+r_j+s_j)\big((x)_\circ^-+(h)_\circ^--\infty^--\infty^+\big)-\sum_{j=0}^{n-1}\big(r_j\,(h)+s_j\,(x)\big),\qquad(5.3.2.13)$$

откуда и следует 5.3.2.12. □

5.3.3. Непрерывные дроби, построенные по двум линейным нормированиям

Пусть свободный от квадратов многочлен $f\in K[x]$, такой, что нормирования v_x и v_h поля $K(x)$ имеют по два неэквивалентных продолжения $v_x^-\neq v_x^+$ и $v_h^-\neq v_h^+$ на поле $L=K(x)(\sqrt{f})$.

Пусть для элемента $\alpha\in L$ построена непрерывная дробь вида (5.3.2.11) с помощью соотношений (5.3.2.10). Тогда в обозначениях §5.1.1 имеем $\mathcal{K}=K(x)$, $b_{j+1}=x^{1+s_j-r_j}h^{1+r_j-s_j}$, $j\in\mathbb{N}_0$.

Отметим, что вообще говоря, значения b_j можно определять иным образом, сохраняя построение обобщенной непрерывной дроби по формулам (5.3.2.10). Но мы хотим, чтобы построенная обобщенная непрерывная дробь обладала некоторыми свойствами, которые также выполняются для числовых непрерывных дробей или для функциональных непрерывных дробей. Например, мы ожидаем, что обобщенная непрерывная дробь существует для любого элемента рассматриваемого поля L, и обобщенная непрерывная дробь элемента $\alpha\in K(x)$ конечна. Оказывается, эти свойства далеко не всегда выполнены в зависимости от выбора значений b_j.

Пример 5.3.3.1. *Рассмотрим $b_j=x^2h^2$, $j\in\mathbb{N}$, и $\alpha=xh$. Тогда по формулам (5.1.1.2) имеем $a_j=0$, $\alpha_{j+1}=xh$ для всех $j\in\mathbb{N}_0$,*

$$\alpha=[0;x^2h^2\mid 0,x^2h^2\mid 0,\dots,x^2h^2\mid\alpha_n],\quad \alpha_n=xh.$$

Пример 5.3.3.1, в частности, показывает важность условий (5.3.2.9).

Предложение 5.3.3.2. *Пусть $[a_0;b_1|a_1,b_2|a_2,\dots]$ — непрерывная дробь вида (5.1.1.1) для элемента $\alpha\in L$, для которой справедливы соотношения (5.1.1.2) и (5.3.2.9). Тогда при $n\in\mathbb{N}$*

имеем

$$v_x(q_n) = \sum_{j=1}^{n} v_x(a_j) = -\sum_{j=1}^{n} r_j, \quad v_x(q_{n+1}) \le v_x(q_n) \le 0, \tag{5.3.3.1}$$

$$v_h(q_n) = \sum_{j=1}^{n} v_h(a_j) = -\sum_{j=1}^{n} s_j, \quad v_h(q_{n+1}) \le v_h(q_n) \le 0, \tag{5.3.3.2}$$

$$v_x(p_n) = \sum_{j=0}^{n} v_x(a_j) = -\sum_{j=0}^{n} r_j, \quad v_x(p_{n+1}) \le v_x(p_n) \le 0, \tag{5.3.3.3}$$

$$v_h(p_n) = \sum_{j=0}^{n} v_h(a_j) = -\sum_{j=0}^{n} s_j, \quad v_h(p_{n+1}) \le v_h(p_n) \le 0, \tag{5.3.3.4}$$

откуда, в частности, следует, что $q_j \neq 0$ *при* $j \in \mathbb{N}_0$.

Доказательство. В силу аналогичности, приведем только доказательство первого тождества (5.3.3.1). В силу (5.3.2.9) справедливо $a_j \neq 0$, $v_x^-(\alpha_j) = v_x(a_j)$ и $v_x^-(\alpha_j - a_j) > 0$ при $j \in \mathbb{N}$. Из (5.1.1.2) получаем

$$v_x(b_{j+1}) = v_x(a_{j+1}) + v_x^-(\alpha_j - a_j) > v_x(a_{j+1}). \tag{5.3.3.5}$$

Следовательно, по индукции

$$v_x(q_{n+1}) = v_x(a_{n+1}q_n + b_{n+1}q_{n-1}) = v_x(a_{n+1}q_n) = \sum_{j=1}^{n+1} v_x(a_j), \tag{5.3.3.6}$$

причем $v_x(q_{n+1}) \le v_x(q_n)$. □

Ясно, что при $\alpha \in L \setminus K(x)$ непрерывная дробь, построенная по формулам (5.1.1.2), будет бесконечной. Покажем, что при выполнении условий (5.3.2.9) для $j \in \mathbb{N}$, бесконечная непрерывная дробь сходится к элементу α как по нормированию v_x^-, так и по нормированию v_h^-.

Предложение 5.3.3.3. *Пусть* $[a_0; b_1|a_1, b_2|a_2, \ldots]$ *— бесконечная непрерывная дробь вида* (5.1.1.1) *для элемента* $\alpha \in L$, *для которой справедливы соотношения* (5.3.2.9) *и* (5.1.1.2). *Тогда*

$$\lim_{n\to\infty} v_x^-\left(\alpha - \frac{p_n}{q_n}\right) = +\infty, \quad \lim_{n\to\infty} v_h^-\left(\alpha - \frac{p_n}{q_n}\right) = +\infty.$$

Доказательство. В силу аналогичности, доказательство можно провести только для одного нормирования v_x^-. По формулам (5.1.1.8), (5.3.3.1) и (5.3.3.5) получаем

$$v_x^-\left(\alpha - \frac{p_n}{q_n}\right) = \sum_{j=1}^{n+1} v_h(b_j) - v_x(q_n) - v_x^-(\alpha_{n+1}q_n + b_{n+1}q_{n-1}) =$$

$$= \sum_{j=1}^{n+1} v_x(b_j) - v_x(q_n) - v_x(q_{n+1}) = \sum_{j=0}^{n} v_x^-(\alpha_j - a_j) - \sum_{j=1}^{n} v_x(a_j).$$

Последнее выражение стремится к бесконечности при n стремящемся к бесконечности, так как $v_x^-(\alpha_j - a_j) > 0$ и $v_x(a_j) \le 0$. □

Пример 5.3.3.4. *Рассмотрим* $b_j = xh(1+xh)$, $j \in \mathbb{N}$, *и* $\alpha = 1 + xh$. *Тогда по формулам* (5.1.1.2) *имеем* $a_j = 1$, $\alpha_{j+1} = 1 + xh$ *для всех* $j \in \mathbb{N}_0$. *По индукции легко установить, что* $v_x^-(\alpha - p_n/q_n) = v_h^-(\alpha - p_n/q_n) = n+1$ *для любого* $n \in \mathbb{N}_0$.

Пример 5.3.3.4 показывает, что условий (5.3.2.9) не достаточно, чтобы непрерывная дробь вида (5.1.1.1) для элемента $\alpha \in K(x)$, удовлетворяющая соотношениям (5.1.1.2), была конечна.

Покажем, как для элемента $\alpha \in L$ строится непрерывная дробь вида (5.3.2.11) — обобщенная непрерывная дробь, удовлетворяющая (5.3.2.9) и (5.1.1.2) с $b_{j+1} = x^{1+s_j-r_j}h^{1+r_j-s_j}$.

Основная задача состоит в конструктивном построении величины $a = [\alpha]_{x,h}^-$. В следующем предложении приведено конструктивное построение $a = [\alpha]_{x,h}^-$, тем самым, для квадратичных иррациональностей дано конструктивное построение непрерывной дроби вида (5.3.2.11).

Предложение 5.3.3.5. *Пусть дан элемент* $\alpha \in L$ *такой, что* $r = -v_x^-(\alpha) \ge -1$, $s = -v_h^-(\alpha) \ge -1$. *Тогда*

1. существует единственный многочлен $e \in K[x]$, $\deg e \le r+s+1$ *такой, что для* $a = ex^{-r}h^{-s}$ *справедливы условия*

$$v_x^-(\alpha - a) > s - r, \qquad v_h^-(\alpha - a) > r - s; \tag{5.3.3.7}$$

2. для элемента $\beta = (\alpha - a)^{-1}x^{r-s-1}h^{s-r-1}$ *справедливы неравенства* $v_x^-(\beta) \le 0$ *и* $v_h^-(\beta) \le 0$.

Доказательство. Сначала отметим, что для $r = s = -1$ мы определяем $e = 0$. Далее считаем, что $r + s + 1 \ge 0$.

С помощью разложений элемента α в $K((x))$ и $K((h))$ найдем

$$a_x = \left[\alpha \cdot x^{r-s}h^s\right]_x^-, \quad a_h = \left[\alpha \cdot h^{s-r}x^r\right]_h^-. \tag{5.3.3.8}$$

Отметим, что $a_x = e_x x^{-s}$, $a_h = e_h h^{-r}$, где $e_x, e_h \in K[x]$, $\deg(e_x) \le s$, $\deg(e_h) \le r$. С помощью алгоритма Евклида найдем $f_x, f_h \in K[x]$ такие, что

$$f_x x^{s+1} \equiv 1 \pmod{h^{r+1}}, \quad \deg f_x \le r,$$
$$f_h h^{r+1} \equiv 1 \pmod{x^{s+1}}, \quad \deg f_h \le s.$$

Покажем, что для многочлена e следующего вида

$$e \equiv e_x f_h h^{r+1} + e_h f_x x^{s+1} \pmod{x^{s+1}h^{r+1}}, \quad \deg e \le s + r + 1,$$

справедливы условия (5.3.3.7).

Действительно, так как

$$e \equiv e_x \pmod{x^{s+1}}, \quad e \equiv e_h \pmod{h^{r+1}}, \tag{5.3.3.9}$$

то

$$v_x^-(\alpha x^r h^s - e) \geq s+1, \quad v_h^-(\alpha x^r h^s - e) \geq r+1. \tag{5.3.3.10}$$

Теперь докажем единственность. Пусть существует еще один многочлен $e_0 \in K[x]$, для которого выполнены условия (5.3.3.7). Тогда для e_0 должны быть выполнены условия (5.3.3.10) и (5.3.3.9), откуда по Китайской теореме об остатках следует, что $e_0 \equiv e \pmod{x^{s+1}h^{r+1}}$.

Условия пункта 2. сразу следуют из пункта 1. □

Обозначим $L_{xh} = \{\alpha \in L : \ v_x^-(\alpha) \leq 1, \ v_h^-(\alpha) \leq 1\}$. Тогда с помощью предложения 5.3.3.5 для любого элемента $\alpha \in L_{xh}$ корректно определена величина $a = [\alpha]_{x,h}^-$, причем $\beta = (\alpha - a)^{-1}x^{r-s-1}h^{s-r-1} \in L_{xh}$. Следовательно, для любого элемента $\alpha_0 = \alpha \in L_{xh}$ существует единственная непрерывная дробь вида (5.3.2.11) — обобщенная непрерывная дробь, удовлетворяющая (5.1.1.2) с $b_{j+1} = x^{1+s_j-r_j}h^{1+r_j-s_j}$, причем $a_j \neq 0$ при $j \in \mathbb{N}$. По предложению 5.3.3.3 непрерывная дробь элемента $\alpha \in L_{xh}$, $\alpha \notin K(x)$, сходится к элементу α как по нормированию v_x^-, так и по нормированию v_h^-.

Предложение 5.3.3.6. *1. Обобщенная непрерывная дробь вида* (5.3.2.11) *элемента* $\alpha \in L$ *конечна тогда и только тогда, когда* $\alpha \in K(x)$.

2. Пусть $\alpha = \phi/\psi \in K(x)$ *— несократимая дробь, тогда найдется такой номер* $n \in \mathbb{N}$, $n \leq \max(\deg\psi, \ \deg\phi - 1)$, *что обобщенная непрерывная дробь вида* (5.3.2.11) *для элемента* $\alpha = \phi/\psi$ *имеет вид* $\phi/\psi = [a_0; a_1, a_2, \ldots, a_n] = p_n/q_n$.

Доказательство. Ясно, что конечная непрерывная дробь вида (5.3.2.11) равна некоторому $\alpha_0 \in K(x)$, причем в силу однозначности построения непрерывной дроби имеем $\alpha = \alpha_0$.

Предположим, что $\alpha = \phi/\psi \in K(x)$ — несократимая дробь. Пусть $\phi_0 = \phi$, $\psi_0 = \psi$, $\alpha_0 = \phi_0/\psi_0$. По построению (5.3.2.10) непрерывной дроби вида (5.3.2.11) для элемента α определены полные частные $\alpha_j = \phi_j/\psi_j$ и неполные частные $a_j = e_j x^{-r_j}h^{-s_j}$, где $e_j \in K[x]$ определен как в предложении 5.3.3.5, $v_x(\phi_j) = v_h(\phi_j) = 0$, $v_x(\psi_j) = r_j \geq 0$, $v_h(\psi_j) = s_j \geq 0$, $j = 1, 2, \ldots$. Положим $\xi_j = \psi_j x^{-r_j}h^{-s_j} \in K[x]$, $b_{j+1} = x^{1+s_j-r_j}h^{1+r_j-s_j}$, тогда

$$\alpha_j - a_j = \frac{\phi_j - e_j\xi_j}{\psi_j} = \frac{b_{j+1}}{\alpha_{j+1}} = \frac{b_{j+1}\psi_{j+1}}{\phi_{j+1}},$$

причем многочлен $e_j \in K[x]$, $\deg e_j \leq r_j + s_j + 1$, может быть однозначно определен из сравнения

$$e_j\xi_j \equiv \phi_j \pmod{x^{s_j+1}h^{r_j+1}}.$$

Тогда

$$\psi_{j+1} = \frac{\phi_j - e_j\xi_j}{x^{s_j+1}h^{r_j+1}} \in K[x], \quad \phi_{j+1} = \xi_j \in K[x],$$

поскольку $\big((\phi_j - e_j\xi_j)x^{-s_j-1}h^{-r_j-1}, \xi_j\big) \in K^*$.

Имеем

$$\deg\phi_{j+1} = \deg\xi_j = \deg\psi_j - r_j - s_j,$$
$$\deg\psi_{j+1} \le \max\big(\deg\phi_j - r_j - s_j - 2,\ \deg\psi_j - r_j - s_j - 1\big) =$$
$$= \max\big(\deg\psi_{j-1} - r_{j-1} - s_{j-1} - r_j - s_j - 2,\ \deg\psi_j - r_j - s_j - 1\big).$$

Продолжая так и далее, получаем, что для всех $n = 1, 2, \dots, j$ выполнены неравенства

$$\deg\psi_n \le \max\big(\deg\psi_0,\ \deg\phi_0 - 1\big) - \sum_{j=0}^{n-1}(r_j + s_j + 1).$$

Отсюда заключаем, что на некотором номере $n \le \max(\deg\psi_0,\ \deg\phi_0 - 1)$ процесс построения непрерывной дроби завершится, причем $\phi_n = a_n\psi_n$. □

Приведем пример функции $\alpha \in K(x)$, для которой неравенство в пункте 2 предложения 5.3.3.6 превращается в равенство.

Пример 5.3.3.7. *Пусть $a_0, a_1 \in K[x]$, линейные многочлены взаимно простые с x и h. Положим*

$$\alpha = \frac{a_0a_1 + xh}{a_1} = a_0 + \frac{xh}{a_1}, \quad r_0 = s_0 = 0.$$

Тогда $\phi = \phi_0 = a_0a_1 + xh$, $\psi = \psi_0 = a_1 = \phi_1$, $\psi_1 = 1$, причем $n = 1 = \max(\deg\psi,\ \deg\phi - 1)$.

Следующее предложение описывает необходимые нам свойства подходящих дробей p_n/q_n непрерывной дроби вида (5.3.2.11).

Предложение 5.3.3.8. *Пусть для элемента $\alpha \in L_{xh}$ построена непрерывная дробь вида (5.3.2.11). Обозначим*

$$Q_n = \prod_{j=0}^{n} x^{r_j + r_{j+1}} h^{s_j + s_{j+1}}.$$

Тогда для $n \in \mathbb{N}_0$ справедливы следующие утверждения:

1. *многочлены $p_nq_{n+1}Q_n, p_{n+1}q_nQ_n \in K[x]$ взаимно просты;*

2. *$v_\infty(p_n) \ge -(n+1)$, $v_\infty(q_n) \ge -n$, $\max\big(-v_\infty(p_nq_{n+1}),\ -v_\infty(p_{n+1}q_n)\big) = 2(n+1)$.*

Доказательство. Утверждения следуют из предложения 5.3.3.2 и соотношения (5.1.1.5) при $b_{j+1} = x^{1+s_j-r_j}h^{1+r_j-s_j}$. □

Предложение 5.3.3.9. *При $j \ge -1$ величины A_j и B_j, определенные в (5.1.1.11), являются многочленами, т. е. $A_j, B_j \in K[x]$.*

Доказательство. Без ограничения общности мы можем предполагать, что

$$\alpha = \frac{-\lambda_1 + \sqrt{d}}{\lambda_2}, \quad d = \lambda_1^2 - \lambda_0\lambda_2, \quad \lambda_0, \lambda_1, \lambda_2 \in K[x]. \tag{5.3.3.11}$$

Оценки нормирований v_x^- и v_h^- различных величин далее проводятся аналогично, поэтому рассматриваем только нормирование v_h^-.

По определению $A_{-1} = \lambda_2$, $B_{-1} = 0$, поэтому $A_{-1}, B_{-1} \in K[x]$.

При $j = 0$ по построению

$$r_0 - s_0 < v_h^- (\alpha_0 - a_0) = v_h^- (q_0\alpha - p_0) = v_h^- \left(\frac{\sqrt{d} - (\lambda_1 + a_0\lambda_2)}{\lambda_2} \right),$$

откуда, учитывая (5.1.1.13), имеем

$$0 \leq v_h \left(\frac{d - (\lambda_1 + a_0\lambda_2)^2}{h^{1+r_0-s_0}\lambda_2} \right) = v_h (A_0).$$

Из равенства $\alpha(\lambda_2\alpha + 2\lambda_1) = -\lambda_0$ следует, что $v_h (\lambda_2\alpha) \geq 0$, поэтому $v_h (a_0) + v_h (\lambda_2) \geq 0$, значит $v_h (B_0) \geq 0$.

Пусть теперь $j \geq 1$. По формулам (5.1.1.3) и (5.1.1.11)-(5.1.1.12) $A_j, B_j \in K(x)$ — рациональные функции, причем их знаменатели могут иметь только вид $cx^n h^m$ для некоторых $n, m \in \mathbb{N}_0$, $c \in K^*$. Чтобы показать, что A_j, B_j многочлены, достаточно доказать неравенства $v_x (A_j) \geq 0$, $v_x (B_j) \geq 0$, $v_h (A_j) \geq 0$, $v_h (B_j) \geq 0$.

Положим

$$H(X, Y) = \lambda_2 X^2 + 2\lambda_1 XY + \lambda_0 Y^2, \tag{5.3.3.12}$$

тогда

$$H(X, Y) = Y^2 \cdot H(X/Y) = \lambda_2 (X - \alpha Y)(X - \overline{\alpha} Y).$$

Из (5.1.1.9) получаем

$$v_h^- (q_j\alpha - p_j) = -v_h (a_{j+1}) - v_h (q_j) + \sum_{i=1}^{j+1} v_h (b_i), \tag{5.3.3.13}$$

следовательно,

$$\begin{aligned} v_h (A_j) &= v_h^- (\lambda_2 (p_j - \alpha q_j)(p_j - \overline{\alpha} q_j)) - \sum_{i=1}^{j+1} v_h (b_i) = \\ &= v_h (\lambda_2) - v_h (a_{j+1}) + v_h^- \left(\frac{p_j}{q_j} - \overline{\alpha} \right). \end{aligned} \tag{5.3.3.14}$$

Если $v_h^- \left(\sqrt{d}/\lambda_2 \right) \leq 0$, то в силу предложения 5.3.3.3 имеем

$$v_h^- \left(\frac{p_j}{q_j} - \alpha \right) \geq 0 \geq v_h^- (\alpha - \overline{\alpha}) = v_h^- \left(\frac{2\sqrt{d}}{\lambda_2} \right) = \frac{1}{2} v_h (d) - v_h (\lambda_2).$$

Тогда

$$v_h^-\left(\frac{p_j}{q_j}-\overline{\alpha}\right)=v_h^-\left(\frac{p_j}{q_j}-\alpha+\alpha-\overline{\alpha}\right)=v_h^-\left(\alpha-\overline{\alpha}\right).$$

Таким образом, из (5.3.3.14) имеем $v_h\left(A_j\right)=\frac{1}{2}v_h\left(d\right)-v_h\left(a_{j+1}\right)\geq 0$.

Если $v_h^-\left(\sqrt{d}/\lambda_2\right)>0$, то, учитывая, что по построению

$$0\leq\sum_{i=1}^{j+1}v_h\left(b_i\right)-v_h\left(q_j\right)-v_h\left(q_{j+1}\right)=v_h^-\left(\frac{p_j}{q_j}-\alpha\right)=v_h^-\left(\frac{p_j}{q_j}+\frac{\lambda_1}{\lambda_2}-\frac{\sqrt{d}}{\lambda_2}\right),$$

имеем $v_h^-\left(\frac{p_j}{q_j}+\frac{\lambda_1}{\lambda_2}\right)>0$. Тогда

$$v_h^-\left(\frac{p_j}{q_j}-\overline{\alpha}\right)\geq\min\left(v_h\left(\frac{p_j}{q_j}+\frac{\lambda_1}{\lambda_2}\right),\ v_h^-\left(\frac{\sqrt{d}}{\lambda_2}\right)\right)>0.$$

Снова, из (5.3.3.14) имеем $v_h\left(A_j\right)>v_h^-\left(\lambda_2\right)-v_h\left(a_{j+1}\right)\geq 0$. Более того, можем записать

$$v_h^-\left(\frac{p_j}{q_j}-\overline{\alpha}\right)=v_h^-\left(\frac{p_j}{q_j}-\alpha+\alpha-\overline{\alpha}\right)\geq$$
$$\geq\min\left(\sum_{i=1}^{j+1}v_h\left(b_i\right)-v_h\left(q_j\right)-v_h\left(q_{j+1}\right),\ v_h^-\left(\frac{2\sqrt{d}}{\lambda_2}\right)\right),$$

причем в последнем выражении будет равенство, если $\sum_{i=1}^{j+1}v_h\left(b_i\right)-v_h\left(q_j\right)-v_h\left(q_{j+1}\right)\neq v_h^-\left(\sqrt{d}/\lambda_2\right)$, то есть

$$v_h\left(A_j\right)=\min\left\{\frac{1}{2}v_h\left(d\right)-v_h\left(a_{j+1}\right),\ v_h\left(\lambda_2\right)+\sum_{i=1}^{j+1}v_h\left(b_i\right)-2\sum_{i=1}^{j+1}v_h\left(a_i\right)\right\}. \tag{5.3.3.15}$$

Найдем нижнюю оценку для $v_h\left(B_j\right)$. Из (5.1.1.14) получаем $B_j=A_j\alpha_{j+1}-\lambda_2\alpha$. Мы уже видели, что $v_h\left(\lambda_2\alpha\right)\geq 0$. Из оценок нормирования $v_h^-\left(A_j\right)$ имеем $v_h^-\left(A_j\alpha_{j+1}\right)=v_h\left(A_ja_{j+1}\right)\geq 0$. Значит, $v_h\left(B_j\right)\geq\min\{v_h^-\left(A_j\alpha_{j+1}\right),\ v_h^-\left(\lambda_2\alpha\right)\}\geq 0$. □

Предложение 5.3.3.10. *Начиная с некоторого номера $j\geq n_0$ справедливы соотношения*

$$v_h\left(A_j\right)=\frac{1}{2}v_h\left(d\right)-v_h\left(a_{j+1}\right),\quad v_h\left(B_j\right)\geq\frac{1}{2}v_h\left(d\right). \tag{5.3.3.16}$$

Если выполнены условия

$$0=v_h\left(\lambda_0\right)<v_h\left(\lambda_2\right)<v_h\left(\lambda_1\right), \tag{5.3.3.17}$$

то соотношения (5.3.3.16) справедливы для всех $j\geq 0$.

Доказательство. Если выполнены условия (5.3.3.17), то $v_h^-\left(\sqrt{d}/\lambda_2\right)=-v_h\left(\lambda_2\right)/2<0$, откуда с помощью (5.3.3.15) следуют соотношения (5.3.3.16). □

Предложение 5.3.3.11. *При $n\geq -1$ степени многочленов A_n и B_n ограничены,*

$$\deg A_n\leq\max\bigl(\deg\lambda_2,\ \deg\lambda_1-1,\ \deg\lambda_0-2\bigr),$$
$$\deg B_n\leq\bigl(\deg\lambda_2+1,\ \deg\lambda_1,\ \deg\lambda_0-1\bigr).$$

Доказательство. По предложению 5.3.3.9 A_j и B_j действительно многочлены. Так как $v_\infty(b_{j+1}) = v_\infty(x^{1+s_j-r_j}h^{1+r_j-s_j}) = -2$, то по формулам (5.1.1.11)-(5.1.1.12) с учетом предложения 5.3.3.8 имеем

$$\deg A_n = -v_\infty(A_n) \le \big(\deg\lambda_2 + 2n + 2,\ \deg\lambda_1 + 2n + 1,\ \deg\lambda_0 + 2n\big) - 2(n+1),$$
$$\deg B_n = -v_\infty(B_n) \le \big(\deg\lambda_2 + 2n + 1,\ \deg\lambda_1 + 2n,\ \deg\lambda_0 + 2n - 1\big) - 2n,$$

откуда и следует ограниченность степеней многочленов A_j и B_j. □

Теорема 5.3.3.12. *Пусть $K = \mathbb{F}_q$ — поле из q элементов. Тогда обобщенная непрерывная дробь вида (5.3.2.11), для которой справедливы соотношения (5.1.1.2) и (5.3.2.9), $b_{j+1} = x^{1+s_j-r_j}h^{1+r_j-s_j}$, периодическая.*

Доказательство. Доказательство очевидно следует из первого тождества предложения 5.3.3.6 и предложений 5.3.3.9 и 5.3.3.11. □

Предложение 5.3.3.13. *Пусть для элемента $\alpha = \sqrt{f}/h^s \in L$, $s \in \mathbb{N}_0$, где $\alpha_0 = \alpha$, $s_{-1} = s$, $r_{-1} = 0$, $b_{j+2} = x^{1+s_j-r_j}h^{1+r_j-s_j}$ для $j \ge -1$, построена непрерывная дробь вида (5.1.1.1), для которой справедливы соотношения (5.1.1.2) и (5.3.2.9). Тогда*

- *определенные в (5.1.1.11)-(5.1.1.12) величины A_j и B_j имеют вид*
$$A_j = \big(h^{2s}p_j^2 - fq_j^2\big)\cdot\prod_{i=1}^{j+1}(-b_i)^{-1}, \quad B_j = \big(h^{2s}p_jp_{j-1} - fq_{j-1}q_j\big)\cdot\prod_{i=1}^{j}(-b_i)^{-1}; \tag{5.3.3.18}$$
- *для $j \in \mathbb{N}_0$ имеем $A_j, B_j \in K[x]$, $v_x(A_j) = r_j$, $v_x(B_j) \ge 0$, $v_h(A_j) = s + s_j$, $v_h(B_j) \ge s$, и справедливы тождества*
$$\alpha_{j+1} = \frac{B_j + h^s\sqrt{f}}{A_j}, \quad B_{j+1} + B_j = a_{j+1}A_j, \quad h^{2s}f - B_{j+1}^2 = A_j\cdot b_{j+1}\cdot A_{j+1}; \tag{5.3.3.19}$$
- *если для $j \ge 0$ положить*
$$T_j = A_jh^{-s}, \quad V_{j-1} = B_jh^{-s}, \quad U_{j-1} = A_{j-1}b_jx^{-1}h^{-s-1}, \quad e_j = a_{j+1}x^{r_j}h^{s_j}, \tag{5.3.3.20}$$
то $U_j, T_j, V_j, e_j \in K[x]$ и для некоторых приведенных дивизоров $D_j, E_j \in \mathrm{Div}(L)$ справедливы соотношения (5.3.2.1)-(5.3.2.8).

Доказательство. В предложении 5.3.3.9 доказано, что $A_j, B_j \in K[x]$. Оценки нормирований A_j и B_j следуют из предложения 5.3.3.10. Тождества 5.3.3.19 следуют из предложений 5.1.1.3 и 5.1.1.4.

Если положить (5.3.3.20), то $U_j, T_j, V_j, e_j \in K[x]$. Определим дивизоры $D_j, E_j \in \mathrm{Div}(L)$ из соотношений (5.3.2.5)-(5.3.2.6), тогда, действительно, справедливы все соотношения (5.3.2.1)-(5.3.2.8), так как $(U_{j-1}xh, V_{j-1})$ — представление Мамфорда дивизора $D_j + (x)_\circ^- + (h)_\circ^-$, (T_jxh, V_{j-1}) — представление Мамфорда дивизора $E_j + (x)_\circ^- + (h)_\circ^-$. □

Положим $S = \{v_x^-, v_h^+\}$.

Лемма 5.3.3.14. *1. Любая нетривиальная S-единица поля L имеет вид*

$$\frac{\mu_1 + \mu_2\sqrt{f}}{h^m} \text{ или } \frac{\mu_1 + \mu_2\sqrt{f}}{x^m}, \tag{5.3.3.21}$$

где $\mu_1, \mu_2 \in K[x]$, $m \in \mathbb{N}$, $v_x(\mu_2) = v_h(\mu_2) = 0$, $\max(\deg(\mu_1^2), \deg(f\mu_2^2)) = 2m$.

2. Если существует нетривиальная S-единица вида (5.3.3.21), то справедливо тождество

$$\mu_1^2 - f\mu_2^2 = bx^m h^m, \quad v_x(\mu_2) = v_h(\mu_2) = 0, \quad b \in K^*, \quad \max\left(\deg(\mu_1^2),\ \deg(f\mu_2^2)\right) = 2m. \tag{5.3.3.22}$$

3. Пусть существуют $\mu_1, \mu_2 \in K[x]$, удовлетворяющие (5.3.3.22), и v_x^- и v_h^+ такие продолжения соответственно нормирований v_x и v_h поля $K(x)$, что $v_x^+\left(\mu_1 + \mu_2\sqrt{f}\right) > 0$ и $v_h^+\left(\mu_1 + \mu_2\sqrt{f}\right) > 0$. Тогда элементы $(\mu_1 + \mu_2\sqrt{f})/x^m$ и $(\mu_1 - \mu_2\sqrt{f})/h^m$ являются нетривиальными S-единицами. В качестве фундаментальной S-единицы можно выбрать любую из этих S-единиц тогда и только тогда, когда $m \in \mathbb{N}$ — минимальное число, для которого (5.3.3.22) имеет решение в многочленах $\mu_1, \mu_2 \in K[x]$.

Доказательство. Пусть $u \in L$ — нетривиальная S-единица поля L, тогда $v_x^-(u) + v_h^+(u) = 0$, поскольку по другим нормированиям поля L элемент u имеет кратность ноль. Без ограничения общности предположим $v_h^+(u) < 0 < v_x^-(u)$. Элемент u можно записать в виде несократимой над $K[x]$ дроби $u = (\mu_1 + \mu_2\sqrt{f})/\mu$, где $\mu_1, \mu_2, \mu \in K[h]$, $\operatorname{lc}(\mu) = 1$. Поскольку $v(u) = 0$ для любого нормирования v поля L, отличного от v_x^- и v_h^+, то $v\left(\mu_1 + \mu_2\sqrt{f}\right) = v(\mu)$, в частности, если бесконечное нормирование v_∞ поля $K(x)$ имеет два продолжения v_∞^- и v_∞^+ на поле L, то $v_\infty^-\left(\mu_1 + \mu_2\sqrt{f}\right) = v_\infty^+\left(\mu_1 + \mu_2\sqrt{f}\right) = v_\infty(\mu)$. Следовательно, $\mu = h^m$, где $v_\infty(\mu) = -m$, причем $\max(\deg(\mu_1^2),\ \deg(\mu_2^2 f)) = 2m$, то есть справедливо представление (5.3.3.21). Если бесконечное нормирование v_∞ поля $K(x)$ имеет единственное продолжение на поле L, то рассуждения аналогичны.

Тождество (5.3.3.22) очевидно следует из (5.3.3.21), поскольку $|v_x^-(u)| = \left|v_h^+(u)\right| = m$, а по другим нормированиям поля L элемент u имеет кратность ноль.

Пункт 3. очевидно вытекает из вышесказанного. Отметим лишь, что поскольку в множестве S всего два нормирования, то из обобщенной теоремы Дирихле о единицах в поле L существует не более одной фундаментальной S-единицы — порождающей группы нетривиальных S-единиц. □

Степенью нетривиальной S-единицы $u \in U$, записанной в виде (5.3.3.21), называется число $\deg u = m \in \mathbb{Z}$.

5.3.4. Необходимые и достаточные условия периодичности

Пусть свободный от квадратов многочлен $f \in K[x]$, такой, что нормирования v_x и v_h поля $K(x)$ имеют по два неэквивалентных продолжения $v_x^- \neq v_x^+$ и $v_h^- \neq v_h^+$ на поле $L = K(x)(\sqrt{f})$. Мы будем использовать обозначения дивизоров ∞^- и ∞^+ поля L, как в случае $\infty^- \neq \infty^+$, так и в случае $\infty^- = \infty^+ = \infty$.

Теорема 5.3.4.1. *Пусть $D_0 \in \mathrm{Div}(L)$ — такой приведенный дивизор, что $r_0 = v_x^-(D_0) = g$ или $s_0 = v_h^-(D_0) = g$. Пусть $(U_{-1}xh, V_{-1})$ — представление Мамфорда дивизора $D_0 + (x)_\circ^- + (h)_\circ^-$ и справедливы построения (5.3.2.1)-(5.3.2.8) для $j \in \mathbb{N}_0$. Тогда следующие условия эквивалентны*

1. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $D_n = D_0$;*
2. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $U_{n-1} = cU_{-1}$ для некоторой постоянной $c \in K^*$;*
3. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $V_{n-1} = V_{-1}$ и $T_n = c^{-1}T_0$ для некоторой постоянной $c \in K^*$;*
4. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $E_n = E_0$;*
5. *классы эквивалентных дивизоров $(h)_\circ^- - (x)_\circ^+ \sim (x)_\circ^- - (h)_\circ^+$ имеют конечный порядок m в группе классов дивизоров $\Delta^\circ(L)$;*
6. *непрерывные дроби типа (5.3.2.11) элементов $\sqrt{f}/x^g$ и $\sqrt{f}/h^g$, квазипериодические с длиной квазипериода n;*
7. *в гиперэллиптическом поле L существует фундаментальная S-единица степени m, где $S = \{v_x^-, v_h^+\}$;*
8. *для некоторого $b \in K^*$ уравнение*

$$\mu_1^2 - \mu_2^2 f = bx^m h^m, \qquad \max\bigl(2\deg\mu_1,\ 2\deg\mu_2 + \deg f\bigr) = 2m, \tag{5.3.4.1}$$

имеет решение $\mu_1, \mu_2 \in K[x]$ такое, что $v_x(\mu_2) = v_h(\mu_2) = 0$, $\mu_2 \neq 0$.

Если существуют $n, m \in \mathbb{N}$, указанные в эквивалентных условиях 1.-6., то они связаны соотношением

$$m = \sum_{j=0}^{n-1}(1 + r_j + s_j), \quad \text{где для } j \in \mathbb{N}_0 \tag{5.3.4.2}$$

$$r_j = -v_x^-(\alpha_j) = -v_x(a_j) = v_x^-(E_j) = v_x(T_j) = v_h(U_j) = v_h^-(D_{j+1}),$$
$$s_j = -v_h^-(\alpha_j) = -v_h(a_j) = v_h^-(E_j) = v_h(T_j) = v_x(U_j) = v_x^-(D_{j+1}).$$

Доказательство. Мы проведем доказательство теоремы 5.3.4.1 с формальным предположением, что $\infty^- \neq \infty^+$, так как в противном случае все рассуждения остаются справедливыми с подстановкой $\infty^- = \infty^+ = \infty$.

В силу симметрии условий теоремы 5.3.4.1 относительно x и h достаточно провести доказательство только для случая $D_0 = g\,(h)_\circ^-$. Тогда $U_{-1} = c_{-1}h^g$ для некоторой постоянной $c_{-1} \in K^*$, и по предложению 5.3.1.2 существуют и единственные многочлены $V_{-1}, T_0 \in K[x]$ такие, что $f - V_{-1}^2 = U_{-1}xhT_0$, и $(U_{-1}xh, V_{-1})$ — представление Мамфорда дивизора $D_0 + (x)_\circ^- + (h)_\circ^-$. По теореме 5.3.2.1 существуют и единственные последовательности многочленов $U_j, T_j, V_j, e_j \in K[x]$, $j \in \mathbb{N}_0$, $U_j \neq 0$, $T_j \neq 0$, $e_j \neq 0$, и приведенных дивизоров $D_j, E_j \in \mathrm{Div}(L)$, $j \in \mathbb{N}_0$, удовлетворяющих соотношениям (5.3.2.1)-(5.3.2.8) для $j \in \mathbb{N}_0$. Кроме того, по следствию 5.3.2.2 для $j \in \mathbb{N}_0$ имеем $(U_{j-1}xh, V_{j-1})$ — представление Мамфорда дивизора $D_j + (x)_\circ^- + (h)_\circ^-$, (T_jxh, V_{j-1}) — представление Мамфорда дивизора $E_j + (x)_\circ^- + (h)_\circ^-$, и корректно определена непрерывная дробь вида (5.3.2.11), где

$$\alpha_j = (\sqrt{f} + V_{j-1})/T_j \in L, \quad a_j = e_j x^{-r_j} h^{-s_j} = [\alpha_j]_{x,h}^-, \quad \left(\frac{x}{h}\right)^{r_j - s_j} (\alpha_j - a_j) = \frac{xh}{\alpha_{j+1}}. \tag{5.3.4.3}$$

По предложениям 5.3.1.2 и 5.3.1.3 представление Мамфорда дивизора $D_j + (x)_\circ^- + (h)_\circ^-$ единственно с точностью до постоянного множителя у многочлена U_{j-1}, дивизор D_j однозначно восстанавливается по паре многочленов $(U_{j-1}xh, V_{j-1})$. Аналогично, однозначно восстанавливаются друг из друга дивизор E_j и пара многочленов (T_jxh, V_{j-1}) с точностью до постоянного множителя у многочлена T_j. Дивизоры D_j и E_j друг из друга однозначно восстанавливаются из соотношения (5.3.2.7). Кроме того, из условия 2. следует условие 1., так как по многочленам $U_{n-1} = cU_{-1}$ дивизоры D_0 и D_n восстанавливаются однозначно. Отсюда следует эквивалентность условий 1., 2., 3., 4.

Докажем, что условие 5. эквивалентно условию 1.

Предположим, что дивизор $\big((h)_\circ^- - (x)_\circ^+\big)$ имеет порядок $m \in \mathbb{N}$. Тогда найдется такой номер $n \in \mathbb{N}$, что

$$\sum_{j=0}^{n-1}(1 + r_j + s_j) \leq m < \sum_{j=0}^{n}(1 + r_j + s_j).$$

Обозначим $\delta = m - \sum_{j=0}^{n-1}(1 + r_j + s_j)$, тогда $0 \leq \delta \leq r_n + s_n \leq g$. Из теоремы 5.3.2.3 следует, что

$$D_n - D_0 \sim -\delta\big((x)_\circ^- - (h)_\circ^+\big) = \delta\big((h)_\circ^+ - (x)_\circ^-\big). \tag{5.3.4.4}$$

Так как

$$(h)_\circ^- + (h)_\circ^+ \sim \infty^- + \infty^+ \sim (x)_\circ^- + (x)_\circ^+, \tag{5.3.4.5}$$

то $(h)_\circ^- - (x)_\circ^+ \sim (x)_\circ^- - (h)_\circ^+$. Из (5.3.4.4) получаем

$$D_n \sim D_0 - \delta\,(h)_\circ^- + \delta\,(x)_\circ^+. \tag{5.3.4.6}$$

Так как $0 \leq \delta \leq g = v_h^-(D_0)$, то в левой и правой частях (5.3.4.6) стоят эффективные дивизоры степени g. Обозначим

$$E = D_n - \left(D_0 - \delta\,(h)_\circ^- + \delta\,(x)_\circ^+\right). \tag{5.3.4.7}$$

По лемме 2.4.5.4 заключаем, что E — главный дивизор некоторой рациональной функции $\phi \in K(x)$. Для любого конечного нормирования $v \in \mathcal{V}$ такого, что $v \neq v_h^\pm$ и $v \neq \iota v$, в силу приведенности дивизоров D_0 и D_n имеем $v(E) \cdot \iota v(E) \leq 0$, а так, как E — главный дивизор рациональной функции, то получаем $v(E) = \iota v(E) = 0$. Для любого конечного нормирования $v \in \mathcal{V}$ такого, что $v = \iota v$, имеем $|v(E)| \leq 1$, а для главного дивизора рациональной функции E это возможно только, если $v(E) = 0$. Значит, дивизор E имеет вид

$$E = s_{n-1}\,(x)_\circ^- + r_{n-1}\,(h)_\circ^- - (g-\delta)\,(h)_\circ^- - \delta\,(x)_\circ^+ = (\phi)\,. \tag{5.3.4.8}$$

Из (5.3.4.8) видно, что $v_h^+(E) = 0$, значит, $v_h(\phi) = 0$. С другой стороны, из (5.3.4.8) имеем $v_x^-(E) \cdot v_x^+(E) \leq 0$, значит, $v_h(\phi) = 0$. Получается, что $\phi \in K$, и $E = 0$, откуда $\delta = 0$ и $D_n = D_0$. Отсюда следует условие 1.

Докажем, что из условия 1. следует условие 5.

Предположим, что n — минимальное число такое, что $D_n = D_0$, тогда из теоремы 5.3.2.3 сразу следует, что класс дивизора $\left((x)_\circ^- - (h)_\circ^+\right)$ имеет конечный порядок m в $\Delta^\circ(L)$, причем m и n связаны соотношением (5.3.4.2).

Рассмотрим элемент $\alpha = \sqrt{f}/x^g$. Имеем $a = [\alpha]_{x,h}^- = e/x^g$, где многочлен $e \in K[x]$, $\deg e \leq g+1$, построен как в предложении 5.3.3.5. Согласно (5.3.3.7) имеем

$$v_x^-\left(\frac{\sqrt{f}-e}{x^g}\right) \geq -g, \quad v_h^-\left(\frac{\sqrt{f}-e}{x^g}\right) \geq g,$$

откуда для некоторого приведенного дивизора $E_0 \in \mathrm{Div}(L)$ получаем

$$\left(\sqrt{f}-e\right)_\circ = (x)_\circ^- + (g+1)\,(h)_\circ^- + E_0. \tag{5.3.4.9}$$

Из (5.3.4.9) имеем $T_0 = (f-e^2)x^{-1}h^{-g-1} \in K[x]$. Положим $U_{-1} = h^g$, $V_{-1} = e$, $\alpha_0 = (\sqrt{f}+V_{-1})/T_0$, тогда из предложения 5.3.1.2 получаем $(U_{-1}xh, V_{-1})$ — представление Мамфорда дивизора $D_0 = g\,(h)_\circ^-$, (T_0xh, V_{-1}) — представление Мамфорда дивизора E_0. Далее по теореме 5.3.2.1 единственным образом восстанавливаются последовательности многочленов $U_j, T_j, V_j, e_j \in K[x]$, $j \in \mathbb{N}_0$, $U_j \neq 0$, $T_j \neq 0$, $e_j \neq 0$, и приведенных дивизоров $D_j, E_j \in \mathrm{Div}(L)$, $j \in \mathbb{N}_0$, удовлетворяющих условиям (5.3.2.1)-(5.3.2.8) для $j \in \mathbb{N}_0$. По следствию 5.3.2.2 корректно и единственным образом для элемента α_0 определена непрерывная дробь (5.3.2.11), полные и неполные частные которой удовлетворяют соотношениям (5.3.2.10) для $j \in \mathbb{N}_0$. Эту непрерывную дробь обозначим $[a_0; a_1|b_1, a_2|b_2, \ldots]$. Заметим, что

$$\alpha - a = \frac{\sqrt{f}-e}{x^g} = \left(\frac{h}{x}\right)^g \frac{\sqrt{f}-e}{h^g} = \frac{x^{1-g}h^{1+g}}{\alpha_0},$$

следовательно, непрерывная дробь типа (5.3.2.11) для элемента α имеет вид $[a; a_0|b_0, a_1|b_1, \ldots]$,

где $b_0 = x^{1-g}h^{1+g}$.

Теперь ясно, что из условия 3. следует $\alpha_n = c\alpha_0$, то есть квазипериодичность непрерывной дроби α. В свою очередь, из квазипериодичности непрерывной дроби α следует $\alpha_n = c\alpha_0$, то есть справедливо условие 3. Отметим, что условие 3 равносильно условию 5., которое симметрично относительно x и h, значит начальное предположение $D_0 = g\,(h)_\circ^-$ можно заменить на $D_0 = g\,(x)_\circ^-$, и рассматривать непрерывную дробь элемента $\sqrt{f}/h^g$. Таким образом, доказана равносильность условий 3. и 6.

Условие 5. теоремы 5.3.4.1 означает, что существует функция $u \in L$ такая, что

$$(u) = m\big((x)_\circ^- - (h)_\circ^+\big). \tag{5.3.4.10}$$

По лемме 2.4.5.1 можем считать, что функция u имеет вид

$$u = \frac{\omega_1 - \omega_2\sqrt{f}}{h^m}, \quad \omega_1, \omega_2 \in K[x], \quad \max\big(2\deg\omega_1,\ 2\deg\omega_2 + \deg f\big) = 2m, \tag{5.3.4.11}$$

поскольку все полюса (u) имеют вид $(h)_\circ^+$. В силу (5.3.4.10) справедливо соотношение $u\cdot\overline{u} = b \in K^*$, поэтому u является нетривиальной S-единицей. Поскольку по условию 5. число m минимальное, для которого выполнено (5.3.4.10), то u является фундаментальной S-единицей. Обратно, из существования фундаментальной S-единицы (5.3.4.11) следует условие 5. Таким образом, условие 7. равносильно условию 5. Условие 8. равносильно условию 7. по лемме 5.3.3.14.

Теорема 5.3.4.1 доказана. □

Покажем, как связаны непрерывные дроби типа (5.3.2.11) элементов $\alpha = \sqrt{f}/x^g$ и $\beta = \sqrt{f}/h^g$. Предположим, что непрерывная дробь α квазипериодическая. Мы уже видели в доказательстве теоремы 5.3.4.1, что это означает $\alpha_n = c\alpha_0$. В этом случае имеем $T_n = c^{-1}T_0$, $U_{n-1} = cU_{-1} = ch^g$, $r_{n-1} = g$, $s_{n-1} = 0$ и согласно (5.3.2.1) $T_{n-1} = U_{n-1}x^g h^{-g} = cx^g$, следовательно, непрерывная дробь элемента α имеет вид

$$\alpha = \left[a; \overline{a_0|b_0, a_1|b_1, \ldots, a_{n-1}|b_{n-1}}^{\,c}\right], \tag{5.3.4.12}$$

где $a = [\alpha]_{x,h}^-$, $b_0 = x^{1-g}h^{1+g}$. Обозначим

$$\beta_j = -\frac{xh}{\overline{\alpha_j}} = \frac{xhT_j}{\sqrt{f} - V_{j-1}} = \frac{\sqrt{f} + V_{j-1}}{U_{j-1}}. \tag{5.3.4.13}$$

Тогда из (5.3.4.3) имеем

$$\beta_{j+1} - \gamma_{j+1} = \frac{w_j}{\beta_j}, \quad \text{где } \gamma_{j+1} = [\beta_{j+1}]_{x,h}^- = a_j\left(\frac{x}{h}\right)^{r_j - s_j},\ w_j = x^{1+r_j-s_j}h^{1+s_j-r_j}. \tag{5.3.4.14}$$

Здесь необходимо пояснить, что величина γ_{j+1} действительно равна $[\beta_{j+1}]_{x,h}^-$. Для этого заметим, что из (5.3.2.7) имеем

$$v_x^-\,(\beta_{j+1}) = 1 - v_x^-\,(\overline{\alpha_{j+1}}) = 1 - v_x^-\left(\frac{\sqrt{f} - V_j}{T_{j+1}}\right) = -s_j,$$

и аналогично $v_h^-(\beta_{j+1}) = -r_j$. С другой стороны,

$$v_x^-\left(\frac{w_j}{\beta_j}\right) = 1 + r_j - s_j - 1 + v_x^-(\overline{\alpha_j}) = r_j - s_j + v_x^-\left(\frac{\sqrt{f} - V_{j-1}}{T_j}\right) = 1 + r_j - s_j + s_{j-1},$$

и аналогично $v_h^-(w_j/\beta_j) = 1 + s_j - r_j + r_{j-1}$. Следовательно,

$$v_x^-(\beta_{j+1} - \gamma_{j+1}) > r_j - s_j, \quad v_h^-(\beta_{j+1} - \gamma_{j+1}) > s_j - r_j.$$

Отсюда следует, что $\gamma_{j+1} = [\beta_{j+1}]_{x,h}^-$. Условие $\alpha_n = c\alpha_0$ равносильно $\beta_0 = c\beta_n$, причем $w_n = w_0$. Тем самым, построена квазипериодическая непрерывная дробь

$$\beta_n = [\gamma_n; \gamma_{n-1}|w_{n-1}, \ldots, \gamma_1|w_1, c\beta_n|w_n].$$

Далее остается заметить, что $U_{-1} = h^g$ и для $\gamma = [\beta]_{x,h}^-$ справедливы соотношения

$$c\beta_n = \beta_0 = \frac{\sqrt{f} + V_{-1}}{U_{-1}}, \quad \beta - \gamma = \beta_0 - [\beta_0]_{x,h}^- = c\beta_n - [c\beta_n]_{x,h}^- = \frac{w_{n-1}}{c^{-1}\beta_{n-1}}.$$

Таким образом,

$$\beta = \left[\gamma; \overline{c^{-1}\gamma_{n-1}|w_{n-1}, \ldots, c^{(-1)^{n-1}}\gamma_1|w_1, c^{1+(-1)^n}\gamma_n|w_n}^{c^{(-1)^{n+1}}}\right].$$

Длины квазипериодов непрерывных дробей α и β равны n. Если длина квазипериода нечетна, и коэффициент квазипериода не равен 1, то непрерывные дроби α и β периодические с длинами периодов $2n$.

5.3.5. Алгоритм поиска S-единиц

Теорема 5.3.4.1 и предложение 5.3.3.5 позволяет сформулировать эффективный алгоритм поиска S-единиц и классов дивизоров $(h)_\circ^- - (x)_\circ^+ \sim (x)_\circ^- - (h)_\circ^+$ конечного порядка в $\Delta^\circ(L)$.

Полные и неполные частные непрерывной дроби обобщенного типа восстанавливаются по формулам (5.3.4.3).

Необходимо отметить, что в пункте 1. алгоритма возможны по два разложения $\sqrt{f}$ в полях $K((x))$ и $K((h))$, отличающиеся знаком. Поэтому, чтобы проверить наличие кручения у дивизоров $(h)_\circ^- - (x)_\circ^+$ и $(h)_\circ^- - (x)_\circ^-$ достаточно дважды воспользоваться алгоритмом, рассматривая разложение $\sqrt{f}$ в поле $K((x))$ с плюсом и с минусом. Тем самым, можно не заботиться о том, какое из двух продолжений нормирования v_x поля $K(x)$ обозначено v_x^-. Следующее предложение показывает, что действительно достаточно только проверить наличие кручения у дивизоров $(h)_\circ^- - (x)_\circ^+$ и $(h)_\circ^- - (x)_\circ^-$.

Предложение 5.3.5.1. *Справедливы следующие утверждения*

1. $\operatorname{Ord}\left((x)_\circ^- - (h)_\circ^+\right) = \operatorname{Ord}\left((h)_\circ^- - (x)_\circ^+\right)$;
2. $\operatorname{Ord}\left((x)_\circ^- - (h)_\circ^-\right) = \operatorname{Ord}\left((h)_\circ^+ - (x)_\circ^+\right)$;

Алгоритм 6. Алгоритм поиска S-единиц для двух несопряженных линейных нормирований.

Дано: многочлены $h, f \in K[x]$, $2g+1 \leq \deg f \leq 2g+2$, $g \geq 2$, $\deg h = 1$, такие, что многочлен f свободен от квадратов и нормировния v_x и v_h поля $K(x)$ имеют по два неэквивалентных продолжения на поле $L = K(x)(\sqrt{f})$, $j_0 \in \mathbb{N}$.

Вычислить:

$$f^{(x)} = \sum_{j=0}^{g} f_j^{(x)} x^j \in K[x], \quad \text{где } \sqrt{f} = \sum_{j=0}^{\infty} f_j^{(x)} x^j \in K((x)),$$
$$f^{(h)} = \sum_{j=0}^{g} f_j^{(h)} h^j \in K[x], \quad \text{где } \sqrt{f} = \sum_{j=0}^{\infty} f_j^{(h)} h^j \in K((h));$$

положить: $T_0 = x^g$, $V_0 = 0$, $r_0 = g$, $s_0 = 0$, $B_0 = 1$;

Цикл для $j \in \mathbb{N}_0$, $j < j_0$, **выполнить:**

вычислить:

$$a_x = \left[\frac{V_j + f^{(x)}}{B_j x^{s_j}}\right]_x^-, \quad e_x = a_x \cdot x^{s_j}, \quad a_h = \left[\frac{V_j + f^{(h)}}{B_j h^{r_j}}\right]_h^-, \quad e_h = a_h \cdot h^{r_j};$$

вычислить: $\psi_x, \psi_h \in K[x]$, $\deg \psi_x \leq s_j$, $\deg \psi_h \leq r_j$, такие, что

$$\psi_x \cdot h^{r_j+1} \equiv e_x \pmod{x^{s_j+1}}, \quad \psi_h \cdot x^{s_j+1} \equiv e_h \pmod{h^{r_j+1}};$$

вычислить:

$$e_j = \psi_x \cdot h^{r_j+1} + \psi_h \cdot x^{s_j+1}, \quad V_{j+1} = e_j B_j - V_j, \quad T_{j+1} = \frac{f - V_{j+1}^2}{B_j x^{s_j+1} h^{r_j+1}},$$
$$r_{j+1} = v_x\left(T_{j+1}\right), \quad s_{j+1} = v_h\left(T_{j+1}\right), \quad B_{j+1} = \frac{T_{j+1}}{x^{r_{j+1}} h^{s_{j+1}}};$$

если $r_{j+1} = g$, **то** успешно завершить цикл.

Конец цикла

Вернуть: $k = j+1$, $\{B_i\}_{i=0}^{j+1}$, $\{T_i\}_{i=0}^{j+1}$, $\{V_i\}_{i=0}^{j+1}$, $\{s_i\}_{i=0}^{j+1}$, $\{r_i\}_{i=0}^{j+1}$, $\{e_i\}_{i=0}^{j}$.

3. $\operatorname{Ord}\left((x)_\circ^- - (x)_\circ^-\right) = \operatorname{Ord}\left((x)_\circ^+ - (x)_\circ^+\right)$;

4. *обозначим множество дивизоров* $M = \{(x)_\circ^- - (h)_\circ^+, (x)_\circ^- - (h)_\circ^-, (x)_\circ^- - (x)_\circ^+, (h)_\circ^- - (h)_\circ^+\}$, *тогда из конечности порядков классов двух из дивизоров из множества* M *в группе классов дивизоров* $\Delta^\circ(L)$ *следует конечность порядков классов всех дивизоров из множества* M *в группе классов дивизоров* $\Delta^\circ(L)$;

Доказательство. Справедливость первых трех утверждений очевидна из соотношений

$$(x)_\circ^- + (x)_\circ^+ - \infty^- - \infty^+ \sim 0, \qquad (h)_\circ^- + (h)_\circ^+ - \infty^- - \infty^+ \sim 0 \tag{5.3.5.1}$$

или из того, что на группе дивизоров $\operatorname{Div}(L)$ корректна определена операция инволюции.

Далее докажем, например, что из конечности классов дивизоров $(x)_\circ^- - (x)_\circ^+$ и $(h)_\circ^- - (h)_\circ^+$ в группе классов дивизоров $\Delta^\circ(L)$ следует конечность классов дивизоров $(x)_\circ^- - (h)_\circ^+$ и $(x)_\circ^- - (h)_\circ^-$ в группе классов дивизоров $\Delta^\circ(L)$. Пусть $m\left((x)_\circ^- - (x)_\circ^+\right) \sim 0$ и $k\left((h)_\circ^- - (h)_\circ^+\right) \sim 0$, тогда из (5.3.5.1) имеем

$$m\left(2\,(x)_\circ^- - \infty^- - \infty^+\right) \sim 0, \qquad k\left(2\,(h)_\circ^- - \infty^- - \infty^+\right) \sim 0. \tag{5.3.5.2}$$

Домножим первое соотношение (5.3.5.2) на k, второе соотношение (5.3.5.2) на m, затем вычтем их, тогда $2mk\left((x)_\circ^- - (h)_\circ^-\right) \sim 0$. Если сначала взять инволюцию второго соотношения (5.3.5.2) и проделать те же операции, то получим $2mk\left((x)_\circ^- - (h)_\circ^+\right) \sim 0$. □

Если алгоритм 6 завершился успешно, то есть был найден номер $n \in \mathbb{N}$ такой, что $U_n = c^{-1}U_0$, то по теореме 5.3.4.1 в поле L существует фундаментальная S-единица. Положим

$$\theta_j = \frac{\sqrt{f} - V_j}{B_j}, \qquad u = \prod_{j=0}^{n-1} \theta_j.$$

Тогда в силу (5.3.2.13) имеем

$$\sum_{j=0}^{n-1} (\theta_j) = \sum_{j=0}^{n-1} (1 + r_j + s_j)\left((x)_\circ^- + (h)_\circ^- - \infty^- - \infty^+\right), \tag{5.3.5.3}$$

следовательно, элемент u имеет вид $\mu_1 + \mu_2\sqrt{f}$, и справедливо тождество $u \cdot \overline{u} = cx^m h^m$ для числа $m \in \mathbb{N}$, удовлетворяющего (5.3.4.2), и некоторого $c \in K^*$. Так как $u \in L \setminus K(x)$, то по лемме 5.3.3.14 в качестве фундаментальной S-единицы можно взять uh^{-m} или ux^{-m}.

С помощью предложения 5.3.3.13 можно другим способом найти фундаментальную S-единицу. Для этого достаточно заметить, что с одной стороны A_{n-1} имеет вид (5.3.3.18), а с другой стороны, $A_{n-1} = ch^{2g}$ для некоторой постоянной $c \in K^*$. Следовательно, из (5.3.3.18) получается тождество вида (5.3.3.22), откуда по лемме 5.3.3.14 мгновенно восстанавливается фундаментальная S-единица.

5.3.6. Новые примеры S-единиц

Приведем примеры гиперэллиптических полей $L = \mathbb{Q}(x)(\sqrt{f})$, в которых существуют нетривиальные S-единицы или нетривиальные S'-единицы, где $S = \{v_x^-, v_h^+\}$, $S' = \{v_x^-, v_h^-\}$.

В следующем примере приведено гиперэллиптическое поле $L = \mathbb{Q}(x)(\sqrt{f})$, в котором непрерывная дробь вида (5.3.2.11) для элемента $\sqrt{f}/x^2$ квазипериодическая, но не периодическая. Это обстоятельство еще раз подчеркивает существенное отличие непрерывная дробь вида (5.3.2.11) от непрерывных дробей в полях $\mathbb{Q}((x))$ и $\mathbb{Q}((h))$.

Пример 5.3.6.1. *Рассмотрим $g = 2$, $h = x - 1$ и многочлен*

$$f(x) = -(x^2 + x + 1)(4x^4 - 7x^3 + 4x^2 - 4) =$$
$$= -(h^2 + 3h + 3)(4h^4 + 9h^3 + 7h^2 + 3h - 3) = \phi(h).$$

Положим $S = \{v_x^-, v_h^+\}$, $S' = \{v_x^-, v_h^-\}$. Для элемента $\sqrt{f}/x^g$ непрерывная дробь вида (5.3.2.11) с положительными разложениями $\sqrt{f}$ в степенные ряды в полях $\mathbb{Q}((x))$ и $\mathbb{Q}((h))$ имеет вид:

$$\left[-\tfrac{7x^3-12x^2+3x-4}{2};\ \overline{\tfrac{x-2}{5}\ \mid\ x^{-1}h^3,\ -(x-2)\left(13x^2+3x+8\right)\ \mid\ xh}^{1/4}\right].$$

Эта непрерывная дробь квазипериодическая, но не периодическая. Длина квазипериода равна 2, коэффициент квазипериода $c = \frac{1}{4}$. Степень соответствующей фундаментальной S-единицы равна 4. В качестве фундаментальной S-единицы можно выбрать $(\omega_1 + \omega_2\sqrt{f})x^{-4}$ или $(\omega_1 + \omega_2\sqrt{f})h^{-4}$, где

$$\omega_1 = 3x^4 - 4x^3 + 3x^2 - 8, \qquad \omega_2 = 2(x - 2).$$

Для элемента $\sqrt{\phi}/h^g$ непрерывная дробь вида (5.3.2.11) с положительными разложениями $\sqrt{f}$ в степенные ряды в полях $\mathbb{Q}((x))$ и $\mathbb{Q}((h))$ имеет вид:

$$\left[\tfrac{h^3+2h^2+5h+12}{4};\ \overline{\tfrac{4(h-1)}{5}\ \mid\ x^3h^{-1},\ -\tfrac{(h-1)(13h^2+29h+24)}{16}\ \mid\ xh}^{4}\right].$$

Для неполных частных приведенных непрерывных дробей элементов $\sqrt{f}/x^g$ и $\sqrt{\phi}/h^g$ действительно выполнены соотношения (5.3.4.14).

Для элемента $\sqrt{f}/x^g$ непрерывная дробь вида (5.3.2.11) с разложениями $\sqrt{f}$ в степенные ряды в полях $\mathbb{Q}((x))$ и $\mathbb{Q}((h))$ разных знаков неквазипериодическая, следовательно, в поле L нет нетривиальных S'-единиц. Непрерывные дроби элементов $\sqrt{f(x)}/x^{g+1}$ и $\sqrt{f(x)}/h^{g+1}$ соответственно в полях $\mathbb{Q}((x))$ и $\mathbb{Q}((h))$ не являются квазипериодическими, поэтому в поле L нет нетривиальных S_x-единиц и S_h-единиц, где $S_x = \{v_x^-, v_x^+\}$ и $S_h = \{v_h^-, v_h^+\}$.

В следующем примере приведено гиперэллиптическое поле $L = \mathbb{Q}(x)(\sqrt{f})$, в котором непрерывная дробь вида (5.3.2.11) для элемента $\sqrt{f}/x^2$ является периодической за счет того, что коэффициент квазипериода оказался конечного порядка в мультиптикативной группе $\mathbb{Q}^*$.

Пример 5.3.6.2. *Рассмотрим* $g = 2$, $h = x - 1$ *и многочлен*

$$f(x) = x^5 - 2x^4 - x^3 + 2x^2 + 1 =$$
$$= h^5 + 3h^4 + h^3 - 3h^2 - 2h + 1 = \phi(h).$$

Положим $S = \{v_x^-, v_h^+\}$, $S' = \{v_x^-, v_h^-\}$. *Для элемента* $\sqrt{f}/x^g$ *непрерывная дробь вида* (5.3.2.11) *с положительными разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *имеет вид:*

$$\left[-x^3 + x^2 + 1;\ \overline{2\,(x^3 - x^2 - 1)\ \mid\ x^{-1}h^3}^{-1}\right].$$

Длина квазипериода равна 1, *коэффициент квазипериода* $c = -1$, *поэтому рассматриваемая непрерывная дробь периодическая с длиной периода* 2. *Степень соответствующей фундаментальной* S*-единицы равна* 3. *В качестве фундаментальной* S*-единицы можно выбрать* $(\omega_1 + \omega_2\sqrt{f})x^{-3}$ *или* $(\omega_1 + \omega_2\sqrt{f})h^{-3}$, *где*

$$\omega_1 = -x^3 + x^2 + 1, \qquad \omega_2 = 1.$$

Для элемента $\sqrt{\phi}/h^g$ *непрерывная дробь вида* (5.3.2.11) *с положительными разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *имеет вид:*

$$\left[-h^3 - 2h^2 - h + 1;\ \overline{2\,(h^3 + 2h^2 + h - 1)\ \mid\ x^3h^{-1}}^{-1}\right].$$

Для неполных частных приведенных непрерывных дробей элементов $\sqrt{f}/x^g$ *и* $\sqrt{\phi}/h^g$ *действительно выполнены соотношения* (5.3.4.14).

Для элемента $\sqrt{f}/x^g$ *непрерывная дробь вида* (5.3.2.11) *с разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *разных знаков неквазипериодическая, следовательно, в поле* L *нет нетривиальных* S'*-единиц. Непрерывные дроби элементов* $\sqrt{f(x)}/x^{g+1}$ *и* $\sqrt{f(x)}/h^{g+1}$ *соответственно в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *не являются квазипериодическими, поэтому в поле* L *нет нетривиальных* S_x*-единиц и* S_h*-единиц, где* $S_x = \{v_x^-, v_x^+\}$ *и* $S_h = \{v_h^-, v_h^+\}$.

В следующем примере приведено гиперэллиптическое поле $L = \mathbb{Q}(x)(\sqrt{f})$, в котором существует фундаментальная S'-единица, но не существует нетривиальных S-единиц. Непрерывная дробь вида (5.3.2.11) для элемента $\sqrt{f}/x^2$ оказалась не только квазипериодической, но и периодической за счет того, что длина квазипериода нечетна.

Пример 5.3.6.3. *Рассмотрим* $g = 2$, $h = x - 4$ *и многочлен*

$$f(x) = -140x^6 + 1680x^5 - 6496x^4 + 7168x^3 + 3024x^2 + 2240x + 1600 =$$
$$= -140h^6 - 1680h^5 - 6496h^4 - 7168h^3 + 3024h^2 - 2240h + 1600 = \phi(h).$$

Положим $S = \{v_x^-, v_h^+\}$, $S' = \{v_x^-, v_h^-\}$. *Для элемента* $\sqrt{f}/x^g$ *непрерывная дробь вида* (5.3.2.11)

с разложениями $\sqrt{f}$ *в степенные ряды разных знаков в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *имеет вид:*

$$\Big[-2\left(5x^3-46x^2+114x-20\right);\ \overline{\tfrac{3x-10}{40}\mid x^{-1}h^3,\ \tfrac{40(x-6)}{3}\mid xh,\ -\tfrac{3(x+2)}{160}\mid xh,}$$
$$\overline{-\tfrac{160(3x-2)}{9}\mid xh,\ \tfrac{9(x-2)(x^2-4x+2)}{320}\mid xh,\ -\tfrac{160(3x-10)}{9}\mid x^{-1}h^3,}$$
$$\overline{-\tfrac{3(x-6)}{160}\mid xh,\ \tfrac{40(x+2)}{3}\mid xh,\ \tfrac{3x-2}{40}\mid xh,\ -20\left(x-2\right)\left(x^2-4x+2\right)\mid xh}\Big].$$

Рассматриваемая непрерывная дробь квазипериодическая и периодическая. Длина квазипериода равна 5*, коэффициент квазипериода* $c=-\frac{6400}{9}$*, длина периода равна* 10*. Степень соответствующей фундаментальной* S*-единицы равна* 7*. В качестве фундаментальной* S'*-единицы можно выбрать* $(\omega_1+\omega_2\sqrt{f})x^{-7}$ *или* $(\omega_1+\omega_2\sqrt{f})h^{-7}$*, где*

$$\omega_1=(x-2)\left(x^6-12x^5+46x^4-48x^3-26x^2-24x-20\right),\quad \omega_2=1.$$

Для элемента $\sqrt{\phi}/h^g$ *непрерывная дробь вида* (5.3.2.11) *с разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *разных знаков выглядит также, как непрерывная дробь* $\sqrt{f}/x^g$ *с точностью до замены* x *на* $-h$*. Для неполных частных приведенных непрерывных дробей элементов* $\sqrt{f}/x^g$ *и* $\sqrt{\phi}/h^g$ *действительно выполнены соотношения* (5.3.4.14)*.*

Для элемента $\sqrt{f}/x^g$ *непрерывная дробь вида* (5.3.2.11) *с положительными разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *неквазипериодическая, следовательно, в поле* L *нет нетривиальных* S*-единиц. Непрерывные дроби элементов* $\sqrt{f(x)}/x^{g+1}$ *и* $\sqrt{f(x)}/h^{g+1}$ *соответственно в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *не являются квазипериодическими, поэтому в поле* L *нет нетривиальных* S_x*-единиц и* S_h*-единиц, где* $S_x=\{v_x^-,v_x^+\}$ *и* $S_h=\{v_h^-,v_h^+\}$*.*

В следующем примере приведено эллиптическое поле $L=\mathbb{Q}(x)(\sqrt{f})$, в котором существуют фундаментальные S- и S'-единицы, а, следовательно, в поле L также существуют фундаментальные S_x- и S_h-единицы, где $S_x=\{v_x^-,v_x^+\}$ и $S_h=\{v_h^-,v_h^+\}$.

Пример 5.3.6.4. *Рассмотрим* $g=1$*,* $h=x-4$ *и многочлен*

$$f(x)=40x^4-320x^3+580x^2+240x+144=$$
$$=40h^4+320h^3+580h^2-240h+144=\phi(h).$$

Положим $S=\{v_x^-,v_h^+\}$*,* $S'=\{v_x^-,v_h^-\}$*. Для элемента* $\sqrt{f}/x^g$ *непрерывная дробь вида* (5.3.2.11) *с положительными разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *имеет вид:*

$$\Big[-\tfrac{5x^2-20x-24}{2};\ \overline{-\tfrac{4(5x^2-20x-24)}{135}\mid h^2,\ -5x^2+20x+24\mid h^2}\Big].$$

Эта непрерывная дробь квазипериодическая и периодическая. Длина квазипериода равна 1*, коэффициент квазипериода* $c=\frac{135}{4}$*, длина периода равна* 2*. Степень соответствующей фундаментальной* S*-единицы равна* 2*. В качестве фундаментальной* S*-единицы можно выбрать* $(\omega_1+\omega_2\sqrt{f})x^{-2}$ *или* $(\omega_1+\omega_2\sqrt{f})h^{-2}$*, где*

$$\omega_1=-5x^2+20x+24,\qquad \omega_2=2.$$

Для элемента $\sqrt{\phi}/h^g$ *непрерывная дробь вида* (5.3.2.11) *с положительными разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *имеет вид:*

$$\left[-\tfrac{5h^2+20h-24}{2};\ \overline{-\tfrac{4(5h^2+20h-24)}{135}\mid x^2,\ -5h^2-20h+24\mid x^2}\right].$$

Для неполных частных приведенных непрерывных дробей элементов $\sqrt{f}/x^g$ *и* $\sqrt{\phi}/h^g$ *действительно выполнены соотношения* (5.3.4.14).

Для элемента $\sqrt{f}/x^g$ *непрерывная дробь вида* (5.3.2.11) *с разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *разных знаков имеет вид:*

$$\left[2\,(2x^2-11x+6);\ \overline{-\tfrac{x-3}{6}\mid h^2,\ 12\mid xh,\ \tfrac{x-1}{6}\mid xh,\ -12\,(x-2)\mid xh}\right].$$

Эта непрерывная дробь периодическая. Длина квазипериода совпадает с длиной периода и равна 4, *коэффициент квазипериода равен 1. Степень соответствующей фундаментальной* S'*-единицы равна* 5. *В качестве фундаментальной* S'*-единицы можно выбрать* $(\omega_1+\omega_2\sqrt{f})x^{-5}$ *или* $(\omega_1+\omega_2\sqrt{f})h^{-5}$, *где*

$$\omega_1=(x-2)\left(x^4-8x^3+14x^2+8x+6\right),\qquad \omega_2=1.$$

Для элемента $\sqrt{\phi}/h^g$ *непрерывная дробь вида* (5.3.2.11) *с разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *разных знаков имеет вид:*

$$\left[2\,(2h^2+11h+6);\ \overline{-\tfrac{h+3}{6}\mid x^2,\ -12\mid xh,\ \tfrac{h+1}{6}\mid xh,\ 12\,(h+2)\mid xh}\right].$$

Для неполных частных приведенных непрерывных дробей элементов $\sqrt{f}/x^g$ *и* $\sqrt{\phi}/h^g$ *действительно выполнены соотношения* (5.3.4.14). *Непрерывная дробь для элемента* $\sqrt{\phi}/h^g$ *выглядит также, как непрерывная дробь* $\sqrt{f}/x^g$ *с точностью до замены* x *на* $-h$.

Из-за того, что в поле L *существуют фундаментальные* S*- и* S'*-единицы, в поле* L *существуют фундаментальные* S_x*- и* S_h*-единицы, где* $S_x=\{v_x^-,v_x^+\}$ *и* $S_h=\{v_h^-,v_h^+\}$. *Непрерывные дроби элементов* $\sqrt{f(x)}/x^{g+1}$ *и* $\sqrt{f(x)}/h^{g+1}$ *соответственно в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *являются периодическими выглядят одинаково с точностью до замены* x *на* $-h$:

$$\left[20+\tfrac{10}{x}+\tfrac{12}{x^2};\ \overline{-\tfrac{1}{90}-\tfrac{1}{30x},\ -\tfrac{80}{3}-\tfrac{20}{x},\ -\tfrac{3}{50}-\tfrac{3}{50x},\ -\tfrac{325}{18}-\tfrac{50}{3x},\ -\tfrac{26}{375}-\tfrac{8}{125x},\ -\tfrac{125}{8}-\tfrac{125}{8x},\ -\tfrac{64}{625}-\tfrac{48}{625x},\ -\tfrac{625}{216}-\tfrac{625}{72x},\ \tfrac{96}{625}+\tfrac{48}{625x}+\tfrac{288}{3125x^2},\ -\tfrac{625}{216}-\tfrac{625}{72x},\ -\tfrac{64}{625}-\tfrac{48}{625x},\ -\tfrac{125}{8}-\tfrac{125}{8x},\ -\tfrac{26}{375}-\tfrac{8}{125x},\ -\tfrac{325}{18}-\tfrac{50}{3x},\ -\tfrac{3}{50}-\tfrac{3}{50x},\ -\tfrac{80}{3}-\tfrac{20}{x},\ -\tfrac{1}{90}-\tfrac{1}{30x},\ 40+\tfrac{20}{x}+\tfrac{24}{x^2}}\right].$$

Эта непрерывная дробь квазипериодическая и периодическая. Длина квазипериода равна 9, *коэффициент квазипериода* $c=\frac{3125}{12}$, *длина периода равна* 18. *Степени соответствующих фундаментальных* S_x*- и* S_h*-единиц равны* 10.

Пример 5.3.6.5. *Рассмотрим* $g = 2$, $h = x - 1$ *и многочлен*

$$f(x) = -3x^6 + 2x^5 + 5x^4 - 8x^3 + 4x^2 + 4 =$$
$$= -3h^6 - 16h^5 - 30h^4 - 28h^3 - 15h^2 - 4h + 4 = \phi(h).$$

Положим $S = \{v_x^-, v_h^+\}$, $S' = \{v_x^-, v_h^-\}$. *Для элемента* $\sqrt{f}/x^g$ *непрерывная дробь вида* (5.3.2.11) *с положительными разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *имеет вид:*

$$\Big[-3x^3 + 5x^2 - 2x + 2;\ \overline{\tfrac{2x-3}{6} \mid x^{-1}h^3,\ -6\,(2x+1) \mid xh,\ \tfrac{3x-4}{36} \mid xh,}$$
$$\overline{36\,(x+1) \mid xh,\ -\tfrac{x^2-2x+2}{72} \mid xh,\ -72\,(2x^3 - 3x^2 + x - 2) \mid h^2}^{1/36}\Big].$$

Эта непрерывная дробь квазипериодическая, но не периодическая. Длина квазипериода равна 6, *коэффициент квазипериода* $c = \frac{1}{36}$. *Степень соответствующей фундаментальной* S*-единицы равна* 9. *В качестве фундаментальной* S*-единицы можно выбрать* $(\omega_1 + \omega_2\sqrt{f})x^{-9}$ *или* $(\omega_1 + \omega_2\sqrt{f})h^{-9}$, *где*

$$\omega_1 = x^9 - 5x^8 + 9x^7 - 12x^6 + 21x^5 - 30x^4 + 26x^3 - 12x^2 + 8x - 8,$$
$$\omega_2 = x^6 - 4x^5 + 7x^4 - 7x^3 + 4x^2 - 4x + 4.$$

Для элемента $\sqrt{\phi}/h^g$ *непрерывная дробь вида* (5.3.2.11) *с положительными разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *имеет вид:*

$$\Big[-h^3 - 2h^2 - h + 2;\ \overline{-\tfrac{h^2+1}{2} \mid x^3h^{-1},\ h+2 \mid x^2,\ 3h-1 \mid xh,}$$
$$\overline{-\tfrac{2h+3}{6} \mid xh,\ 6\,(2h-1) \mid xh,\ -\tfrac{2h^3+3h^2+h-2}{18} \mid xh}^{36}\Big].$$

Для неполных частных приведенных непрерывных дробей элементов $\sqrt{f}/x^g$ *и* $\sqrt{\phi}/h^g$ *действительно выполнены соотношения* (5.3.4.14).

Для элемента $\sqrt{f}/x^g$ *непрерывная дробь вида* (5.3.2.11) *с разложениями* $\sqrt{f}$ *в степенные ряды в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *разных знаков неквазипериодическая, следовательно, в поле* L *нет нетривиальных* S'*-единиц. Непрерывные дроби элементов* $\sqrt{f(x)}/x^{g+1}$ *и* $\sqrt{f(x)}/h^{g+1}$ *соответственно в полях* $\mathbb{Q}((x))$ *и* $\mathbb{Q}((h))$ *не являются квазипериодическими, поэтому в поле* L *нет нетривиальных* S_x*-единиц и* S_h*-единиц, где* $S_x = \{v_x^-, v_x^+\}$ *и* $S_h = \{v_h^-, v_h^+\}$.

5.4. Непрерывные дроби обобщенного типа для нормирования второй степени

В данном разделе предложен новый подход к проблеме существования и построения нетривиальных S_h-единиц гиперэллиптического поля L для множества S_h, состоящего из двух сопряженных нормирований второй степени. Идея нового подхода заключается в построении теории непрерывных дробей обобщенного типа, связанных с нормированием второй степени. В разделах 5.2 и 5.3 исследовались обобщенные непрерывные дроби, построенные соответственно по одному и двум линейным нормированиям. Отметим, что расширив базовое поле, нормирование второй степени распадается на два линейных, и тем самым можно применять уже полученные в разделе 5.3 результаты. Однако, с точки зрения вычислений это не всегда удобно: во-первых необходимо применять арифметику в расширенном поле, а во вторых сам алгоритм для двух линейных нормирований по вычислительной сложности превосходит найденный в данном разделе алгоритм, который сравним по эффективности с известными алгоритмом для одного линейного нормирования из 5.2.

В статьях [92] и [130] изложен альтернативный подход к проблеме поиска S-единиц в гиперэллиптических полях, основанный на методе матричной линеаризации. Сильной стороной этого метода является его универсальность: метод матричной линеаризации может быть применим к произвольному набору нормирований S. С помощью указанного подхода в статье [92] было завершено доказательство гипотезы о существовании $\mathbb{Q}$-точек всех порядков, не превосходящих 30, в якобианах гиперэллиптических кривых рода 2 над полем $\mathbb{Q}$, и были единообразно построены гиперэллиптических кривые рода 2 над полем $\mathbb{Q}$, якобианы которых соответственно содержат $\mathbb{Q}$-точки всех простых порядков, не превосходящих 29. Кроме того были впервые построены гиперэллиптические кривые рода 2 над полем $\mathbb{Q}$, якобианы которых соответственно содержат $\mathbb{Q}$-точки больших порядков 33, 36 и 48.

Основные результаты этого раздела обобщают методы статьи [156] для дивизоров, обобщенных непрерывных дробей и S_h-единиц, связанных с нормированиями второй степени. В частном случае $\deg f = 2g + 1$ теория непрерывных дробей обобщенного типа, построенных по нормированию второй степени, впервые была рассмотрена в статье [16]. Основные результаты этого раздела изложены в статье [11], и не имеют ограничений на степень многочлена f.

Пусть K — произвольное поле характеристики отличной от 2. Обозначим через K^* мультипликативную группу поля K. Пусть $f \in K[x]$ свободный от квадратов многочлен, $L = K(x)(\sqrt{f})$. Пусть дан неприводимый многочлен $h \in K[x]$, $\deg h = 2$, и нормирование v_h поля $K(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле L.

Перед тем, как перейти к изложению основных результатов, мы дадим общий обзор содержания данного раздела.

В §5.4.1 мы вводим удобные для дальнейшего изложения обозначения и доказываем ряд базовых результатов для работы с дивизорами поля L. Мы придерживаемся алгебраического взгляда на дивизоры, определяя дивизоры квадратичного поля функций L, рассматриваемых над базовым полем K, с помощью теории нормирований, с основами которой можно познакомиться в §2.3.1-2.3.2, а также в [115] и [130]. В §5.4.1 мы напоминаем понятие *приведенного дивизора* поля L, а также для приведенного дивизора $D \in \mathrm{Div}(L)$ и дивизора $(h)_\circ^-$, соответствующего нормированию v_h^- второй степени, корректно определяем *представление Мамфорда* дивизора $D + (h)_\circ^-$. Представление Мамфорда позволяет работать с приведенными дивизорами, используя только многочлены и функции поля L. В предложении 5.4.1.1 мы формулируем важные для наших дальнейших рассуждений утверждения о дивизорах поля L. Некоторые из этих утверждений в частных случаях с базовым полем $\mathbb{C}$ комплексных чисел могут быть выделены из шага II §2 гл. IIIa [48]. С введенными нами обозначениями мы даем наглядное и эффективное доказательство предложения 5.4.1.1 в общем случае над произвольным полем констант K, характеристики отличной от 2.

В §5.4.2 мы даем схему построения обобщенной непрерывной дроби с нормированием второй степени, а также полное исследование каждого шага построения этой непрерывной дроби с точки зрения арифметики дивизоров поля L. Для явного построения обобщенной непрерывной дроби элемента $\beta \in L$ по данному нормированию v_h^- необходимо корректно определить понятие целой части $[\beta]_h^-$ элемента $\beta \in L$ по нормированию v_h^-. Лемма 5.4.2.1 сводит определение $[\beta]_h^-$ к решению степенного сравнения, что позволяет эффективно искать неполные частные непрерывной дроби. Предложение 5.4.2.2, описывающее связь между обобщенными непрерывными дробями и специальной последовательностью дивизоров поля L, является основным в §5.4.2 и ключевым для доказательства теоремы 5.4.4.1.

В §5.4.3 мы напоминаем необходимые сведения из теории обобщенных функциональных непрерывных дробей, а также для нашего случая доказываем некоторые свойства конечных и бесконечных обобщенных непрерывных дробей. В частности, свойство 3 предложения 5.4.3.3 демонстрирует важное отличие рассматриваемого нами случая $\deg h = 2$ от $\deg h > 2$. Целью §5.4.3 является доказательство теоремы 5.4.3.4 о том, что при определенных условиях решение норменного уравнения (5.4.3.8) является достаточно хорошим приближением к элементу вида $\sqrt{f}/h^{s_0}$, и дает подходящую дробь p_n/q_n к непрерывной дроби элемента $\sqrt{f}/h^{s_0}$. Теорема 5.4.3.4 является важнейшим звеном в доказательстве теоремы 5.4.4.4. Наконец, в §5.4.3 получено важное замечание о том, что непрерывная дробь (5.4.2.18), построенная с помощью соотношений (5.4.2.13), и последовательность многочленов $U_j, V_j \in K[x]$, дающих соответственно представление Мамфорда для последовательности приведенных дивизоров $D_j \in \mathrm{Div}(L)$, удовлетворяющих соотношениям (5.4.2.4)-(5.4.2.7), восстанавливаются друг из друга однозначным образом.

В §5.4.4 мы доказываем основные результаты данной статьи — теоремы 5.4.4.1, 5.4.4.3 и 5.4.4.4. В теореме 5.4.4.1 доказана эквивалентность ряда условий, из которых особенно примечательны условия периодичности обобщенной непрерывной дроби типа (5.4.2.18) специального элемента поля L, и условие конечности класса дивизора $\left((h)_\infty^- - (h)_\infty^+\right)$, в группе классов дивизоров степени ноль $\Delta^\circ(L)$. В теореме 5.4.4.3 к эквивалентным условиям теоремы 5.4.4.1 добавлены еще два эквивалентных условия о существовании в поле L фундаментальной S_h-единицы и о разрешимости норменного уравнения (5.4.4.12). В теореме 5.4.4.4 при четных значениях рода g гиперэллиптического поля L некоторые эквивалентные условия теорем 5.4.4.1 и 5.4.4.3 могут быть значительно упрощены. Из теорем 5.4.4.1, 5.4.4.3 и 5.4.4.4 следует, что для наших целей ключевыми элементами являются элементы вида $\sqrt{f}/h^{s_0}$ и их непрерывные дроби, подобно тому, как это было для непрерывных дробей с нормированиями первой степени (см. [17; 20]).

В §5.4.5 показано, что в гиперэллиптическом поле L рода два корни последовательности многочленов U_j, построенной в §5.4.2 по данному приведенному дивизору $D_0 \in \mathrm{Div}(L)$, являются индикаторами для существования в поле L нетривиальных S-единиц, где множество S состоит из нормирований первой степени, связанных с корнями многочленов U_j. Для наглядности мы рассматриваем граф G, у которого вершинами являются корни многочленов U_j, а ребрами являются сами многочлены U_j. Каждую вершину графа G мы красим в один из четырех цветов в зависимости от наличия нетривиальных S-единиц в поле L, где множество S состоит из двух сопряженных нормирований первой степени, связанных с соответствующим корнем, стоящем в рассматриваемой вершине графа G. Предложения 5.4.5.1-5.4.5.3 описывают свойства графа G в предположении, что в поле L существует фундаментальная S_h-единица. Из этих свойств в частности следует, что по периодической обобщенной непрерывной дроби ключевых элементов для нормирования второй степени мы можем определить периодичность непрерывных дробей ключевых элементов для нормирований первой степени, соответствующих полюсам дивизоров полных частных обобщенной непрерывной дроби. Это дает нам возможность глубже понимать строение подгруппы J_{tor} элементов кручения якобиана гиперэллиптической кривой.

В главе 4 дано полное описание эллиптических полей $L = \mathbb{Q}(x)(\sqrt{f})$, обладающих периодическими непрерывными дробями элементов $\sqrt{f}$ для $3 \le \deg f \le 4$. Для полей L с $\deg f > 4$ на данный момент такого описания нет. В предложении 5.4.5.5 §5.4.5 мы даем достаточные условия для существования в гиперэллиптическом поле $L = K(x)(\sqrt{f})$ рода 2 элемента вида $\sqrt{f}+V$, где $V \in K[x]$, такого, что его обобщенная непрерывная дробь, построенная с помощью нормирования второй степени в поле L, является периодической. С помощью предложения 5.4.5.5 нами найден пример элемента вида $\sqrt{f}+V$, обобщенная непрерывная дробь которого периодическая (см. пример 5.4.5.6).

На основании теорем 5.4.4.1, 5.4.4.3 и 5.4.4.4 мы приводим в §3.2.1 алгоритм для определения порядка класса дивизора, связанного с нормированием v_h^-, в группе классов дивизоров степени ноль. По сложности данный алгоритм совпадает с соответствующим алгоритмом поиска порядка класса дивизора, связанного с линейным нормированием, в группе классов дивизоров степени ноль (см. §5.2 и [20; 156]).

В §5.4.7 с помощью нового алгоритма найдены примеры, показывающие, что в гиперэллиптических полях существуют фундаментальные S_h-единицы, которые невозможно найти известными методами, основанными на свойствах непрерывных дробей, построенных по нормированиям первой степени. Для случая нечетного рода g в §5.4.7 приведены примеры к теореме 5.4.4.1 и контрпример к теореме 5.4.4.4.

Обозначим множество целых неотрицательных чисел $\mathbb{N}_0$. Для многочленов $A, B \in K[x]$ символом $\gcd(A,\ B)$ обозначим их наибольший общий делитель, причем условие взаимнопросты многочленов $A, B \in K[x]$ будем записывать как $\gcd(A,\ B) \in K^*$. Если нормирование v поля $K(x)$ имеет два неэквивалентных продолжения на поле L, то мы их будем обозначать v^- и v^+, не придавая значения, какое именно из продолжений мы обозначили v^-, а какое v^+. Некоторые связанные с нормированиями v^- и v^+ объекты мы также соответственно помечаем символами “$-$” и “$+$”. Для свойств, которые выполняются аналогично для объектов, помеченных символами “$-$” и “$+$”, мы используем символ $\pm$.

Результаты этого раздела опубликованы в статьях [11; 16].

5.4.1. Дивизоры гиперэллиптического поля

Пусть $f \in K[x]$ — свободный от квадратов многочлен, $\deg f \geq 3$, $L = K(x)(\sqrt{f})$. Пусть $\mathcal{V}$ — множество нормирований поля L, определенных над полем K.

Пусть неприводимому многочлену $h_v \in K[x]$ соответствует нормирование v поля $K(x)$. Обозначим $K(x)_v$ пополнение поля $K(x)$ по нормированию v. Предположим, что нормирование v поля $K(x)$ имеет два продолжения v^- и v^+ на поле L. Это означает, что поле L может быть вложено в $K(x)_v$ двумя способами, которые соответствуют нормированиям v^- и v^+, и каждый элемент $\beta \in L$ имеет два разложения в степенные ряды в поле формальных степенных рядов, которые также соответствуют нормированиям v^- и v^+:

$$\beta = \sum_{j=s_0}^{\infty} b_j^{(\pm)} h_v^j, \quad b_j^{(\pm)} \in K[x],\ \deg b_j^{(\pm)} < \deg h_v,$$

причем для любого $s \geq s_0$ имеем

$$v^{\pm}\left(\beta - \sum_{j=s_0}^{s} b_j^{(\pm)} h_v^j\right) > s.$$

Обозначим $\mathrm{Div}(L)$ — группу K-дивизоров поля L,

$$\mathrm{Div}(L) = \left\{ D = \sum_{v \in \mathcal{V}} n_v v,\ n_v \in \mathbb{Z} \right\},$$

где для каждого дивизора D в наборе чисел $\{n_v\}_{v \in \mathcal{V}}$ только конечное количество отлично от нуля. Там, где ясно, что суммирование берется по $v \in \mathcal{V}$, будем его опускать. Все дивизоры, о которых далее пойдет речь, лежат в $\mathrm{Div}(L)$.

Для $D \in \mathrm{Div}(L)$, $D = \sum n_v v$, определим

$$\deg D = \sum n_v \deg v, \quad \deg_z D = \sum_{n_v > 0} n_v \deg v.$$

Для фиксированного нормирования $v \in \mathcal{V}$ определим число $v(D) = n_v = n_v(D)$. Определим в качестве носителя дивизора D множество нормирования, входящих в дивизор D:

$$\mathrm{Supp}\ D = \{ v \in \mathcal{V} :\ v(D) \neq 0 \}.$$

Дивизор $D \in \mathrm{Div}(L)$ называется эффективным, если $v(D) \geq 0$ для всех $v \in \mathcal{V}$. Скажем, что для дивизоров $D, E \in \mathrm{Div}(L)$ выполнено сравнение $D \leq E$, если $E - D$ эффективный дивизор. Для двух эффективных дивизоров $D, E \in \mathrm{Div}(L)$ определим эффективный дивизор $\mathrm{gcdiv}\,(D,\ E) \in \mathrm{Div}(L)$ следующим образом

$$\mathrm{gcdiv}\,(D,\ E) = \sum \min\big(v(D), v(E)\big) \cdot v.$$

Если $\min(v(D), v(E)) = 0$ для всех $v \in \mathcal{V}$, то будем писать $\mathrm{gcdiv}\,(D,\ E) = 0$.

Для главного дивизора (α) функции $\alpha \in L$, $\alpha \neq 0$, обозначим $(\alpha)_\circ$ и $(\alpha)_\infty$ соответственно эффективный дивизор нулей и эффективный дивизор полюсов функции α так, что $(\alpha) = (\alpha)_\circ - (\alpha)_\infty$, причем $v\big((\alpha)_\circ\big) \cdot v\big((\alpha)_\infty\big) = 0$ для всех $v \in \mathcal{V}$. Для функций $\alpha, \beta \in L$ будем писать $\mathrm{gcdiv}\,(\alpha,\ \beta) = \mathrm{gcdiv}\,((\alpha)_\circ,\ (\beta)_\circ)$.

Инволюция ι поля L, действующая $\iota : \sqrt{f} \to -\sqrt{f}$, $\iota^2 = \mathrm{id}$, может быть естественным образом определена на группе дивизоров $\mathrm{Div}(L)$ поля L.

Для нормирования v_h поля $K(x)$, заданного с помощью неприводимого многочлена $h \in K[x]$, имеющего два неэквивалентных продолжения v_h^- и v_h^+ на поле L, обозначим соответствующие эффективные дивизоры $(h)_\circ^- = 1 \cdot v_h^-$, $(h)_\circ^+ = 1 \cdot v_h^+$, $(h)_\circ^-, (h)_\circ^+ \in \mathrm{Div}(L)$, $(h)_\circ^- = \iota\,(h)_\circ^+ \neq (h)_\circ^+$. Если же продолжения v_h^- и v_h^+ нормирования v_h поля $K(x)$ на поле L эквивалентны, то будем писать $v_h = v_h^- = v_h^+$, $(h)_\circ^- = (h)_\circ^+ \in \mathrm{Div}(L)$. Аналогично, для продолжений v_∞^- и v_∞^+ бесконечного нормирования v_∞ поля $K(x)$, будем использовать обозначения эффективных дивизоров $\infty^- = 1 \cdot v_\infty^-$ и $\infty^+ = 1 \cdot v_\infty^+$, причем $\infty^+ = \iota\infty^- \neq \infty^+$, если $v_\infty^- \neq v_\infty^+$, и $\infty^+ = \infty^- = \infty$, если $v_\infty^- = v_\infty^+ = v_\infty$. Таким образом, например, запись $\infty^- + \infty^+$ мы будем использовать, как для случая $\infty^- \neq \infty^+$, так и для случая $\infty^- = \infty^+$, когда $\infty^- + \infty^+ = 2\infty$. Обозначим $g = [(\deg f - 1)/2]$.

Группу дивизоров степени ноль поля L обозначим $\mathrm{Div}^\circ(L)$, группу главных дивизоров по-

ля L обозначим $\operatorname{Princ}(L)$, группу классов дивизоров степени ноль поля L обозначим $\Delta^\circ(L) = \operatorname{Div}^\circ(L)/\operatorname{Princ}(L)$. Скажем, что дивизоры $D, E \in \operatorname{Div}^\circ(L)$ эквивалентны $D \sim E$, если они принадлежат одному классу в группе классов дивизоров $\Delta^\circ(L)$.

Для эффективного дивизора $D \in \operatorname{Div}(L)$ обозначим $\operatorname{Pol}(D) \in K[x]$ многочлен минимальной степени такой, что $(\operatorname{Pol}(D))_\circ \geq D$ и $\operatorname{lc}(\operatorname{Pol}(D)) = 1$.

Назовем дивизор $D \in \operatorname{Div}(L)$ *приведенным*, если D эффективный дивизор степени g, такой, что $2\operatorname{gcdiv}(D,\ \iota D) \leq (f)_\circ$. Если $v_\infty^-(D) = v_\infty^+(D) = 0$, то для приведенного дивизора D корректно определен многочлен $U = \operatorname{Pol}(D) \in K[x]$, причем $\deg U = g$ и главный дивизор многочлена U имеет вид

$$(U) = D + \iota D - g(\infty^- + \infty^+). \tag{5.4.1.1}$$

Пусть дан многочлен $U \in K[x]$, $\deg U \leq g$. Ясно, что по многочлену U приведенный дивизор D, удовлетворяющий (5.4.1.1), восстанавливается не всегда однозначно. Для эффективного дивизора $(U)_\circ^-$ такого, что дивизор нулей многочлена U имеет вид $(U)_\circ = (U)_\circ^- + \iota(U)_\circ^-$, определим эффективные дивизоры $(U)_\circ^+, (U)_{[g]}^-, (U)_{[g]}^+ \in \operatorname{Div}(L)$ такие, что $(U)_\circ^+ = \iota(U)_\circ^-$, $(U)_{[g]}^- \geq (U)_\circ^-$, $(U)_{[g]}^+ \geq (U)_\circ^+$ и

$$(U) = (U)_{[g]}^- + (U)_{[g]}^+ - g(\infty^- + \infty^+), \quad \deg(U)_{[g]}^- = \deg(U)_{[g]}^+ = g. \tag{5.4.1.2}$$

Далее мы будем везде использовать сокращенную запись $(U)_\circ^-, (U)_\circ^+$, подразумевая под ней дивизоры $(U)_{[g]}^-$ и $(U)_{[g]}^+$ степени g соответственно.

Для многочлена $V \in K[x]$, $\deg V \leq g+1$, обозначим $\left(V - \sqrt{f}\right)_{[2(g+1)]}$ такой эффективный дивизор, что $\deg\left(V - \sqrt{f}\right)_{[2(g+1)]} = 2(g+1)$, и главный дивизор функции $V - \sqrt{f} \in L$ имеет вид

$$\left(V - \sqrt{f}\right) = \left(V - \sqrt{f}\right)_{[2(g+1)]} - (g+1)(\infty^- + \infty^+). \tag{5.4.1.3}$$

Далее мы будем под сокращенной записью $\left(V - \sqrt{f}\right)_\circ$, иметь ввиду дивизор $\left(V - \sqrt{f}\right)_{[2(g+1)]}$ степени $2(g+1)$.

В случае $K = \mathbb{C}$ следующее утверждение может быть доказано методами гл. IIIa [48] (см. также [156]).

Предложение 5.4.1.1. *Пусть $g \geq 2$ и нормирование v_h поля $K(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле L, которым соответствуют эффективные дивизоры $(h)_\circ^-$ и $(h)_\circ^+$ такие, что $\deg(h)_\circ^- = \deg(h)_\circ^+ = 2$. Пусть $D \in \operatorname{Div}(L)$ — некоторый приведенный дивизор. Тогда существует единственный многочлен $V \in K[x]$, $\deg V \leq g+1$, такой, что $D + (h)_\circ^- \leq \left(V - \sqrt{f}\right)_\circ$, причем*

1. *дивизор $E = \left(V - \sqrt{f}\right)_\circ - D - (h)_\circ^-$ является приведенным;*

2. *если $\infty^- \neq \infty^+$, то $v_\infty^\pm\left(V - \sqrt{f}\right) = \delta^\pm - (g+1)$, причем $\delta^\pm \in \mathbb{N}_0$, $\delta^\pm \geq v_\infty^\pm(D)$, $\delta^- \cdot \delta^+ = 0$;*

3. корректно определен многочлен $T \in K[x]$:

$$T = \frac{f - V^2}{Uh} \in K[x], \quad \deg T \le g, \quad (\mathrm{Pol}\,(E)) = (T)\,.$$

Доказательство. Доказательство проведем конструктивным образом.

Представим в виде суммы дивизор $D + (h)_\circ^- = D_1 + D_2 + D_\infty$, где

$$D_1 = \sum_{v=\iota v \ne v_\infty^\pm} n_v(D) \cdot v, \quad D_2 = \sum_{v \ne \iota v \ne v_\infty^\pm} n_v(D) \cdot v, \quad D_\infty = n_\infty^-(D) \cdot \infty^- + n_\infty^+(D) \cdot \infty^+,$$

причем $\deg D_2 > 0$. Без ограничения общности мы рассмотрим только случай, когда $D_\infty = n_\infty \cdot \infty^-$, $n_\infty \in \mathbb{N}_0$. Так как D — приведенный дивизор, то для $v = \iota v \in \mathcal{V}$ имеем $n_v(D) = n_v(D_1) \le 1$. Положим $V_1 = \mathrm{Pol}\,(D_1)$, тогда многочлен V_1 делит f. Для каждого нормирования $v \in \mathrm{Supp}\, D_2$ определим многочлен $V_v \in K[x]$, $\deg V_v < n_v(D) \deg v$, так, что $v\left(\sqrt{f} - V_v\right) \ge n_v(D)$. Мы можем это сделать, например, разложив $\sqrt{f}$ в ряд по нормированию v. По китайской теореме об остатках существует единственный многочлен $V_2 \in K[x]$, $\deg V_2 < \deg D_2$, такой, что для всех нормирований $v \in \mathrm{Supp}\, D_2$ выполнено сравнение

$$V_1 V_2 \equiv V_v \pmod{h_v^{n_v(D)}},$$

где многочлены $h_v \in K[x]$ соответствуют нормированиям $v \in \mathrm{Div}(L)$. Определим многочлен $V_\infty \in K[x]$, $\deg V_\infty < n_\infty$, так, что

$$v_\infty^-\left(\sqrt{f} - V_\infty \cdot \mathrm{Pol}\,(D_2) \cdot V_1\right) \le n_\infty - (g+1),$$

причем, если $n_\infty = 0$, то $V_\infty = 0$. Это можно сделать, например, разложив $\sqrt{f}$ в ряд по нормированию v_∞^-. Остается положить

$$V = V_1\big(V_2 + \mathrm{Pol}\,(D_2) \cdot V_\infty\big).$$

Действительно, для любого $v \in \mathrm{Supp}\, D_2$ имеем

$$V \equiv V_1 V_2 \equiv V_v \pmod{h_v^{n_v(D)}},$$

следовательно, $v\left(\sqrt{f} - V\right) \ge n_v(D)$. Также $V_1 \mid \gcd(V,\ f)$, следовательно, для $v \in \mathrm{Supp}\, D_1$ имеем $v\left(\sqrt{f} - V\right) \ge n_v(D)$. Наконец,

$$\deg\big(V - \mathrm{Pol}\,(D_2)\, V_1 V_\infty\big) = \deg V_1 + \deg V_2 < \deg D_1 + \deg D_2 = g + 2 - n_\infty,$$

следовательно, $v_\infty^-\left(\sqrt{f} - V\right) \ge n_\infty - (g+1)$. Теперь ясно, что $D + (h)_\circ^- = D_1 + D_2 + D_\infty \le \left(V - \sqrt{f}\right)_\circ$.

Докажем, что построенный многочлен V единственный. Предположим, что существует еще один многочлен $V' \in K[x]$ такой, что $V' \ne V$, $\deg V' \le g+1$ и $D + (h)_\circ^- \le \left(V' - \sqrt{f}\right)_\circ$. Тогда $D + (h)_\circ^- \le (V' - V)_\circ$ и $\iota(D + (h)_\circ^-) \le (V' - V)_\circ$, следовательно, $Uh \mid (V' - V)$ и $\deg(V' - V) \le g + 1 - \deg(D_\infty)$, но $\deg(Uh) = g + 2 - \deg(D_\infty)$. Противоречие.

По лемме 2.4.5.1 имеем

$$2\operatorname{gcdiv}\left(V+\sqrt{f},\ V-\sqrt{f}\right)=\operatorname{gcdiv}\left(V,\ f\right)\geq(V_1)_\circ\,.$$

Для $E=\left(V-\sqrt{f}\right)_\circ-D-(h)_\circ^-$ имеем $\deg E=g$ и опять по лемме 2.4.5.1

$$2\operatorname{gcdiv}\left(E,\ \iota E\right)=\operatorname{gcdiv}\left(V,\ f\right)-(V_1)_\circ\leq(f)_\circ^-\,,$$

откуда следует пункт 1 о том, что дивизор E приведенный. Пункт 2 следует из проведенных построений и леммы 2.4.5.1. Пункт 3 следует из того, что по лемме 2.4.5.1 справедливы равенства

$$\begin{gathered}\operatorname{gcdiv}\left(f-V^2,\ Uh\right)=\operatorname{gcdiv}\left(\sqrt{f}-V,\ Uh\right)+\operatorname{gcdiv}\left(\sqrt{f}+V,\ Uh\right)=\\=\operatorname{gcdiv}\left(\sqrt{f}-V,\ D+(h)_\circ^-\right)+\iota\operatorname{gcdiv}\left(\sqrt{f}-V,\ D+(h)_\circ^-\right)=\\=D+(h)_\circ^-+\iota(D+(h)_\circ^-)=(Uh)_\circ\,,\\(\operatorname{Pol}(E))_\circ=E+\iota E=\left(\frac{f-V^2}{Uh}\right)_\circ.\end{gathered}$$

Предложение 5.4.1.1 доказано. □

Отметим, что в предложении 5.4.1.1 в случае $\deg f=2g+1$ имеем $\infty^-=\infty^+=\infty$, $g-1\leq\deg U\leq g$ и $g-1\leq\deg T\leq g$; в случае $\deg f=2g+2$ и $\infty^-=\infty^+=\infty$ имеем $\deg U=\deg T=g$ и $v_\infty\left(V-\sqrt{f}\right)=-2(g+1)$; в случае $\deg U<g$ и $\infty^-\neq\infty^+$ имеем $\deg V=g+1$; в случае $\deg V<g+1$ и $\infty^-\neq\infty^+$ имеем $\deg U=\deg T=g$.

Для данного приведенного дивизора $D\in\operatorname{Div}(L)$ и данного дивизора $(h)_\circ^-$, соответствующего нормированию v_h^- второй степени, назовем *представлением Мамфорда* дивизора $D+(h)_\circ^-$ набор из двух многочленов $(U\cdot h,V)$, определенный по предложению 5.4.1.1. Представление Мамфорда данного приведенного дивизора определено однозначно с точностью до умножения многочлена U на постоянную из K^*. Из предложения 5.4.1.1 следует, что представлением Мамфорда дивизора $\left(V-\sqrt{f}\right)_\circ-D$ является набор $(T\cdot h,V)$.

5.4.2. Построение непрерывной дроби с помощью представления Мамфорда

Рассмотрим неприводимый многочлен $h\in K[x]$. Пусть свободный от квадратов многочлен $f\in K[x]$, такой, что нормирование v_h поля $K(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле $L=K(x)(\sqrt{f})$.

Для построения непрерывной дроби по нормированию v_h^- поля L нам понадобится следующая лемма.

Лемма 5.4.2.1. *Пусть $U,T\in K[x]$, $U\neq0$, и $s=v_h(U)$, тогда существует единственный многочлен $b\in K[x]$ такой, что*

$$bUh^{-s}\equiv T\pmod{h^{s+1}},\qquad\deg b<(s+1)\cdot\deg h.\tag{5.4.2.1}$$

Доказательство. Обозначим $R = Uh^{-s}$, тогда $(R, h^{s+1}) \in K^*$, следовательно, по алгоритму Евклида можно найти многочлены $A, B \in K[x]$ такие, что $BR - Ah^{s+1} = 1$. Искомый многочлен b восстанавливается из сравнения $b \equiv BT \pmod{h^{s+1}}$. Единственность очевидна. □

Для элемента

$$\beta = \frac{V + \sqrt{f}}{U} \in L, \quad \text{где} \quad U, V \in K[x], \quad U \neq 0,$$

определим $[\beta]_h^-$ следующим образом. Положим $s = v_h(U)$, тогда существует единственный многочлен $T \in K[x]$ такой, что

$$v_h^-\left(V + \sqrt{f} - T\right) \geq s + 1, \quad \deg T < (s+1) \cdot \deg h.$$

По лемме 5.4.2.1 существует многочлен $b \in K[x]$, удовлетворяющий (5.4.2.1) с данными многочленами $U, T \in K[x]$. Положим $[\beta]_h^- = bh^{-s}$.

Предположим теперь, что $\deg h = 2$ и дан приведенный дивизор $D_0 \in \mathrm{Div}(L)$ такой, что $v_h^+(D_0) = 0$. Для построения обобщенной непрерывной дроби, соответствующей приведенному дивизор D_0, нам необходимо для каждого $j \in \mathbb{N}_0$ построить дивизоры D_{j+1}, многочлены $U_j, V_j \in K[x]$, и соответствующие им дивизоры $(U_j)_\infty^-$, $(U_j)_\infty^+$ и $\left(V_j - \sqrt{f}\right)_\infty$. Как ранее отмечалось, мы везде далее считаем, что $\deg (U_j)_\infty^- = \deg (U_j)_\infty^+ = g$ и $\deg \left(V_j - \sqrt{f}\right)_\infty = 2g+2$, рассматривая соответственно $\left((U_j)_\infty^-\right)_{[g]}$, $\left((U_j)_\infty^+\right)_{[g]}$ и $\left(V - \sqrt{f}\right)_{[2(g+1)]}$. Кроме того, будем использовать обозначения дивизоров ∞^- и ∞^+, как в случае $\infty^- \neq \infty^+$, так и в случае $\infty^- = \infty^+ = \infty$.

Обозначим $s_0 = v_h^-(D_0)$ и $(U_0)_\infty^- = D_0 - s_0\left((h)_\infty^- - (h)_\infty^+\right)$. По предложению 5.4.1.1 корректно определено представление Мамфорда $(U_0 \cdot h, V_0)$ дивизора $D_0 + (h)_\infty^-$. Обозначим

$$U_1 = \frac{f - V_0^2}{U_0 \cdot h}, \qquad (U_1)_\infty^+ = \left(V_0 - \sqrt{f}\right)_\infty - D_0 - (h)_\infty^-.$$

По предложению 5.4.1.1 U_1 является многочленом, $U_1 \in K[x]$, $\deg U_1 \leq g$ и $(U_1)_\infty^+$ — приведенный дивизор. Положим $s_1 = v_h(U_1)$ и определим приведенный дивизор $(U_1)_\infty^-$ из соотношения $(U_1) = (U_1)_\infty^- + (U_1)_\infty^+ - g(\infty^- + \infty^+)$, тогда $v_h^+\left((U_1)_\infty^-\right) = s_1$, $v_h^-\left((U_1)_\infty^-\right) = 0$. Определим

$$\alpha_1 = \frac{V_0 + \sqrt{f}}{U_1}, \qquad a_1 = [\alpha_1]_h^-, \qquad V_1 = a_1 U_1 - V_0. \tag{5.4.2.2}$$

Покажем, что $(U_1 \cdot h, V_1)$ является представлением Мамфорда дивизора $D_1 + (h)_\infty^-$, где $D_1 = (U_1)_\infty^- - s_1(h)_\infty^+ + s_1(h)_\infty^-$ — приведенный дивизор. Ясно, что $\deg V_1 \leq g + 1$. Нужно показать, что $D_1 + (h)_\infty^- \leq \left(V_1 - \sqrt{f}\right)_\infty$. Рассмотрим тождество

$$\frac{\sqrt{f} - V_1}{U_1} = \frac{\sqrt{f} + V_0}{U_1} - a_1. \tag{5.4.2.3}$$

Поскольку $\mathrm{gcdiv}\left((a_1)_\infty, (U_1 h^{-s_1})_\infty^-\right) = 0$, то

$$\left(\frac{U_1}{h^{s_1}}\right)_\infty^- \leq \left(\frac{\sqrt{f} + V_0}{U_1} - a_1\right)_\infty \qquad \mathrm{gcdiv}\left(\left(\frac{\sqrt{f} + V_0}{U_1} - a_1\right)_\infty, \left(\frac{U_1}{h^{s_1}}\right)_\infty^+\right) = 0,$$

следовательно, $(U_1 h^{-s_1})^+_\circ \le \left(\sqrt{f} - V_1\right)_\circ$. С другой стороны, по построению $v_h(a_1) = -s_1$ и

$$v_h^-\left(\frac{\sqrt{f}+V_0}{U_1} - a_1\right) = v_h^-(\alpha_1 - a_1) \ge 0,$$

следовательно, $(s_1+1)(h)^-_\circ \le \left(\sqrt{f} - V_1\right)_\circ$.

Далее с помощью предложения 5.4.1.1 продолжаем построение дивизоров D_j, функций $\alpha_j \in L$, $a_j \in K(x)$ и многочленов $U_j, V_j \in K[x]$ по индукции. В результате получим, что для каждого $j \in \mathbb{N}_0$ выполнены соотношения

$$U_{j+1} = \frac{f - V_j^2}{U_j \cdot h}, \quad \alpha_{j+1} = \frac{V_j + \sqrt{f}}{U_{j+1}}, \quad a_{j+1} = [\alpha_{j+1}]_h^-, \tag{5.4.2.4}$$

$$s_{j+1} = v_h(U_{j+1}) = -v_h(a_{j+1}) = -v_h^-(\alpha_{j+1}), \quad V_{j+1} = a_{j+1}U_{j+1} - V_j, \tag{5.4.2.5}$$

$$D_j = (U_j)^-_\circ - s_j(h)^+_\circ + s_j(h)^-_\circ, \quad \left(V_j - \sqrt{f}\right)_\circ = D_j + (h)^-_\circ + (U_{j+1})^+_\circ, \tag{5.4.2.6}$$

$$(U_{j+1})^-_\circ + (U_j)_\circ + (h)^-_\circ = \left(V_j + \sqrt{f}\right)_\circ + (U_j)^-_\circ + (s_j+1)\big((h)^-_\circ - (h)^+_\circ\big), \tag{5.4.2.7}$$

где эффективные дивизоры $(U_j)^-_\circ$, $(U_j)^+_\circ$, $(U_j)_\circ$ такие, что главный дивизор многочлена U_j можно записать в следующем виде

$$(U_j) = (U_j)_\circ - g(\infty^- + \infty^+) = (U_j)^-_\circ + (U_j)^+_\circ - g(\infty^- + \infty^+). \tag{5.4.2.8}$$

Просуммируем (5.4.2.7) по $j = 0, \dots, n-1$, получим

$$(U_n)^-_\circ + \sum_{j=0}^{n-1}(U_j)_\circ + n(h)^-_\circ = (U_0)^-_\circ + \sum_{j=0}^{n-1}\left(V_j + \sqrt{f}\right)_\circ + \sum_{j=0}^{n-1}(s_j+1)\big((h)^-_\circ - (h)^+_\circ\big)$$

или

$$(U_n)^-_\circ - (U_0)^-_\circ = \sum_{j=0}^{n-1}\left(\left(V_j + \sqrt{f}\right)_\circ - (U_j)_\circ - (h)^+_\circ\right) + \sum_{j=0}^{n-1} s_j((h)^-_\circ - (h)^+_\circ). \tag{5.4.2.9}$$

Обозначим

$$\beta_j = \frac{V_j + \sqrt{f}}{U_j \cdot h^{s_j+1}}, \tag{5.4.2.10}$$

тогда в силу (5.4.2.8) и (5.4.1.3) тождество (5.4.2.9) можно записать так:

$$(U_n)^-_\circ - (U_0)^-_\circ = \sum_{j=0}^{n-1}\Big((\beta_j) + (2s_j+1)\big((h)^-_\circ - \infty^- - \infty^+\big)\Big). \tag{5.4.2.11}$$

Таким образом, справедливо следующее предложение.

Предложение 5.4.2.2. *Пусть $D_0 \in \mathrm{Div}(L)$ — такой приведенный дивизор, что $v_h^+(D_0) = 0$. Пусть $(U_0 \cdot h, V_0)$ — представление Мамфорда дивизора $D_0 + (h)^-_\circ$. Пусть $s_0 = v_h^-(D_0)$ и $(U_0)^-_\circ = D_0 - s_0\big((h)^-_\circ - (h)^+_\circ\big)$. Пусть для $j \in \mathbb{N}$ многочлены $U_j, V_j \in K[x]$ построены по формулам (5.4.2.4), и дивизоры D_j определены по формулам (5.4.2.6). Тогда $(U_j \cdot h, V_j)$*

является представлением Мамфорда дивизора $D_j + (h)_\circ^-$ *и*

$$(U_n)_\circ^- - (U_0)_\circ^- \sim \sum_{j=0}^{n-1}(2s_j+1)\big((h)_\circ^- - \infty^- - \infty^+\big). \tag{5.4.2.12}$$

Из (5.4.2.4) следует, что для $j \in \mathbb{N}$ справедливы равенства

$$a_j = [\alpha_j]_h^-, \quad \alpha_{j+1}(\alpha_j - a_j) = h, \tag{5.4.2.13}$$

то есть α_j есть частные, и a_j — неполные частные обобщенной непрерывной дроби

$$\alpha_1 = a_1 + \cfrac{h}{a_2 + \cfrac{h}{a_3 + \cdots}}. \tag{5.4.2.14}$$

Отметим, что из (5.4.2.4) и (5.4.2.13) следует, что

$$-\overline{\alpha_j} = -\frac{h}{\overline{\alpha_{j+1}}} - a_j = \frac{\sqrt{f}+V_j}{U_j} - a_j, \tag{5.4.2.15}$$

причем из (5.4.2.5) и (5.4.2.6) имеем $v_h(U_j) = s_j$ и $v_h^-\left(V_{j-1} - \sqrt{f}\right) = s_{j-1} + s_j + 1$, значит,

$$v_h^-(\overline{\alpha_j}) = v_h^-\left(\frac{V_{j-1}-\sqrt{f}}{U_j}\right) > 0, \quad a_j = -\left[\frac{h}{\overline{\alpha_{j+1}}}\right]_h^- = \left[\frac{\sqrt{f}+V_j}{U_j}\right]_h^-. \tag{5.4.2.16}$$

Таким образом, по формулам (5.4.2.15) и (5.4.2.16) можно положить

$$a_0 = \left[\frac{\sqrt{f}+V_0}{U_0}\right]_h^-, \quad \alpha_0 = \frac{h}{\alpha_1} + a_0 = \frac{\sqrt{f}-V_0}{U_0} + \left[\frac{\sqrt{f}+V_0}{U_0}\right]_h^-, \tag{5.4.2.17}$$

и в итоге получаем обобщенную непрерывную дробь

$$\alpha_0 = a_0 + \cfrac{h}{a_1 + \cfrac{h}{a_2 + \cdots}}, \tag{5.4.2.18}$$

полные и неполные частные которой удовлетворяют соотношениям (5.4.2.13) для $j \in \mathbb{N}_0$. Мы будем рассматривать только такие обобщенные непрерывные дроби, поэтому далее для краткости будем называть выражение (5.4.2.18) непрерывной дробью и сохраним для нее обозначение $[a_0; a_1, a_2, \ldots]$.

5.4.3. Непрерывные дроби с нормированиями второй степени

Пусть дан неприводимый многочлен $h \in K[x]$. Пусть свободный от квадратов многочлен $f \in K[x]$, такой, что нормирование v_h поля $K(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле $L = K(x)(\sqrt{f})$. Пусть дана непрерывная дробь вида (5.4.2.18). Для краткости будем обозначать ее стандартным образом $\alpha = [a_0; a_1, a_2, \ldots]$.

Подходящей дробью называется $p_j/q_j = [a_0; a_1, \ldots, a_j] \in K(x)$, $j \in \mathbb{N}_0$. Положим $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, $q_0 = 1$. Тогда аналогично числовому случаю справедливы рекуррентные формулы для построения подходящих дробей

$$p_{j+1} = a_{j+1}p_j + hp_{j-1}, \quad q_{j+1} = a_{j+1}q_j + hq_{j-1}, \quad j \in \mathbb{N}. \tag{5.4.3.1}$$

Кроме того, для непрерывной дроби $\alpha = [a_0; a_1, a_2, \ldots]$ аналогично числовому случаю при $n \in \mathbb{N}$ справедливы тождества

$$p_{n-1}q_n - p_n q_{n-1} = (-1)^n h^n, \tag{5.4.3.2}$$

$$\alpha = \frac{\alpha_{n+1}p_n + hp_{n-1}}{\alpha_{n+1}q_n + hq_{n-1}}, \quad \alpha - \frac{p_n}{q_n} = \frac{(-1)^n h^{n+1}}{q_n(\alpha_{n+1}q_n + hq_{n-1})}. \tag{5.4.3.3}$$

Предложение 5.4.3.1. *1. Обобщенная непрерывная дробь* $[a_0; a_1, a_2, \ldots]$ *вида* (5.4.2.18) *элемента* $\alpha \in L$ *конечна тогда и только тогда, когда* $\alpha \in K(x)$.

2. Пусть $\deg h \geq 2$ *и* $\alpha = \phi/\psi \in K(x)$ *— несократимая дробь, тогда найдется такой номер* $n \in \mathbb{N}$, $n \leq 2\max(\deg\psi,\ \deg\phi - 1)/\deg h$, *что обобщенная непрерывная дробь вида* (5.4.2.18) *для элемента* $\alpha = \phi/\psi$ *имеет вид* $\phi/\psi = [a_0; a_1, a_2, \ldots, a_n] = p_n/q_n$, *причем справедливо неравенство*

$$\sum_{j=0}^{n-1} v_h(a_j) \leq \frac{\max(\deg\psi + 1,\ \deg\phi)}{\deg h} - \left[\frac{n+1}{2}\right]. \tag{5.4.3.4}$$

Доказательство. Ясно, что конечная непрерывная дробь $[a_0; a_1, a_2, \ldots, a_n]$ равна некоторому $\alpha_0 \in K(x)$, причем в силу однозначности построения непрерывной дроби имеем $\alpha = \alpha_0$.

Предположим, что $\alpha = \phi/\psi \in K(x)$ — несократимая дробь. Пусть $\phi_0 = \phi$, $\psi_0 = \psi$, $\alpha_0 = \phi_0/\psi_0$. По построению непрерывной дроби $[a_0; a_1, a_2, \ldots]$ для элемента α определены полные частные $\alpha_j = \phi_j/\psi_j$ и неполные частные $a_j = \tilde{a}_j/h^{s_j}$, где $\tilde{a}_j \in K[x]$, $v_h(\phi_j) = 0$, $v_h(\psi_j) = s_j \geq 0$, $j = 1, 2, \ldots$. Положим $\tilde{\psi}_j = \psi_j h^{-s_j} \in K[x]$, тогда

$$\alpha_j - a_j = \frac{\phi_j - \tilde{a}_j\tilde{\psi}_j}{h^{s_j}\tilde{\psi}_j} = \frac{h}{\alpha_{j+1}} = \frac{h\psi_{j+1}}{\phi_{j+1}},$$

причем многочлен $\tilde{a}_j \in K[x]$ с условием $\deg\tilde{a}_j \leq (s_j+1)\deg h - 1$ может быть однозначно определен из сравнения $\tilde{a}_j\tilde{\psi}_j \equiv \phi_j \pmod{h^{s_j+1}}$. Следовательно, $\psi_{j+1} = (\phi_j - \tilde{a}_j\tilde{\psi}_j)h^{-s_j-1}$, $\phi_{j+1} = \tilde{\psi}_j$. Имеем $\deg\phi_{j+1} = \deg\tilde{\psi}_j = \deg\psi_j - s_j\deg h$,

$$\deg\psi_{j+1} \leq \max\big(\deg\phi_j - (s_j+1)\deg h,\ \deg\psi_j - s_j\deg h - 1\big) =$$

$$= \max\big(\deg\psi_{j-1} - (s_{j-1}+s_j+1)\deg h,\ \deg\psi_j - s_j\deg h - 1\big) \leq$$

$$\leq \max\big(\deg\psi_{j-1} - (s_{j-1}+s_j+1)\deg h,\ \deg\psi_j - (s_j+1)\deg h + 1\big),$$

так как по условию $\deg h \geq 2$. Продолжая так и далее, получаем, что для всех $k = 1, 2, \ldots, j$ выполнены неравенства

$$\deg\psi_{j+1} \leq \max_{t=k,k+1}\left(\deg\psi_{j+1-t} - \left(\left[\frac{t+1}{2}\right] + \sum_{i=1}^{t} s_{j+1-i}\right)\deg h + (t \bmod 2)\right),$$

где символом $(m \bmod r)$ мы обозначили остаток от деления m на r для $m, r \in \mathbb{N}$. Учитывая, что

$$\deg\psi_1 \leq \max\big(\deg\phi_0,\ \deg\psi_0 + 1\big) - (s_0+1)\deg h,$$

получаем

$$\deg\psi_{j+1} \le \max\bigl(\deg\psi_0,\ \deg\phi_0 - 1\bigr) - \left(\left[\frac{j+2}{2}\right] + \sum_{i=0}^{j} s_i\right)\deg h + (j+1 \bmod 2).$$

Отсюда заключаем, что на номере $n \le 2\max(\deg\psi_0,\ \deg\phi_0 - 1)/\deg h$ процесс построения непрерывной дроби завершится, причем $\phi_n = a_n\psi_n$. □

Приведем пример функции $\alpha \in K(x)$, для которой неравенство (5.4.3.4) в предложении 5.4.3.1 превращается в равенства.

Пример 5.4.3.2. *Пусть* $\deg h = 2$, $a_0, a_1 \in K[x]$, $\deg a_0 \le 1$, $\deg a_1 = 1$, *положим*

$$\alpha = \frac{a_0a_1 + h}{a_1} = a_0 + \frac{h}{a_1}.$$

Тогда $\phi = \phi_0 = a_0a_1 + h$, $\psi = \psi_0 = a_1 = \phi_1$, $\psi_1 = 1$, *причем*

$$n = 1 = 2\max(\deg\psi,\ \deg\phi - 1)/\deg h, \quad \sum_{j=0}^{n-1} v_h\left(a_j\right) = 0 = \frac{\max(\deg\psi + 1,\ \deg\phi)}{\deg h} - 1.$$

Следующее предложение описывает необходимые нам свойства подходящих дробей p_n/q_n непрерывной дроби вида (5.4.2.18).

Предложение 5.4.3.3. *Пусть* $[a_0; a_1, a_2, \ldots]$ — *обобщенная непрерывная дробь вида* (5.4.2.18) *для элемента* $\alpha \in L$, $v_h^-(\alpha) \le 0$. *Обозначим* $t_0 = 0$, $t_j = \sum_{i=1}^{j} s_i$ *для* $j \in \mathbb{N}$, *где* $v_h^-(\alpha_j) = v_h(a_j) = -s_j$ *для* $j \in \mathbb{N}_0$. *Тогда для* $j \in \mathbb{N}_0$ *справедливы следующие утверждения:*

1. $s_j \ge 0$, $v_h(p_j) = -t_j - s_0$, $v_h(q_j) = -t_j$;

2. *многочлены* $p_jq_{j+1}h^{t_j+t_{j+1}+s_0}$, $p_{j+1}q_jh^{t_j+t_{j+1}+s_0} \in K[x]$ *взаимно просты, то есть*

$$\left(p_jq_{j+1}h^{t_j+t_{j+1}+s_0},\ p_{j+1}q_jh^{t_j+t_{j+1}+s_0}\right) \in K^*; \tag{5.4.3.5}$$

3. *если* $\deg h = 2$, *то* $v_\infty(p_j) \ge -(j+1)$, $v_\infty(q_j) \ge -j$ *и*

$$\max\left(-v_\infty\left(p_jq_{j+1}\right),\ -v_\infty\left(p_{j+1}q_j\right)\right) = 2(j+1); \tag{5.4.3.6}$$

4. *справедливы соотношения*

$$v_h^-\left(\alpha - \frac{p_j}{q_j}\right) = n + 1 - v_h(q_j) - v_h(q_{j+1}) = n + 1 + t_j + t_{j+1}. \tag{5.4.3.7}$$

Доказательство. По построению (5.4.2.13) имеем $v_h^-(\alpha_{j+1}) = 1 - v_h^-(\alpha_j - a_j)$, следовательно, $s_{j+1} \ge 0$. Из (5.4.3.1) по индукции, предполагая, что $v_h(p_j) = -t_j - s_0$, в силу $v_h(a_{j+1}p_j) < v_h(hp_{j-1})$, имеем

$$v_h(p_{j+1}) = v_h(a_{j+1}p_j) = -s_j - t_j - s_0 = -t_{j+1} - s_0.$$

Соотношение $v_h(q_j) = -t_j$ доказывается аналогично.

Получается, что $v_h\left(p_j h^{t_j+s_0}\right)=0$ и $v_h\left(q_j h^{t_j}\right)=0$. Так как $v_\infty\left(a_j\right)\geq 1-\deg h$, то из (5.4.3.2) получаем (5.4.3.5) и (5.4.3.6).

Теперь соотношение (5.4.3.7) следует из (5.4.3.3). □

Обозначим $\Sigma_h=\{b\in K[x],\ \deg b<\deg h\}$. Из (5.4.3.6) следует, что в случае $\deg h=2$ можно положить

$$\tilde{p}_j=p_j h^{-[(j+1)/2]}\in\Sigma_h[h^{-1}],\quad \tilde{q}_j=q_j h^{-[(j+1)/2]}\in\Sigma_h[h^{-1}].$$

Отметим, что $h\tilde{p}_j, h\tilde{q}_j\in\Sigma_h[h^{-1}]$ только, если j нечетно и $v_\infty\left(p_j\right)>-(j+1)$.

Свойство 3 в предложении 5.4.3.3 демонстрирует ключевое отличие случая $\deg h=2$ от $\deg h>2$.

Следующая теорема устанавливает связь между решениями норменного уравнения и подходящими дробями.

Теорема 5.4.3.4. *Пусть* $\deg h=2$ *и уравнение*

$$\mu_1^2-\mu_2^2 f=bh^m \tag{5.4.3.8}$$

для некоторых $s_0\in\mathbb{N}_0$, $m\in\mathbb{N}$, $b\in K[x]$, $v_h\left(b\right)=0$, *имеет решение* $\mu_1,\mu_2\in K[x]$ *такое, что* $v_h\left(\mu_2\right)=0$ *и* $m+s_0>2r$, *где* $r=\max\bigl([\deg(\mu_1)/2]\,,\ s_0+[\deg(\mu_2)/2]\bigr)$. *Тогда* $h^{-s_0}\mu_1/\mu_2=p_{n-1}/q_{n-1}$ *для некоторой подходящей дроби* p_{n-1}/q_{n-1} *к элементу* $\alpha=h^{-s_0}\sqrt{f}\in L$.

Доказательство. Поскольку $v_h\left(\mu_1\right)=v_h\left(\mu_2\right)=0$ и

$$h^{2s_0}\mu_2^2\left(\frac{\mu_1}{h^{s_0}\mu_2}-\frac{\sqrt{f}}{h^{s_0}}\right)\left(\frac{\mu_1}{h^{s_0}\mu_2}+\frac{\sqrt{f}}{h^{s_0}}\right)=bh^m,$$

то

$$v_h^-\left(\frac{\mu_1}{h^{s_0}\mu_2}+\frac{\sqrt{f}}{h^{s_0}}\right)=-s_0,\quad v_h^-\left(\frac{\mu_1}{h^{s_0}\mu_2}-\frac{\sqrt{f}}{h^{s_0}}\right)=m-s_0. \tag{5.4.3.9}$$

Обозначим $\tilde{\mu}_1=h^{-r}\mu_1$, $\tilde{\mu}_2=h^{s_0-r}\mu_2$, тогда $\tilde{\mu}_1,\tilde{\mu}_2\in\Sigma[1/h]$. Найдется такой номер $n\in\mathbb{N}_0$, что

$$v_h\left(\tilde{q}_n\right)=v_h\left(q_n\right)-\left[\frac{n+1}{2}\right]<v_h\left(\tilde{\mu}_2\right)\leq v_h\left(q_{n-1}\right)-\left[\frac{n}{2}\right]=v_h\left(\tilde{q}_{n-1}\right). \tag{5.4.3.10}$$

Предположим, что $h^{-s_0}\mu_1/\mu_2$ не является подходящей дробью. Тогда $h^{-s_0}\mu_1/\mu_2\neq p_{n-1}/q_{n-1}$ и справедливы неравенства

$$v_h\left(\frac{1}{\tilde{q}_{n-1}\cdot\tilde{\mu}_2}\right)\geq v_h\left(\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}}-\frac{\tilde{\mu}_1}{\tilde{\mu}_2}\right)\geq\min\left(v_h^-\left(\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}}-\alpha\right),\ v_h^-\left(\alpha-\frac{\tilde{\mu}_1}{\tilde{\mu}_2}\right)\right), \tag{5.4.3.11}$$

то есть согласно предложению 5.4.3.3 и соотношениям (5.4.3.9) выполнено

$$-v_h\left(\tilde{q}_{n-1}\right)-v_h\left(\tilde{\mu}_2\right)\geq\min\Bigl(n+t_{n-1}+t_n,\ m-s_0\Bigr). \tag{5.4.3.12}$$

Из соотношений (5.4.3.10) имеем $v_h\left(\tilde{q}_n\right)<v_h\left(\tilde{\mu}_2\right)$, откуда

$$-v_h\left(\tilde{q}_{n-1}\right)-v_h\left(\tilde{\mu}_2\right)<-v_h\left(\tilde{q}_n\right)-v_h\left(\tilde{q}_{n-1}\right)=\left[\frac{n+2}{2}\right]+\left[\frac{n}{2}\right]+t_n+t_{n-1}=n+t_{n-1}+t_n.$$

С другой стороны по условию $m+s_0 > 2r$, а по предположению (5.4.3.10) $v_h(\tilde{\mu}_2) \le v_h(\tilde{q}_{n-1})$, следовательно,

$$-v_h(\tilde{q}_{n-1}) - v_h(\tilde{\mu}_2) \le -2v_h(\tilde{\mu}_2) = 2(r-s_0) < m - s_0.$$

Таким образом, неравенство (5.4.3.12) невозможно. Данное противоречие показывает, что не могут быть выполнены одновременно неравенства (5.4.3.11), откуда следует, что $h^{-s_0}\mu_1/\mu_2 = p_{n-1}/q_{n-1}$. □

Предложение 5.4.3.5. *Пусть* $[a_0; a_1, a_2, \ldots]$ — *обобщенная непрерывная дробь вида* (5.4.2.18) *для элемента* $\alpha = \sqrt{f}/h^{s_0} + \left[\sqrt{f}/h^{s_0}\right]_h^- \in L$, $s_0 \in \mathbb{N}_0$. *Для* $j \in \mathbb{N}_0$ *обозначим*

$$A_j = (-h)^{-(j+1)}\left(h^{2s_0}p_j^2 - fq_j^2\right), \quad B_j = (-h)^{-j}\left(h^{2s_0}p_jp_{j-1} - fq_{j-1}q_j\right). \tag{5.4.3.13}$$

Тогда $A_j, B_j \in K[x]$ *и для* $j \in \mathbb{N}_0$ *справедливы тождества*

$$\alpha_{j+1} = \frac{B_j + h^{s_0}f}{A_j}, \quad B_{j+1} + B_j = a_{j+1}A_j, \quad h^{2s_0}f - B_{j+1}^2 = A_j \cdot h \cdot A_{j+1}. \tag{5.4.3.14}$$

Доказательство. Тождества (5.4.3.14) могут быть доказаны аналогичным образом, как это делается для традиционных числовых непрерывных дробей или для функциональных непрерывных дробей, построенных по нормированию первой степени (см. §§3.1.2-3.1.4). □

Предложение 5.4.3.6. *Пусть* $s_0 = g/2 \in \mathbb{N}$ *и* $\deg h = 2$. *Пусть* $\alpha_0 = [a_0; a_1, a_2, \ldots]$ — *обобщенная непрерывная дробь вида* (5.4.2.18), *построенная с помощью соотношений* (5.4.2.4)-(5.4.2.7) *по приведенному дивизору* $D_0 = s_0(h)_\infty^-$. *Тогда*

$$\alpha_0 = \frac{\sqrt{f}}{h^{s_0}} + \left[\frac{\sqrt{f}}{h^{s_0}}\right]_h^- \tag{5.4.3.15}$$

и справедливы соотношения

$$A_j = h^{s_0}U_{j+1}, \quad B_j = h^{s_0}V_j, \qquad j \in \mathbb{N}. \tag{5.4.3.16}$$

Обобщенная непрерывная дробь вида (5.4.2.18) *для элемента* $\beta = \beta_0 = \frac{\sqrt{f}}{h^{s_0}}$ *имеет вид* $\beta_0 = [a_0/2; a_1, a_2, \ldots]$, *причем* $\beta_j = \alpha_j$ *для* $j \in \mathbb{N}$.

Доказательство. Представление Мамфорда дивизора $D_0 + (h)_\infty^- = (s_0+1)(h)_\infty^-$ имеет вид $(U_0h,\ V_0)$, где $U_0 = ch^{s_0}$, $V_0 = h^{s_0}\left[\sqrt{f}/h^{s_0}\right]_h^-$, $c \in K^*$. Следовательно, по формулам (5.4.2.17) получаем (5.4.3.15). В силу однозначности разложения α_0 в непрерывную дробь вида (5.4.2.18) соотношения (5.4.3.16) следуют из тождеств (5.4.3.14). □

Так как U_{j+1} и V_j являются многочленами, то из предложения 5.4.3.6 можно получить еще одно доказательство того, что A_j и B_j также многочлены, $A_j, B_j \in K[x]$. Кроме того, $v_h(B_j) = s_0$ и $v_h(A_j) = s_0 + s_{j+1}$. Отметим, что $v_h(U_{j+1}) = -v_h(a_{j+1}) = s_{j+1} \ge 0$, причем, в отличии от случая $\deg h = 1$, вообще говоря возможно $s_{j+1} = 0$.

Отметим, что также справедливо обратное утверждение в предложении (5.4.3.6): если дана непрерывная дробь (5.4.2.18), построенная с помощью соотношений (5.4.2.13), то в силу единственности разложения элемента α_0 в непрерывную дробь вида (5.4.2.18), однозначно определены многочлены $A_j, B_j \in K[x]$, а, следовательно, из соотношений (5.4.3.16) и (5.4.2.6) можно однозначно восстановить многочлены $U_j, V_j \in K[x]$ и последовательность приведенных дивизоров D_j для $j \in \mathbb{N}_0$.

5.4.4. Необходимые и достаточные условия периодичности

Рассмотрим неприводимый многочлен $h \in K[x]$ второй степени. Пусть свободный от квадратов многочлен $f \in K[x]$, $\deg f \geq 5$, такой, что нормирование v_h поля $K(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле $L = K(x)(\sqrt{f})$. Мы будем использовать обозначения дивизоров ∞^- и ∞^+ поля L, как в случае $\infty^- \neq \infty^+$, так и в случае $\infty^- = \infty^+ = \infty$.

Центральное утверждение этого раздела сформулировано в следующей теореме.

Теорема 5.4.4.1. *Пусть $D_0 \in \mathrm{Div}(L)$ — такой приведенный дивизор, что $s_0 = v_h^-(D_0) = [g/2]$. Пусть $(U_0 \cdot h, V_0)$ — представление Мамфорда дивизора $D_0 + (h)_\circ^-$ и справедливы построения (5.4.2.4)-(5.4.2.7) для $j \in \mathbb{N}_0$. Тогда следующие условия эквивалентны*

1. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $D_n = D_0$;*
2. *найдется минимальный номер $n \in \mathbb{N}$ такой, что $V_n = V_0$ и $U_n = cU_0$ для некоторой постоянной $c \in K^*$;*
3. *класс дивизора $\left((h)_\circ^- - \infty^- - \infty^+\right)$ имеет конечный порядок m в группе классов дивизоров $\Delta^\circ(L)$;*
4. *класс дивизора $\left((h)_\circ^- - (h)_\circ^+\right)$ в группе классов дивизоров $\Delta^\circ(L)$ имеет конечный порядок m_h;*
5. *для элемента α, определенного в (5.4.2.17),*
$$\alpha = \alpha_0 = \frac{\sqrt{f} - V_0}{U_0} + \left[\frac{\sqrt{f} + V_0}{U_0}\right]_h^-,$$
непрерывная дробь типа (5.4.2.18), определенная соотношениями (5.4.2.13), квазипериодическая с длиной квазипериода n.

Если существуют $n, m, m_h \in \mathbb{N}$, указанные в эквивалентных условиях 1.-5., то

- *непрерывная дробь α чисто периодическая с длиной периода либо n, если постоянная $c = 1$ из пункта 2., либо с длиной периода $2n$ и коэффициентом квазипериода $1/c$, если $c \neq 1$;*

- *справедливы соотношения*

$$m=\sum_{j=0}^{n-1}(2s_j+1),\quad \text{где } s_j=-v_h^-(\alpha_j)=-v_h(a_j)=v_h^-(D_j)=v_h(U_j),\ j\in\mathbb{N}_0; \tag{5.4.4.1}$$

- *для минимального $t\in\mathbb{N}$, такого, что $D_{2t}=D_0$, справедливы соотношения*

$$m_h=t+\sum_{j=0}^{2t-1}s_j; \tag{5.4.4.2}$$

- *либо $m_h=m/2$, если m четно, либо $m_h=m$, если m нечетно.*

Доказательство. Мы проведем доказательство теоремы 5.4.4.1 с формальным предположением, что $\infty^-\neq\infty^+$, так как в противном случае все рассуждения остаются справедливыми с подстановкой $\infty^-=\infty^+=\infty$.

В силу предложения 5.4.1.1 имеем единственность (с точностью до постоянного множителя у многочлена U_j) представления Мамфорда. Отсюда следует эквивалентность условий 1. и 2.

Докажем, что из условия 3. следует условие 1.

Предположим, что дивизор $\big((h)_\circ^- -\infty^- -\infty^+\big)$ имеет порядок $m\in\mathbb{N}$. Тогда найдется такой номер $n\in\mathbb{N}$, что

$$\sum_{j=0}^{n-2}(2s_j+1)<m\le\sum_{j=0}^{n-1}(2s_j+1).$$

Обозначим $\delta=\sum_{j=0}^{n-1}(2s_j+1)-m$, тогда $0\le\delta\le 2s_{n-1}$. Из предложения 5.4.2.2 следует, что

$$(U_n)_\circ^- -(U_0)_\circ^-\sim\delta\big((h)_\circ^- -\infty^- -\infty^+\big). \tag{5.4.4.3}$$

Пусть $\delta=2\delta_0-\delta_1$, где $\delta_1\in\{0,1\}$, $0\le\delta_0\le s_{n-1}$, $\delta_1\le\delta_0$. Так как

$$2\big((h)_\circ^- -\infty^- -\infty^+\big)\sim\big((h)_\circ^- -(h)_\circ^+\big), \tag{5.4.4.4}$$

то из (5.4.4.3) получаем

$$(U_n)_\circ^-\sim(U_0)_\circ^-+\delta_0(h)_\circ^+ +(\delta_0-\delta_1)(h)_\circ^- +\delta_1(\infty^-+\infty^+). \tag{5.4.4.5}$$

Так как по условию теоремы $s_{n-1}\le s_0$, то в левой и правой частях (5.4.4.5) стоят эффективные дивизоры степени g. Обозначим

$$E=(U_n)_\circ^- -\Big((U_0)_\circ^- +\delta_0(h)_\circ^+ +(\delta_0-\delta_1)(h)_\circ^- +\delta_1(\infty^-+\infty^+)\Big). \tag{5.4.4.6}$$

По лемме 2.4.5.4 заключаем, что E — главный дивизор некоторой рациональной функции $\beta\in K(x)$. Для любого конечного нормирования $v\in\mathcal{V}$ такого, что $v\neq v_h^\pm$ и $v\neq\iota v$, в силу приведенности дивизоров $(U_0)_\circ^-$ и $(U_n)_\circ^-$ имеем $v(E)\cdot\iota v(E)\le 0$, а так, как E — главный дивизор рациональной функции, то получаем $v(E)=\iota v(E)=0$. Для любого конечного нормирования $v\in\mathcal{V}$ такого, что $v=\iota v$, имеем $|v(E)|\le 1$, а для главного дивизора рациональной функции E

это возможно только, если $v(E)=0$. Получается, что $\beta = bh^q$ для некоторых $q \in \mathbb{Z}$ и $b \in K^*$. Из (5.4.4.6) имеем $-1 \leq v_\infty^-(E) + v_\infty^+(E) \leq 3$, следовательно, $q=0$. Так как по построению $v_h^-\left((U_0)_\circ^-\right) = v_h^-\left((U_n)_\circ^-\right) = 0$, то $\delta = 0$, $(U_n)_\circ^- = (U_0)_\circ^-$, что равносильно $D_n = D_0$. Отсюда следует условие 1.

Докажем, что из условия 1. следует условие 3.

Предположим, что n — минимальное число такое, что $D_n = D_0$, тогда $(U_n)_\circ^- = (U_0)_\circ^-$ и по предложению 5.4.2.2 сразу следует, что класс дивизора $\left((h)_\circ^- - \infty^- - \infty^+\right)$ имеет конечный порядок m в $\Delta^\circ(L)$, причем m и n связаны соотношениями (5.4.4.1).

В силу (5.4.4.4) из условия 3. следует конечность порядка класса дивизора $\left((h)_\circ^- - (h)_\circ^+\right)$ в $\Delta^\circ(L)$, то есть следует условие 4.

Далее покажем, что при условии конечности порядка класса дивизора $\left((h)_\circ^- - (h)_\circ^+\right)$ в $\Delta^\circ(L)$ для некоторого $t \in \mathbb{N}$ справедливо соотношение (5.4.4.2).

Натуральный ряд можно разбить на следующие непересекающиеся множества

$$\mathbb{N} = \bigcup_{t=0}^{\infty}\left(t + \sum_{j=0}^{2t-1} s_j,\ t + \sum_{j=0}^{2t} s_j\right] \cup \bigcup_{t=0}^{\infty}\left(t + \sum_{j=0}^{2t} s_j,\ t+1 + \sum_{j=0}^{2t+1} s_j\right]. \tag{5.4.4.7}$$

Предположим, что дивизор $\left((h)_\circ^- - (h)_\circ^+\right)$ имеет конечный порядок $m_h \in \mathbb{N}$ в $\Delta^\circ(L)$. Рассмотрим два случая, когда m_h принадлежит соответственно первому или второму объединению в (5.4.4.7).

1) Пусть для некоторого $t \in \mathbb{N}_0$ справедливы неравенства $t + \sum_{j=0}^{2t-1} s_j < m_h \leq t + \sum_{j=0}^{2t} s_j$. При нечетном $n = 2t+1$ соотношение (5.4.2.12) можно записать в следующем виде

$$(U_{2t+1})_\circ^- - (U_0)_\circ^- + \left((h)_\circ^+ - \infty^- - \infty^+\right) \sim \left(t + \sum_{j=0}^{2t} s_j\right)\left((h)_\circ^- - (h)_\circ^+\right). \tag{5.4.4.8}$$

Обозначим $\delta = t + \sum_{j=0}^{2t} s_j - k$, тогда $0 \leq \delta < s_{2t}$, и из (5.4.4.8) следует, что

$$(U_{2t+1})_\circ^- \sim (U_0)_\circ^- - \left((h)_\circ^+ - \infty^- - \infty^+\right) + \delta\left((h)_\circ^- - (h)_\circ^+\right). \tag{5.4.4.9}$$

Так как $0 \leq \delta < s_{2t} \leq s_0$, то в левой и правой частях (5.4.4.9) стоят эффективные дивизоры степени g. Обозначим

$$E = (U_{2t+1})_\circ^- - \Big((U_0)_\circ^- - (\delta+1)(h)_\circ^+ + \delta(h)_\circ^- + (\infty^- + \infty^+)\Big).$$

По лемме 2.4.5.4 заключаем, что E — главный дивизор некоторой рациональной функции $\beta \in K(x)$. Для любого конечного нормирования $v \in \mathcal{V}$ такого, что $v \neq v_h^\pm$ и $v \neq \iota v$, по построению дивизоров $(U_j)_\circ^-$ имеем $v(E)\cdot \iota v(E) \leq 0$, а так, как E — главный дивизор, то получаем $v(E) = \iota v(E) = 0$. Для любого конечного нормирования $v \in \mathcal{V}$ такого, что $v = \iota v$, имеем $|v(E)| \leq 1$, а для главного дивизора E это возможно только, если $v(E) = 0$. Получается, что $\beta = bh^q$ для некторых $q \in \mathbb{Z}$ и $b \in K^*$, но это противоречит тому, что $1 \leq v_\infty^-(E) + v_\infty^+(E) \leq 3$. Таким образом, данный случай невозможен.

2) Пусть для некоторого $t \in \mathbb{N}_0$ справедливы неравенства $t+\sum_{j=1}^{2t} s_j < m_h \le t+1+\sum_{j=1}^{2t+1} s_j$. При четном $n = 2t$ соотношение (5.4.2.12) можно записать в следующем виде

$$(U_{2t})_\circ^- - (U_0)_\circ^- \sim \left(t + \sum_{j=0}^{2t-1} s_j\right)\left((h)_\circ^- - (h)_\circ^+\right). \tag{5.4.4.10}$$

Обозначим $\delta = t + 1 + \sum_{j=1}^{2t+1} s_j - k$, тогда $0 \le \delta \le s_{2t+1}$, и из (5.4.4.10) следует, что

$$(U_{2t+2})_\circ^- \sim (U_0)_\circ^- + \delta\left((h)_\circ^- - (h)_\circ^+\right). \tag{5.4.4.11}$$

В левой и правой частях (5.4.4.11) стоят эффективные дивизоры степени g. Обозначим

$$E = (U_{2t+1})_\circ^- - \Big((U_0)_\circ^- - \delta\,(h)_\circ^+ + \delta\,(h)_\circ^-\Big).$$

По лемме 2.4.5.4 заключаем, что E — главный дивизор некоторой рациональной функции $\beta \in K(x)$, и, более того, $\beta \in K^*$.

Если справедливо условие 4, то из (5.4.4.4) имеем условие 3.

Таким образом, образ дивизора $\left((h)_\circ^- - (h)_\circ^+\right)$ в группе классов дивизоров $\Delta^\circ(L)$ имеет конечный порядок m_h тогда и только тогда, когда $(U_{2t})_\circ^- = (U_0)_\circ^-$ для некоторого $t \in \mathbb{N}$, причем, если t минимальное такое число, то справедливо равенство (5.4.4.2).

Из (5.4.4.1) видно, что n и m одновременно четны или нечетны, следовательно, сравнивая (5.4.4.1) и (5.4.4.2), при нечетном m имеем $n = t$ и $m_h = m$, а при четном m имеем $n = 2t$ и $m_h = m/2$.

Докажем, что условие 2. эквивалентно условию 5.

При заданном нормировании v_h^- второй степени непрерывная дробь полного частного $\alpha_j \in L$, построенная с помощью соотношений (5.4.2.13), зависит только от значения α_j, поэтому, в силу (5.4.2.4), квазипериодичность α_0 эквивалентна условиям $V_n = V_0$ и $U_n = cU_0$ для некоторого минимального $n \in \mathbb{N}$, то есть квазипериодичность α_0 эквивалентна условию 2. Далее, в силу симметрии квазипериода непрерывной дроби (5.4.2.18) (аналогично теореме 3 [156]) имеем $c = 1$, если n четно; для нечетного n длина периода совпадает с длиной квазипериода или в два раза больше длины квазипериода. □

Следствие 5.4.4.2. *Пусть справедливы предположения теоремы 5.4.4.1. Пусть порядок класса дивизора* $\left((h)_\circ^- - \infty^- - \infty^+\right)$ *в группе классов дивизоров* $\Delta^\circ(L)$ *равен* $m \in \mathbb{N} \cup \{\infty\}$. *Если для некоторого приведенного дивизора* D *и* $\delta \in \mathbb{N}$ *справедливо соотношение* $D - (U_0)_\circ^- \sim \delta\left((h)_\circ^- - \infty^- - \infty^+\right)$, *то* $\delta > 2s_0$.

Доказательство. Для доказательства достаточно предположить, что $0 \le \delta \le 2s_0$, и в (5.4.4.3) заменить приведенный дивизор $(U_n)_\circ^-$ на приведенный дивизор D. Тогда с данной заменой будет справедливо соотношение (5.4.4.5) и будут справедливы дальнейшие рассуждения о главном дивизоре E, приводящие нас к противоречию. □

К пяти эквивалентным условиям теоремы 5.4.4.1 можно также добавить еще два эквивалентных условия.

Теорема 5.4.4.3. *Пусть выполнены условия теоремы 5.4.4.1 и* $S_h = \{v_h^-, v_h^+\}$. *Приведенные условия 1.-5. эквивалентны следующим условиям:*

6. *в гиперэллиптическом поле* L *существует фундаментальная* S_h*-единица* u_h *степени* m_h*;*

7. *для некоторого* $b \in K^*$ *уравнение*

$$\mu_1^2 - \mu_2^2 f = bh^m, \qquad \max\bigl(2\deg\mu_1,\ 2\deg\mu_2 + \deg f\bigr) = 2m, \tag{5.4.4.12}$$

имеет решение $\mu_1, \mu_2 \in K[x]$.

Доказательство. Условие 4. теоремы 5.4.4.1 означает, что существует функция $\beta \in L$ такая, что

$$(\beta) = m_h\bigl((h)_\infty^- - (h)_\infty^+\bigr). \tag{5.4.4.13}$$

По лемме 2.4.5.1 можем считать, что функция β имеет вид

$$\beta = \frac{\omega_1 - \omega_2\sqrt{f}}{h^{m_h}}, \quad \omega_1, \omega_2 \in K[x], \quad \max\bigl(2\deg\omega_1,\ 2\deg\omega_2 + \deg f\bigr) = 4m_h, \tag{5.4.4.14}$$

поскольку все полюса (β) имеют вид $(h)_\infty^+$. В силу (5.4.4.13) справедливо соотношение $\beta\cdot\overline{\beta} = b \in K^*$, поэтому β является нетривиальной S_h-единицей. Поскольку по условию 4. теоремы 5.4.4.1 число m минимальное, для которого выполнено (5.4.4.13), то β является фундаментальной S_h-единицей. Обратно, из существования фундаментальной S_h-единицы (5.4.4.14) следует условие 4. теоремы 5.4.4.1. Таким образом, условие 6. равносильно условию 4. теоремы 5.4.4.1. Аналогично, условие 7. равносильно условию 3. теоремы 5.4.4.1. □

Для случая гиперэллиптических полей рода два условия 1. и 6. можно уточнить.

Теорема 5.4.4.4. *Пусть выполнены условия теоремы 5.4.4.1. Если* g *четно, то приведенные условия 1.-5. эквивалентны следующим эквивалентным условиям:*

1'. *найдется минимальный номер* $n \in \mathbb{N}$ *такой, что* $U_n = cU_0$ *для некоторой постоянной* $c \in K^*$*;*

6'. *для некоторого* $b \in K^*$ *уравнение (5.4.3.8) имеет решение* $\mu_1, \mu_2 \in K[x]$ *такое, что* $v_h(\mu_2) = 0$ *и* $m + s_0 > 2r$, *где* $r = \max\bigl([\deg(\mu_1)/2],\ s_0 + [\deg(\mu_2)/2]\bigr)$.

Доказательство. Докажем, что условие 6'. эквивалентно условию 1'.

Предположим, что g четно и $U_n = cU_0$, $c \in K^*$. Тогда по предложению 5.4.3.6 имеем $A_{n-1} = c_1 h^{s_0} U_0 = c_2 h^{2s_0}$ для $c_1, c_2 \in K^*$. Согласно (5.4.3.13) запишем

$$A_{n-1} = (-h)^{-n}\bigl(h^{2s_0}p_{n-1}^2 - fq_{n-1}^2\bigr) = (-h)^{-n+2s_0}q_{n-1}^2\left(\frac{p_{n-1}}{q_{n-1}} - \alpha\right)\left(\frac{p_{n-1}}{q_{n-1}} + \alpha\right). \tag{5.4.4.15}$$

По предложению 5.4.3.3 имеем $v_h(p_{n-1}) = -t_{n-1} - s_0$, $v_h(q_{n-1}) = -t_{n-1}$, $v_h(A_{n-1}) = s_0 + s_n$. Домножая (5.4.4.15) на $h^{n+2t_{n-1}}$, получаем (5.4.3.8) с

$$\mu_1 = p_{n-1}h^{s_0+t_{n-1}} \in K[x], \quad \mu_2 = q_{n-1}h^{t_{n-1}} \in K[x], \quad m = n + 2t_{n-1} + 2s_0 = \sum_{j=0}^{n-1}(2s_j + 1). \tag{5.4.4.16}$$

По предложению 5.4.3.3 имеем $\max\bigl(-v_\infty(p_{n-1}),\ -v_\infty(q_{n-1}) + 1\bigr) = n$, следовательно,

$$2r \leq \max\bigl(\deg\mu_1,\ \deg\mu_2 + 1 + 2s_0\bigr) = n + 2t_{n-1} + 2s_0 = m < m + s_0,$$

то есть выполнены условия пункта 6'.

Если предположить, что справедливы условия пункта 6'., то по теореме 5.4.3.4 имеем $h^{-s_0}\mu_1/\mu_2 = p_{n-1}/q_{n-1}$. Тогда, принимая во внимание (5.4.3.13), получаем $A_{n-1} = c_1h^{s_0}U_0 = c_2h^{2s_0}$ для $c_1, c_2 \in K^*$, откуда $U_n = cU_0$, то есть выполнены условия пункта 1'.

При четном g из условия 1'. следует условие 1, так как по многочленам U_0 и U_n дивизоры D_0 и D_n в этом случае восстанавливаются однозначно.

Теорема 5.4.4.4 доказана. □

Следствие 5.4.4.5. *Пусть $g = 2$ и справедливы предположения теоремы 5.4.4.1. Пусть порядок класса дивизора $\bigl((h)_\circ^- - \infty^- - \infty^+\bigr)$ в группе классов дивизоров $\Delta^\circ(L)$ равен $m \in \mathbb{N} \cup \{\infty\}$.*

1. Если для некоторого приведенного дивизора D справедливо соотношение

$$D - (U_0)_\circ^- \sim \delta\bigl((h)_\circ^- - \infty^- - \infty^+\bigr), \quad 2 < \delta < m, \tag{5.4.4.17}$$

то $D = (U_{\delta-2})_\circ^-$ и порядок m конечен.

2. Если порядок m конечен, то для минимального номера $n \in \mathbb{N}$ из теоремы 5.4.4.1 справедливо равенство $n = m - 2$.

Доказательство. В случае $g = 2$ условие $s_j > 0$ для некоторого $j \in \mathbb{N}$ равносильно тому, что $s_j = 1$ и $U_j = ch$ для некотрого $c \in K^*$ и $m < \infty$. Следовательно, для минимального номера $n \in \mathbb{N}$ такого, что $s_n = 1$, справедливы равенства $s_1 = \ldots = s_{n-1} = 0$.

Пусть для некоторого приведенного дивизора D справедливо соотношение (5.4.4.17). По предложению 5.4.2.2 существует номер $k = \delta - 2 \in \mathbb{N}$ такой, что

$$(U_k)_\circ^- - (U_0)_\circ^- \sim \delta\bigl((h)_\circ^- - \infty^- - \infty^+\bigr). \tag{5.4.4.18}$$

Вычитая из (5.4.4.18) выражение (5.4.4.17), получаем $(U_k)_\circ^- - D \sim 0$, что по лемме 2.4.5.4 возможно только, если $(U_k)_\circ^- = D$.

Если $m < \infty$, то по формуле (5.4.4.1) имеем $n = m - 2$. □

Следствие 5.4.4.6. *Пусть справедливы предположения теоремы 5.4.4.1. Пусть нормирование $v \neq v_h$ поля $K(x)$ степени r продолжается на поле L одним $v = v^- = v^+$ или двумя*

$v^- \neq v^+$ *способами. Пусть* $S_v = \{v_h^-, v^-, v^+\}$, *если* $v^- \neq v^+$ *и* $S_v = \{v_h^-, v\}$, *если* $v = v^- = v^+$. *Тогда условия 1.-5. теоремы 5.4.4.1 эквивалентны следующему условию:*

8. *класс дивизора* $\left(r\,(h)_\circ^- - (d)_\circ^- - (d)_\circ^+\right)$ *имеет конечный порядок* m_2 *в группе классов дивизоров* $\Delta^\circ(L)$, *причем* $m_2 = 2m/(r,m)$, *если* $2 \mid r$, $2 \mid m_2$, $v = v^- = v^+$, *и* $m_2 = m/(r,m)$ *в противном случае.*

Доказательство. Если $v = \infty$, то условие 8. следствия совпадает с условием 3. теоремы 5.4.4.1.

Рассмотрим теперь v — конечное нормирование поля $K(x)$, соответствующее многочлену $d \in K[x]$, $\deg d = r$, и пусть $(d)_\circ^-$, $(d)_\circ^+$ — эффективные дивизоры, соответствующие нормированиям v^- и v^+ в поле L. Тогда главный дивизор многочлена d имеет вид $(d) = (d)_\circ^- + (d)_\circ^+ - r(\infty^- + \infty^+)$.

Предположим, что выполнено условие 3. теоремы 5.4.4.1. Обозначим $m_1 = m/(r,m)$. Из соотношения $m\left((h)_\circ^- - \infty^- - \infty^+\right) \sim 0$ имеем $m_1\left(r\,(h)_\circ^- - (d)_\circ^- - (d)_\circ^+\right) \sim 0$ и, следовательно, класс дивизора $\left(r\,(h)_\circ^- - (d)_\circ^- - (d)_\circ^+\right)$ имеет конечный порядок $m_2 \mid m_1$ в группе классов дивизоров $\Delta^\circ(L)$.

Пусть теперь $m_2\left(r\,(h)_\circ^- - (d)_\circ^- - (d)_\circ^+\right) \sim 0$ для некоторого минимального $m_2 \in \mathbb{N}$. Покажем, что тогда справедливо условие 3. теоремы 5.4.4.1, причем $m \mid m_2 r$. Имеем $m_2 r\left((h)_\circ^- - \infty^- - \infty^+\right) \sim 0$, следовательно, дивизор $\left((h)_\circ^- - \infty^- - \infty^+\right)$ имеет конечный порядок $m \mid m_2 r$ в группе классов дивизоров $\Delta^\circ(L)$. Но ранее мы получили условие $m_2 \mid m_1$, следовательно, $m_1 = m_2$.

Остается рассмотреть случай, когда $(d)_\circ = (d)_\circ^- = (d)_\circ^+$, $2 \mid r$ и $m_2\left(\frac{r}{2}\,(h)_\circ^- - (d)_\circ\right) \sim 0$ для некоторого минимального $m_2 \in \mathbb{N}$. Если $2 \mid m_2$, то имеем $\frac{m_2 r}{2}\left((h)_\circ^- - \infty^- - \infty^+\right) \sim 0$, откуда следует, что дивизор $\left((h)_\circ^- - \infty^- - \infty^+\right)$ имеет конечный порядок $m \mid \frac{m_2 r}{2}$ в $\Delta^\circ(L)$. Но из соотношения $m\left((h)_\circ^- - \infty^- - \infty^+\right) \sim 0$ имеем $m_1\left(r\,(h)_\circ^- - 2\,(d)_\circ\right) \sim 0$ и, следовательно, для порядка класса дивизора $\left(\frac{r}{2}\,(h)_\circ^- - (d)_\circ\right)$ в $\Delta^\circ(L)$ справедливо соотношение $m_2 \mid 2m_1$. Из условий $m \mid \frac{m_2 r}{2}$ и $m_2 \mid 2m_1$ получаем $m_2 = 2m_1$. Если же m_2 нечетно, то, рассуждая аналогично, получаем $m_2 = m_1$. □

Предложение 5.4.4.7. *Пусть справедливы предположения теоремы 5.4.4.1 и* g *нечетно. Если для некоторого минимального* $t \in \mathbb{N}$ *и некоторого* $c \in K^*$ *имеем* $U_0 = cU_{2t}$, *причем* $V_0 \neq V_{2t}$, *то существует многочлен* $d \in K[x]$ *такой, что* $d \mid f$, $\deg d \leq g$. *В случае* $\infty^- \neq \infty^+$ *степень многочлена* d *нечетна.*

Доказательство. Предположим, что g нечетно и для некоторого $t \in \mathbb{N}$ справедливо $U_{2t} = cU_0$, где $c \in K^*$. Если справедливо (5.4.4.10), то, как и в случае $g \equiv 0 \pmod 2$, дивизор $\left((h)_\circ^- - (h)_\circ^+\right)$ имеет конечный порядок $m = t + \sum_{j=1}^{2t} s_j$ в $\Delta^\circ(L)$, что равносильно квазипериодичности непрерывной дроби типа (5.4.2.18). Предположим, что (5.4.4.10) не выполняется.

Это возможно только, если $D_0 = s_0\,(h)_\circ^- + P$, $D_{2t} = s_0\,(h)_\circ^- + \iota P$, где $P \neq \iota P$ — дивизоры, соответствующие линейному нормированию, и $(U_0)_\circ = P + \iota P + s_0\,(h)_\circ$. Справедливы равенства $D_0 = (U_{2t})_\circ^+$ и из (5.4.2.6) имеем

$$\left(V_0 - \sqrt{f}\right)_\circ = D_0 + (h)_\circ^- + (U_1)_\circ^+\,, \quad \left(V_{2t-1} - \sqrt{f}\right)_\circ = D_{2t-1} + (h)_\circ^- + (U_{2t})_\circ^+\,. \tag{5.4.4.19}$$

Вычитая первое равенство (5.4.4.19) из второго, по лемме Мамфорда получаем, что $(U_1)_\circ^+ = D_{2t-1}$, что эквивалентно $D_1 = (U_{2t-1})_\circ^+$. Продолжая также рассуждать дальше, легко видеть, что $D_j = (U_{2t-j})_\circ^+$ для любого $0 \leq j \leq 2t$. В частности, $D_t = (U_t)_\circ^+$, то есть для $E = D_t - s_t\,(h)_\circ^-$ согласно (5.4.2.6) имеем $E = \iota E$, причем $E \neq 0$, так как g нечетно. Следовательно, существует многочлен $d \in K[x]$ такой, что $d \mid f$, $\deg d \leq g$. Если $\infty^- \neq \infty^+$, то $v_\infty^-(E) = v_\infty^+(E) = 0$, следовательно, $\deg d = \deg E = g - 2s_t$ нечетно. □

5.4.5. О линейных дивизорах гиперэллиптического поля рода 2

Пусть K — числовое поле, $L = K(x)(\sqrt{f})$ — гиперэллиптическое поле рода $g = 2$, $h \in K[x]$ — неприводимый многочлен, $\deg h = 2$, нормирование v_h поля $K(x)$ имеет два неэквивалентных продолжения v_h^- и v_h^+ на поле L. Возьмем в качестве начального приведенного дивизора $D_0 = (h)_\circ^- \in \mathrm{Div}(L)$. Пусть $(U_0 \cdot h, V_0)$ — представление Мамфорда дивизора $D_0 + (h)_\circ^-$ и справедливы построения (5.4.2.4)-(5.4.2.7) для $j \in \mathbb{N}_0$. Обозначим $\Sigma_h = \{b \in K[x],\ \deg b < \deg h\}$.

Пусть C — гиперэллиптическая кривая, заданная уравнением $y^2 = f(x)$, J — ее якобиан, J_{tor} — подгруппа кручения якобиана J.

Обозначим $\overline{K}$ — замыкание поля K. Так как для каждого $j \in \mathbb{N}_0$ по построению степень многочлена $U_j \in K[x]$ не превосходит $g = 2$, то у каждого многочлена U_j может быть не более двух корней в $\overline{K}$. Если степень многочлена U_j меньше двух, то дополним символом ∞ множество корней многочлена U_j до двух штук. Таким образом, будем считать, что у каждого многочлена U_j ровно два корня.

По теореме Фалтингса [30; 47] на гиперэллитической кривой C существует только конечное число рациональных K-точек $P_1, \ldots, P_N$. Нарисуем граф G, в котором вершины обозначим $x_j = x(P_j) \in K \cup \{\infty\}$, $j = 1, \ldots, N$. В графе G проведем ребро $[x_q,\ x_r]$, если для некоторого $j \in \mathbb{N}_0$ пара $(x_q,\ x_r)$ является корнями многочлена U_j. Если для некоторого $j \in \mathbb{N}_0$ многочлен U_j имеет кратный корень x_q, то ребро $[x_q,\ x_q]$ в графе G будет являться петлей. Таким образом, G — конечный граф с петлями, но без кратных ребер.

Для каждого $j = 1, \ldots, N$ обозначим v_j — нормирование поля $K(x)$, соответствующее линейному многочлену $x - x_j$. Сперва раскрасим вершины графа G в три цвета — красный, желтый и зеленый — следующим образом: вершина x_j красного цвета, если нормирование v_j имеет два продолжения v_j^- и v_j^+ на поле L, и образ дивизора $v_j^- - v_j^+$ в якобиане J имеет бесконечный порядок; вершина x_j желтого цвета, если нормирование v_j имеет единственное

продолжение v_j на поле L; вершина x_j зеленого цвета, если нормирование v_j имеет два продолжения v_j^- и v_j^+ на поле L, и образ дивизора $v_j^- - v_j^+$ в якобиане J имеет конечный порядок. Перекрасим в графе G изолированные вершины без петель в синий цвет. Назовем *степенью* зеленой вершины x_j графа G порядок образа дивизора $v_j^- - v_j^+$ в якобиане J.

Теорема 5.4.5.1. *Граф G есть совокупность несвязных друг с другом полных подграфов, некоторые из вершин которых могут иметь петли.*

Доказательство. Для доказательства достаточно показать, что из наличия двух ребер $[x_1,\ x_2]$ и $[x_1,\ x_3]$ следует, что есть ребро $[x_2,\ x_3]$. Пусть $U_{1,2}$ и $U_{1,3}$ — многочлены соответствующие ребрам $[x_1,\ x_2]$ и $[x_1,\ x_3]$. По предложению 5.4.2.2 существуют числа $m_0 \in \mathbb{N}$, $m_1 \in \mathbb{Z}$, $m_1 \neq 0$, такие, что

$$(U_{1,2})_\circ^- - (U_0)_\circ^- \sim m_0\big((h)_\circ^- - \infty^- - \infty^+\big), \tag{5.4.5.1}$$

$$(U_{1,2})_\circ^- - (U_{1,3})_\circ^- \sim m_1\big((h)_\circ^- - \infty^- - \infty^+\big), \tag{5.4.5.2}$$

где по построению графа G имеем $(U_0)_\circ^- = (h)_\circ^+$. Если порядок m класса дивизора $\big((h)_\circ^- - \infty^- - \infty^+\big)$ конечен, то по следствию 5.4.4.5 можно считать, что $|m_1| \leq m-3$. Отметим, что с точность до замены обозначений v_j^- на v_j^+ возможен один из двух случаев:

$$(U_{1,2})_\circ^- = v_1^- + v_2^-, \quad (U_{1,3})_\circ^- = v_1^- + v_3^-, \tag{5.4.5.3}$$

$$(U_{1,2})_\circ^- = v_1^- + v_2^-, \quad (U_{1,3})_\circ^- = v_1^+ + v_3^-. \tag{5.4.5.4}$$

В первом случае (5.4.5.3) из (5.4.5.2) имеем

$$\begin{gathered}(v_1^- + v_2^-) - (v_1^- + v_3^-) - \big((h)_\circ^- - \infty^- - \infty^+\big) \sim (m_1-1)\big((h)_\circ^- - \infty^- - \infty^+\big),\\ v_2^- - v_3^- + (h)_\circ^+ - \infty^- - \infty^+ \sim (m_1-1)\big((h)_\circ^- - \infty^- - \infty^+\big).\end{gathered} \tag{5.4.5.5}$$

Запишем (5.4.5.5) следующим образом

$$(U_{2,3})_\circ^- - (U_0)_\circ^- \sim (1-m_1)\big((h)_\circ^- - \infty^- - \infty^+\big), \quad (U_{2,3})_\circ^- = v_2^+ + v_3^-, \tag{5.4.5.6}$$

и, аналогичным образом,

$$(U_{2,3})_\circ^- - (U_0)_\circ^- \sim (1+m_1)\big((h)_\circ^- - \infty^- - \infty^+\big), \quad (U_{2,3})_\circ^- = v_2^- + v_3^+. \tag{5.4.5.7}$$

Заметим, что $|m_1| > 1$, так как по лемме 2.4.5.4 при $m_1 = \pm 1$ следует, что $(U_{2,3})_\circ^- = (U_0)_\circ^-$, а это невозможно. Остается воспользоваться следствием 5.4.4.5 с дивизором $D = (U_{2,3})_\circ^-$, чтобы показать, что в построениях (5.4.2.4)-(5.4.2.7) действительно найдется номер $n \in \mathbb{N}$ такой, что $(U_n)_\circ^- = (U_{2,3})_\circ^-$, где дивизор $(U_{2,3})_\circ^-$ определен в (5.4.5.6) или (5.4.5.7) в зависимости от знака m_1.

Во втором случае (5.4.5.4), вычитая из удвоенного (5.4.5.1) выражение (5.4.5.2), имеем

$$(v_1^- + v_2^-) + (v_1^+ + v_3^-) - 2\,(h)_\circ^+ \sim (2m_0 - m_1)\big((h)_\circ^- - \infty^- - \infty^+\big),$$

$$(v_2^- + v_3^-) - (h)_\circ^+ \sim (2m_0 - m_1 - 1)\big((h)_\circ^- - \infty^- - \infty^+\big). \tag{5.4.5.8}$$

Если $2m_0 > m_1 + 1$, то положим $(U_{2,3})_\circ^- = v_2^- + v_3^-$, а иначе $(U_{2,3})_\circ^- = v_2^+ + v_3^+$, тогда из (5.4.5.9) получаем

$$(U_{2,3})_\circ^- - (U_0)_\circ^- \sim (1 + |2m_0 - m_1 - 2|)\big((h)_\circ^- - \infty^- - \infty^+\big). \tag{5.4.5.9}$$

Рассуждая как в первом случае, заключаем, что по лемме 2.4.5.4 и следствию 5.4.4.5 существует многочлен $U_n = U_{2,3}$, для которого $(U_n)_\circ^- = (U_{2,3})_\circ^-$. □

Предложение 5.4.5.2. *Если образ дивизора $v_h^- - v_h^+$ в якобиане J имеет конечный порядок, то красные вершины графа G могут быть связны только с красными вершинами.*

Доказательство. Пусть в графе G есть ребро $[x_0,\ x_1]$, которому соответствует многочлен U_n, $(U_n)_\circ^- = v_0^- + v_1^-$. Так как образ дивизора $v_h^- - v_h^+$ в якобиане J имеет конечный порядок, то по теореме 5.4.4.1 дивизор $\big((h)_\circ^- - \infty^- - \infty^+\big)$ имеет конечный порядок $m \in \mathbb{N}$. По лемме 2.4.5.4 для некоторого $m_1 \in \mathbb{N}$, $m_1 < m$, имеем

$$(U_n)_\circ^- - (U_0)_\circ^- \sim m_1\big((h)_\circ^- - \infty^- - \infty^+\big). \tag{5.4.5.10}$$

Предположим, что вершина x_0 желтая, то есть $v_0 = v_0^- = v_0^+$ и $2v_0 - \infty^- - \infty^+ \sim 0$. Домножим (5.4.5.10) на m и вычтем сопряженное (5.4.5.10), домноженное на m, тогда $m(v_1^- - v_1^+) \sim 0$, то есть вершина x_1 зеленая или желтая, причем, если x_1 зеленая, то ее степень делит $\mathrm{Ord}(v_h^- - v_h^+)$.

Теперь предположим, что вершина x_0 зеленая, то есть $k(v_0^- - v_0^+) \equiv 0$, для некоторого $k \in \mathbb{N}$. Пусть q — наименьшее общее кратное чисел m и k. Домножим (5.4.5.10) на q и вычтем сопряженное (5.4.5.10), домноженное на q, тогда $q(v_1^- - v_1^+) \sim 0$, то есть вершина x_1 зеленая или желтая. □

Предложение 5.4.5.3. *Пусть образ дивизора $v_h^- - v_h^+$ в якобиане J имеет конечный порядок m.*

1. Если у вершины графа G есть петля, то эта вершина зеленая и ее степень делит $2m$.

2. Если в графе G есть ребро, соединяющее зеленую и желтую вершины, то у этой зеленой вершины есть петля.

Доказательство. 1. Пусть в графе G есть ребро $[x_0,\ x_0]$, которому соответствует многочлен U_n, $(U_n)_\circ^- = 2v_0^-$. По построениям (5.4.2.4)-(5.4.2.7) имеем $D_n = (U_n)_\circ^- = 2v_0^-$, причем D_n приведенный дивизор, поэтому вершина x_0 не может быть желтой. По лемме 2.4.5.4 для некоторого $m_1 \in \mathbb{N}$ имеем (5.4.5.10). Домножим (5.4.5.10) на m и вычтем сопряженное (5.4.5.10), домноженное на m, тогда $2m(v_0^- - v_0^+) \sim 0$, то есть вершина x_0 зеленая и ее степень делит $2m$.

2. Пусть в графе G есть ребро $[x_0,\ x_1]$, которому соответствует многочлен U_n, x_1 — зеленая, x_0 — желтая, $v_0 = v_0^- = v_0^+$ и $2v_0 - \infty^- - \infty^+ \sim 0$, $(U_n)_\circ^- = v_0 + v_1^-$. По лемме 2.4.5.4 для некоторого $m_1 \in \mathbb{N}$ имеем (5.4.5.10). Домножим (5.4.5.10) на 2, тогда

$$2v_1^- - (U_0)_\circ^- \sim (m_1 - 1)\big((h)_\circ^- - \infty^- - \infty^+\big). \tag{5.4.5.11}$$

Воспользовавшись следствием 5.4.4.5 с дивизором $D = 2v_1^-$, заключаем, что существует многочлен U_r, для которого $(U_r)_\circ^- = 2v_1^-$, то есть у вершины x_1 есть петля. □

Пример 5.4.5.4. *Приведем пример графа G, в котором три зеленые вершины соединены ребрами между собой, но не имеют петель.*

Рассмотрим

$$C:\ y^2 = (x^2 + x - 5)(x^2 + x - 1)(4x^2 + 4x + 5), \quad h = -x^2 - \frac{5}{2}x + 1.$$

Подгруппа кручения якобиана J гиперэллиптической кривой C имеет вид $\mathbb{Z}/2 + \mathbb{Z}/24$. Многочлены U_j имеют следующие рациональные корни: $x_1 = \infty$, $x_2 = -1$, $x_3 = 0$. Граф G имеет вид полного графа с тремя вершинами без петель. Так как нас сейчас интересуют только рациональные корни многочленов U_j, то нам не обязательно пояснять, что в графе G нет синих вершин, то есть на кривой C нет других рациональных точек, кроме точек, соответствующий указанным трем значениям x_j, $j = 1, 2, 3$. Вычислим порядки соответствующих образов дивизоров $v_j^- - v_j^+$ в якобиане J:

$$Ord(v_1^- - v_1^+) = 6, \quad Ord(v_2^- - v_2^+) = 12, \quad Ord(v_3^- - v_3^+) = 12.$$

Таким образом, все три вершины графа G зеленые.

Предложение 5.4.5.5. *Пусть род кривой $C: y^2 = f(x)$ равен 2 и J — ее якобиан. Пусть $h \in K[x]$, $\deg h = 2$ и образ дивизора $v_h^- - v_h^+$ в якобиане J имеет конечный порядок. Пусть $(U_0 \cdot h, V_0)$ — представление Мамфорда дивизора $2\,(h)_\circ^-$ и справедливы построения (5.4.2.4)-(5.4.2.7) для $j \in \mathbb{N}_0$. Пусть среди многочленов $U_j \in K[x]$, $j \in \mathbb{N}$, существует $U_n \in K^*$. Тогда найдется такой многочлен $V \in K[x]$, $\deg V \le 3$, такой, что элемент $\sqrt{f} + V$ имеет периодическую непрерывную дробь в $\Sigma_h((h))$.*

Доказательство. Рассмотрим полное частное $\alpha_n = (\sqrt{f} + V_n)/U_n$, непрерывная дробь которого также периодическая. Так как $U_n \in K^*$, то в качестве V можно взять V_n. □

Предложение 5.4.5.5 говорит о том, что, при наличии S_h-единицы, если у вершины $x = \infty$ есть петля, то найдется элемент вида $\sqrt{f} + V$, $V \in K[x]$, $\deg V \le 3$, имеющий периодическую непрерывную дробь в $\Sigma_h((h))$.

Пример 5.4.5.6. *Рассмотрим*

$$f = 9x^6 + 6x^5 + 49x^4 + 40x^3 + 96x^2 + 64x + 64, \quad h = x^2 + 2.$$

Разложение $\sqrt{f}$ *в* $\Sigma_h((h))$ *имеет вид*

$$\sqrt{f} = (2x+2) + (x+3)h + \dots,$$

Разложение $\sqrt{f}$ *в* $K((1/x))$ *имеет вид*

$$\sqrt{f} = 3x^3 + x^2 + \dots.$$

Набор $\left(h^2, (2x+2) + (x+3)h\right)$ *является представлением Мамфорда дивизора* $D_0 + (h)_\circ^- = 2\,(h)_\circ^-$, *а набор* $\left(h, (2x+2) + (3x+1)h\right)$ *является представлением Мамфорда дивизора* $\tilde{D}_0 + (h)_\circ^- = 2\infty^- + (h)_\circ^-$, *то есть* $\tilde{V}_0 = (2x+2) + (3x+1)h$. *Непрерывная дробь элемента* $\tilde{V}_0 - \sqrt{f}$ *имеет вид*

$$\tilde{V}_0 - \sqrt{f} = \Big[2\,(x+1)\,;\, \overline{\tfrac{1}{6}\,(x+1)\,, -2\,(x-1)\,, \tfrac{1}{4}\,(2x-1)\,, -\tfrac{4}{9}\,(x-2)\,, \tfrac{9}{8},}$$
$$\overline{\tfrac{8}{9}\,(x-2)\,, -\tfrac{3}{16}\,(x+1)\,, \tfrac{8}{3}\tfrac{x^3+3x^2+4x+8}{x^2+2}, -\tfrac{3}{16}\,(x+1)\,, \tfrac{8}{9}\,(x-2)\,,}$$
$$\overline{\tfrac{9}{8}, -\tfrac{4}{9}\,(x-2)\,, \tfrac{1}{4}\,(2x-1)\,, -2\,(x-1)\,, \tfrac{1}{6}\,(x+1)\,, 4\,(x+1)\,, -\tfrac{1}{12}\,(x-1)\,,}$$
$$\overline{6\,(2x-1)\,, -\tfrac{1}{54}\,(x-2)\,, 27, \tfrac{1}{27}\,(x-2)\,, -\tfrac{9}{2}\,(x+1)\,, \tfrac{1}{9}\tfrac{x^3+3x^2+4x+8}{x^2+2},}$$
$$\overline{-\tfrac{9}{2}\,(x+1)\,, \tfrac{1}{27}\,(x-2)\,, 27, -\tfrac{1}{54}\,(x-2)\,, 6\,(2x-1)\,, -\tfrac{1}{12}\,(x-1)\,, 4\,(x+1)}\Big].$$

Длина квазипериода равна 15, *коэффициент квазипериода* $c = 24$, *длина периода равна* 30, *степень соответствующей фундаментальной* S_h*-единицы равна* 17. *Отметим, что период данной непрерывной дроби несимметричный, однако можно его циклически сдвинуть, чтобы он стал симметричным. Для сравнения приведем непрерывную дробь элемента* $\sqrt{f}/h$:

$$\tfrac{\sqrt{f}}{h} = \Big[\tfrac{x^3+3x^2+4x+8}{x^2+2}; \overline{-\tfrac{1}{4}\,(x+1)\,, \tfrac{2}{3}\,(x-2)\,, \tfrac{3}{2}, -\tfrac{1}{3}\,(x-2)\,, \tfrac{1}{3}\,(2x-1)\,,}$$
$$\overline{-\tfrac{3}{2}\,(x-1)\,, \tfrac{2}{9}\,(x+1)\,, 3\,(x+1)\,, -\tfrac{1}{9}\,(x-1)\,, \tfrac{9}{2}\,(2x-1)\,, -\tfrac{2}{81}\,(x-2)\,,}$$
$$\overline{\tfrac{81}{4}, \tfrac{4}{81}\,(x-2)\,, -\tfrac{27}{8}\,(x+1)\,, \tfrac{4}{27}\tfrac{x^3+3x^2+4x+8}{x^2+2}, -\tfrac{27}{8}\,(x+1)\,,}$$
$$\overline{\tfrac{4}{81}\,(x-2)\,, \tfrac{81}{4}, -\tfrac{2}{81}\,(x-2)\,, \tfrac{9}{2}\,(2x-1)\,, -\tfrac{1}{9}\,(x-1)\,, 3\,(x+1)\,, \tfrac{2}{9}\,(x+1)\,,}$$
$$\overline{-\tfrac{3}{2}\,(x-1)\,, \tfrac{1}{3}\,(2x-1)\,, -\tfrac{1}{3}\,(x-2)\,, \tfrac{3}{2}, \tfrac{2}{3}\,(x-2)\,, -\tfrac{1}{4}\,(x+1)\,, \tfrac{2(x^3+3x^2+4x+8)}{x^2+2}}\Big].$$

Длина квазипериода также равна 15, *коэффициент квазипериода* $c = \frac{4}{27}$, *длина периода равна* 30.

5.4.6. Алгоритм поиска S_h-единиц

Теоремы 5.4.4.1, 5.4.4.3, 5.4.4.4 позволяют для неприводимого многочлена h второй степени сформулировать эффективный алгоритм поиска S_h-единиц и классов дивизоров конечного порядка в $\Delta^\circ(L)$. Обозначим $\Sigma_h = \{b \in K[x],\ \deg b < \deg h\}$.

Если алгоритм 7 завершился успешно, то есть был найден номер $n \in \mathbb{N}$ такой, что $U_n = U_0$ и $V_n = V_0$, то по теореме 5.4.4.3 в поле L существует фундаментальная S_h-единица. Для ее

Алгоритм 7. Алгоритм поиска S_h-единиц, $\deg h = 1$.

1: **Дано:** многочлены $h, f \in K[x]$, $2g+1 \leq \deg f \leq 2g+2$, $g \geq 2$, $\deg h = 2$, такие, что $f = c_{g+1}h^{g+1} + \ldots + c_0$, где $c_j \in \Sigma_h$, $0 \leq j \leq s_0$, $s_0 = [g/2]$, $c_{g+1} \in K$ и c_{g+1} является полным квадратом в K, $c_{g+1} = \gamma^2$, $j_0 \in \mathbb{N}$.

2: **Вычислить:**
$$\xi = \sum_{j=0}^{s_0} f_j h^j \in K[x], \quad \text{где } \sqrt{f} = \sum_{j=0}^{\infty} f_j h^j \in \Sigma_h((h));$$

3: **положить:** $U_0 = h^{s_0}$ и
$$V_0 = \begin{cases} \xi, & \text{если } g \text{ четно}, \\ \xi + \gamma h^{s_0+1}, & \text{если } g \text{ нечетно}; \end{cases}$$

4: **Цикл для** $j \in \mathbb{N}_0$, $j < j_0$, **выполнить:**

5: **вычислить:** $U_{j+1} = \frac{f - V_j^2}{U_j \cdot h}$;

6: **вычислить:** $a_{j+1} = \left[\frac{V_j + \xi}{U_{j+1}}\right]_h^-$;

7: **вычислить:** $V_{j+1} = a_{j+1} \cdot U_{j+1} - V_j$;

8: **если** $U_{j+1} = U_0$ и $V_{j+1} = V_0$, **то** успешно завершить цикл.

9: **Конец цикла**

10: **Вернуть**: $n = j+1$, $\{U_i\}_{j=0}^{j+1}$, $\{V_i\}_{j=0}^{j+1}$, $\{a_i\}_{j=0}^{j+1}$.

явного задания по (5.4.2.10) определим функции β_j. В силу (5.4.2.11) для функции
$$u = \prod_{j=0}^{n-1} \beta_j^{-1} \tag{5.4.6.1}$$
имеем $u \cdot \overline{u} = bh^m$ для некоторого $b \in K^*$. Так как $u \in L \setminus K(x)$, то функция u имеет вид $u = \mu_1 - \mu_2\sqrt{f}$, где $\mu_1, \mu_2 \in K[x]$, $v_h(\mu_2) = 0$ и имеет место равенство (5.4.4.12). Следовательно, u является фундаментальной S-единицей. Для нечетного m имеем $m_h = m$, и фундаментальную S_h-единицу u_h можно найти по формуле
$$u_h = \frac{u^2}{h^m} = \frac{(\mu_1^2 + f\mu_2^2) - 2\mu_1\mu_2\sqrt{f}}{h^m}, \tag{5.4.6.2}$$
а для четного m имеем $m_h = m/2$, и $u_h = u \cdot h^{-m_h}$.

В случае четного рода g по теоремам 5.4.3.4 и 5.4.4.4 фундаментальная S_h-единица может быть также найдена с помощью формул (5.4.4.16). Примеры 5.4.7.5 и 5.4.7.4 показывает, что для нечетного рода g мы не можем пользоваться формулами (5.4.4.16) для поиска фундаментальной S_h-единицы.

5.4.7. Новые примеры S_h-единиц

Приведем примеры гиперэллиптических полей $L = K(x)(\sqrt{f})$ таких, что для некоторого $h \in K[x]$, $\deg h = 2$, в L существуют нетривиальные S_h-единицы, но не существует нормиро-

вания первой степени v поля $K(x)$, имеющих два продолжения на поле L.

Пример 5.4.7.1. *Рассмотрим* $h = x^2 - 2$ *и*

$$f = 12x^6 - 45x^4 - 27x^3 + \frac{225x^2}{4} + 54x + 12.$$

Разложение многочлена f *в кольце* $\Sigma_h[h]$ *имеет вид*

$$f(h) = \frac{81}{2} - \left(27x - \frac{81}{4}\right) h + 27h^2 + 12h^3.$$

Разложение $\sqrt{f}$ *в поле* $\Sigma_h((h))$ *имеет вид*

$$\sqrt{f} = \frac{9x}{2} - 3h + xh^2 + \left(\frac{x}{6} + \frac{2}{3}\right) h^3 + \dots.$$

Непрерывная дробь $\sqrt{f}/h$ *типа* (5.4.2.18) *имеет вид:*

$$\left[-\tfrac{6x^2-9x-12}{2x^2-4};\ \overline{\tfrac{x}{2},\ -3\,(x-1)\,,\ x+2,\ -\tfrac{1}{4}\,(3x-6)\,,\ -4,}\right.$$
$$\overline{-\tfrac{3}{4},\ -4\,(x-2)\,,\ \tfrac{1}{16}\,(3x+6)\,,\ -16\,(x-1)\,,\ \tfrac{3x}{32},\ -\tfrac{1}{x^2-2}\,(32x^2-48x-64)\,,}$$
$$\overline{\tfrac{3x}{32},\ -16\,(x-1)\,,\ \tfrac{1}{16}\,(3x+6)\,,\ -4\,(x-2)\,,\ -\tfrac{3}{4},\ -4,}$$
$$\left.\overline{-\tfrac{1}{4}\,(3x-6)\,,\ x+2,\ -3\,(x-1)\,,\ \tfrac{x}{2},\ -\tfrac{1}{x^2-2}\,(6x^2-9x-12)}\right].$$

Длина квазипериода равна 11, *коэффициент квазипериода* $c = \frac{3}{16}$, *длина периода равна* 22, *период симметричен, степень соответствующей фундаментальной* S*-единицы равна* 13. *Фундаментальная* S*-единица имеет вид* $u = \omega_1 + \omega_2\sqrt{f}$, *где*

$$\omega_1 = \tfrac{6561x}{16} - \tfrac{2187}{4} + \left(\tfrac{22599x}{32}h - \tfrac{9477}{8}\right) + \left(\tfrac{43011x}{64} - \tfrac{18225}{16}\right) h^2 +$$
$$+ \left(\tfrac{41877x}{128} - \tfrac{21951}{32}\right) h^3 + \left(\tfrac{3375x}{32} - \tfrac{1917}{8}\right) h^4 + \left(\tfrac{63x}{4} - \tfrac{189}{4}\right) h^5 + \left(\tfrac{3x}{4} - \tfrac{9}{2}\right) h^6,$$

$$\omega_2 = -\tfrac{243x}{4} + \tfrac{729}{8} - \left(\tfrac{567x}{8} - \tfrac{1863}{16}\right) h - \left(\tfrac{621x}{16} - \tfrac{2619}{32}\right) h^2 -$$
$$- \left(\tfrac{369x}{32} - \tfrac{1701}{64}\right) h^3 + \left(\tfrac{9x}{8} - \tfrac{75}{16}\right) h^4 + \tfrac{1}{4}h^5.$$

Имеем $u \cdot \overline{u} = -\frac{3}{16}\,(x^2-2)^{13}$. *Степень фундаментальной* S_h*-единицы равна* 13. *Фундаментальная* S_h*-единица имеет вид*

$$u_h = \frac{\omega_1^2 + \omega_2^2 f + 2\omega_1\omega_2\sqrt{f}}{h^{13}}.$$

Гиперэллиптическая кривая $C:\ y^2 = f(x)$ *не имеет рациональных точек с высотой менее* 10^5. *Значит, в поле* $K(x)$ *нет нормирований первой степени с малой высотой, имеющих два продолжения на поле* $L = K(x)(\sqrt{f})$. *Отсюда следует, что в поле* $L = K(x)(\sqrt{f})$ *не может быть нетривиальных* S_v*-единиц с малой высотой, где* $S_v = \{v^-, v^+\}$, $v^- \neq v^+$.

Пример 5.4.7.2. *Рассмотрим* $h = x^2 - 7$ *и*

$$f = 3x^6 - 12x^5 - 92x^4 - 16x^3 + 495x^2 + 764x + 478.$$

Разложение многочлена f в кольце $\Sigma_h[h]$ имеет вид

$$f(h) = 64x + 464 - (184x + 352)\,h - (12x + 29)\,h^2 + 3h^3.$$

Разложение $\sqrt{f}$ в поле $\Sigma_h((h))$ имеет вид

$$\sqrt{f} = 8x + 4 - (3x + 10)\,h - (x + 4)\,h^2 - \left(\frac{5x}{6} + \frac{7}{3}\right)h^3 + \dots.$$

Непрерывная дробь $\sqrt{f}/h$ типа (5.4.2.18) имеет вид:

$$\Big[-\tfrac{1}{x^2-7}\,(x+2)\,(3x^2+4x-37)\,;\ \overline{\tfrac{1}{9}\,(x-4)\,,\ 18\,(x-2)\,,\ -\tfrac{1}{27}\,(x+2)\,,}$$
$$\overline{-18\,(x-4)\,,\ -\tfrac{1}{9},\ 18\,(x-1)\,,\ -\tfrac{1}{27}\,(x-1)\,,\ 54,\ \tfrac{1}{27}\,(x-4)\,,\ 18\,(x+2)\,,}$$
$$\overline{-\tfrac{1}{27}\,(x-2)\,,\ -54\,(x-4)\,,\ \tfrac{1}{243x^2-1701}\,(x+2)\,(3x^2+4x-37)\,,\ -54\,(x-4)\,,}$$
$$\overline{-\tfrac{1}{27}\,(x-2)\,,\ 18\,(x+2)\,,\ \tfrac{1}{27}\,(x-4)\,,\ 54,\ -\tfrac{1}{27}\,(x-1)\,,\ 18\,(x-1)\,,\ -\tfrac{1}{9},\ -18\,(x-4)\,,}$$
$$\overline{-\tfrac{1}{27}\,(x+2)\,,\ 18\,(x-2)\,,\ \tfrac{1}{9}\,(x-4)\,,\ -\tfrac{2}{x^2-7}\,(x+2)\,(3x^2+4x-37)}\Big]\,.$$

Длина квазипериода равна 13*, коэффициент квазипериода* $c = -486$*, длина периода равна* 26*, период симметричен, степень соответствующей фундаментальной S-единицы равна* 15*. Фундаментальная S-единица имеет вид* $u = \omega_1 + \omega_2\sqrt{f}$*, где*

$$\omega_1 = 5385728x - 14234624 + h\,(4095232x - 11923712) + h^2\,(2013984x - 5933632) +$$
$$+h^3\,(547312x - 1921888) + h^4\,(125248x - 373472) + h^5\,(11676x - 58600) +$$
$$+h^6\,(1062x - 4956) + h^7\,(27x - 126)\,,$$

$$\omega_2 = -313472x + 829952 - h\,(174528x - 518560) - h^2\,(65408x - 207760) +$$
$$-h^3\,(13328x - 43808) - h^4\,(1464x - 6916) - h^5\,(108x - 414) + 9h^6$$

$$u \cdot \overline{u} = 486\left(x^2 - 7\right)^{15}.$$

Степень фундаментальной S_h-единицы равна 15*. Фундаментальная S_h-единица имеет вид*

$$u_h = \frac{\omega_1^2 + \omega_2^2 f + 2\omega_1\omega_2\sqrt{f}}{h^{15}}.$$

Гиперэллиптическая кривая $C: \ y^2 = f(x)$ не имеет рациональных точек с высотой менее 10^5. Значит, в поле $K(x)$ нет нормирований первой степени с малой высотой, имеющих два продолжения на поле $L = K(x)(\sqrt{f})$. Отсюда следует, что в поле $L = K(x)(\sqrt{f})$ не может быть нетривиальных S_v-единиц с малой высотой, где $S_v = \{v^-, v^+\}$, $v^- \neq v^+$.

Пример 5.4.7.3. *Рассмотрим $h = x^2 - 7$ и*

$$f = 5x^6 + 2x^5 - 109x^4 - 32x^3 + \frac{3137x^2}{4} + 128x - 1858 =$$
$$= \frac{1}{4}\left(x^2 - 8\right)\left(20x^4 + 8x^3 - 276x^2 - 64x + 929\right).$$

Разложение многочлена f в кольце $\Sigma_h[h]$ имеет вид

$$f(h) = 2x + \frac{23}{4} - \left(4x + \frac{27}{4}\right) h + (2x-4)\, h^2 + 5h^3.$$

Разложение $\sqrt{f}$ в поле $\Sigma_h((h))$ имеет вид

$$\sqrt{f} = \frac{x}{2} + 2 - xh + (2x-6)\, h^2 - \left(\frac{26x}{3} - \frac{68}{3}\right) h^3 + \dots.$$

Непрерывная дробь $\sqrt{f}/h$ типа (5.4.2.18) имеет вид:

$$\Big[-\tfrac{2x^3-15x-4}{2x^2-14};\ \overline{-\tfrac{1}{4}(x+3),\ -\tfrac{1}{7}(4x+28),\ -\tfrac{1}{48}(14x+49),\ -\tfrac{1}{49}(48x+192),}$$
$$\overline{-\tfrac{49}{144},\ \tfrac{1}{49}(36x+36),\ -\tfrac{1}{324}(49x+245),\ -\tfrac{1}{98}(81x+324),\ -\tfrac{1}{729}(196x+784),}$$
$$\overline{-\tfrac{1}{98}(81x+324),\ -\tfrac{1}{324}(49x+245),\ \tfrac{1}{49}(36x+36),\ -\tfrac{49}{144},\ -\tfrac{1}{49}(48x+192),}$$
$$\overline{-\tfrac{1}{48}(14x+49),\ -\tfrac{1}{7}(4x+28),\ -\tfrac{1}{4}(x+3),\ -\tfrac{1}{x^2-7}(2x^3-15x-4)}\Big].$$

Длина периода совпадает с длиной квазипериода и равна 18*, период симметричен, степень соответствующей фундаментальной S-единицы равна* 20*. Фундаментальная S-единица имеет вид $u = \omega_1 + \omega_2\sqrt{f}$, где*

$$\omega_1 = -\tfrac{2479259x}{8} - \tfrac{26238011}{32} + h\left(\tfrac{1442913x}{4} + \tfrac{3583321}{4}\right) + h^2\left(\tfrac{1478839x}{4} + \tfrac{16774767}{16}\right) +$$
$$-h^3\left(\tfrac{610229x}{2} + \tfrac{5919783}{8}\right) - h^4\left(\tfrac{2076655x}{8} + \tfrac{23896315}{32}\right) + h^5\left(\tfrac{163013x}{4} + \tfrac{487863}{8}\right) +$$
$$+h^6\left(\tfrac{153869x}{2} + 212836\right) + h^7\left(23582x + \tfrac{153093}{2}\right) + h^8(2792x + 11362) +$$
$$+h^9(104x + 682) + 9h^{10},$$

$$\omega_2 = -\tfrac{1492237x}{16} - \tfrac{493511}{2} + h\left(\tfrac{591225x}{16} + \tfrac{320557}{4}\right) + h^2\left(\tfrac{1829571x}{16} + \tfrac{620299}{2}\right) +$$
$$+h^3\left(\tfrac{150535x}{16} + \tfrac{92415}{2}\right) - h^4\left(\tfrac{336945x}{8} + \tfrac{220815}{2}\right) - h^5\left(\tfrac{84417x}{4} + \tfrac{255243}{4}\right) +$$
$$-h^6\left(3949x + \tfrac{28317}{2}\right) - h^7(282x + 1374) - h^8(4x + 46),$$

Имеем $u\cdot\overline{u} = (x^2-7)^{20}$. Степень фундаментальной S_h-единицы равна 10*. Фундаментальная S_h-единица имеет вид*

$$u_h = \frac{\omega_1 + \omega_2\sqrt{f}}{h^{10}}.$$

Гиперэллиптическая кривая $C: \ y^2 = f(x)$ не имеет рациональных точек с высотой менее 10^5. Значит, в поле $K(x)$ нет нормирований первой степени с малой высотой, имеющих два продолжения на поле $L = K(x)(\sqrt{f})$. Отсюда следует, что в поле $L = K(x)(\sqrt{f})$ не может быть нетривиальных S_v-единиц с малой высотой, где $S_v = \{v^-, v^+\}$, $v^- \neq v^+$.

Приведем пример к теореме 5.4.4.1 для гиперэллиптического поля $L = \mathbb{Q}(x)(\sqrt{f})$ с нечетным родом g. В статье [16] подробно разобран алгоритм для случая $K = \mathbb{Q}$ и $g = 3$, а также приведены соответствующие примеры для $\deg f = 7$. Далее приведены примеры для $\deg f = 8$.

Пример 5.4.7.4. *Рассмотрим поле* $K=\mathbb{Q}$, *многочлены* $h=x^2+2$ *и*

$$f=x^8+4x^6+2x^5+4x^4+12x^3+x^2+16x=$$
$$=x\left(x^7+4x^5+2x^4+4x^3+12x^2+x+16\right).$$

Нормирование v_h *поля* $\mathbb{Q}(x)$ *имеет два неэквивалентных продолжения* v_h^- *и* v_h^+ *на поле* $L=\mathbb{Q}(x)(\sqrt{f})$. *Элемент* $\sqrt{f}$ *имеет следующее разложение в* $\Sigma_h((h))$

$$\sqrt{f}=x+2\cdot h+\dots$$

Бесконечное нормирование v_∞ *поля* $\mathbb{Q}(x)$ *имеет два продолжения* v_∞^- *и* v_∞^+ *на поле* $L=\mathbb{Q}(x)(\sqrt{f})$. *Рассмотрим* $D_0=(h)_\circ^-+v_\infty^-$. *Находим* $\gamma=1$ *и*

$$U_0=h,\quad V_0=x+2\cdot h+1\cdot h^2=x^4+6x^2+x+8.$$

Далее по нормированию v_h^- *строим непрерывную дробь для элемента* $\alpha=\alpha_0$ *вида* (5.4.2.17):

$$\alpha=\Bigg[\frac{2\left(2x^2+x+4\right)}{x^2+2};\overline{-\frac{2x^2+x+4}{4(x^2+2)},-4,-\frac{x}{8},\frac{8(x^3+2x-1)}{x^2+2},-\frac{x}{8},-4,}$$
$$\overline{-\frac{2x^2+x+4}{4(x^2+2)},\frac{2(2x^2+x+4)}{x^2+2},\frac{1}{2},x,-\frac{x^3+2x-1}{x^2+2},x,\frac{1}{2},\frac{2(2x^2+x+4)}{x^2+2}}\Bigg].$$

Непрерывная дробь элемента α *чисто периодическая, причем длина квазипериода равна* 7, *а длина периода равна* 14, *коэффициент квазипериода* $c=-1/8$. *Легко видеть, что период несимметричен. Замечаем, что* $U_7=-8U_0$ *и* $V_7=V_0$, *поэтому справедливы условия теоремы* 5.4.4.1 *и, следовательно, в якобиане гиперэллиптического поля* L *класс дивизора* $\left((h)_\circ^--\infty^--\infty^+\right)$ *имеет порядок* $m=13$, *класс дивизора* $\left((h)_\circ^--(h)_\circ^+\right)$ *также имеет порядок* $m=13$. *В поле* L *существует фундаментальная* S*-единица и степени* 13, *которую можно найти с помощью формулы* (5.4.6.1):

$$u=\mu_1-\mu_2\sqrt{f},\qquad u\cdot\overline{u}=32h^{13}$$
$$\mu_1=9x^{13}+96x^{11}-21x^{10}+432x^9-122x^8+1139x^7-124x^6+$$
$$+1990x^5+425x^4+2144x^3+960x^2+1024x+512,$$
$$\mu_2=7x^9+50x^7-34x^6+108x^5-208x^4+55x^3-408x^2-32x-256.$$

Также в поле L *существует фундаментальная* S_h*-единица* u_h *степени* 13, *которую можно найти с помощью формулы* (5.4.6.2).

Пример 5.4.7.5. *Рассмотрим поле* $K=\mathbb{Q}$, *многочлены* $h=x^2+2$ *и*

$$f=x^8+4x^6-2x^5+4x^4-8x^3+x^2-4x+4=$$
$$=(x-1)\left(x^2+x+1\right)\left(x^2+x+2\right)\left(x^3-x^2+3x-2\right).$$

Нормирование v_h *поля* $\mathbb{Q}(x)$ *имеет два неэквивалентных продолжения* v_h^- *и* v_h^+ *на поле* $L=\mathbb{Q}(x)(\sqrt{f})$. *Элемент* $\sqrt{f}$ *имеет следующее разложение в* $\Sigma_h((h))$

$$\sqrt{f}=(x+2)+0\cdot h+\dots$$

Бесконечное нормирование v_∞ *поля* $\mathbb{Q}(x)$ *имеет два продолжения* v_∞^- *и* v_∞^+ *на поле* $L = \mathbb{Q}(x)(\sqrt{f})$. *Рассмотрим* $D_0 = (h)_\circ^- + v_\infty^-$. *Находим* $\gamma = 1$ *и*

$$U_0 = h, \quad V_0 = x + 2 + 0 \cdot h + 1 \cdot h^2 = x^4 + 4x^2 + 4.$$

Далее по нормированию v_h^- *строим непрерывную дробь для элемента* $\alpha = \alpha_0$ *вида* (5.4.2.17):

$$\alpha = \Big[\tfrac{2(x+2)}{x^2+2}; \overline{\tfrac{1}{2}(x-1), -2, -\tfrac{1}{2}(x+2), 2, \tfrac{1}{4}(x+2), -\tfrac{4}{3}(x+2), \tfrac{3}{8}(x-2),}$$
$$\overline{-\tfrac{4}{3}(x+2), \tfrac{1}{4}(x+2), 2, -\tfrac{1}{2}(x+2), -2, \tfrac{1}{2}(x-1), \tfrac{2(x+2)}{x^2+2}, \tfrac{1}{4}(x+2),}$$
$$\overline{-\tfrac{4}{3}(x-2), -\tfrac{3}{8}(x-4), \tfrac{8}{9}, \tfrac{9}{8}(x-1), \tfrac{8}{9}, -\tfrac{3}{8}(x-4), -\tfrac{4}{3}(x-2), \tfrac{1}{4}(x+2), \tfrac{2(x+2)}{x^2+2}}\Big].$$

Непрерывная дробь элемента α *чисто периодическая, причем длина периода равна длине квазипериода и равна* 24. *Замечаем, что* $U_{24} = U_0$ *и* $V_{24} = V_0$, *поэтому справедливы условия теоремы* 5.4.4.1 *и, следовательно, в якобиане гиперэллиптического поля* L *класс дивизора* $\left((h)_\circ^- - \infty^- - \infty^+\right)$ *имеет порядок* $m = 28$, *а класс дивизора* $\left((h)_\circ^- - (h)_\circ^+\right)$ *имеет порядок* $m/2 = 14$. *В поле* L *существует фундаментальная* S*-единица и степени* 28, *которую можно найти с помощью формулы* (5.4.6.1):

$$u = \mu_1 - \mu_2\sqrt{f}, \qquad u \cdot \overline{u} = 4h^{28}$$
$$\mu_1 = 2x^{28} + 105x^{26} + 63x^{25} + 2129x^{24} + 1921x^{23} + 24180x^{22} + 25106x^{21} +$$
$$+176820x^{20} + 185928x^{19} + 883503x^{18} + 856127x^{17} + 3071523x^{16} +$$
$$+2474217x^{15} + 7330613x^{14} + 4047683x^{13} + 11362865x^{12} + 1569801x^{11} +$$
$$+9732754x^{10} - 7785790x^9 + 1772905x^8 - 16768251x^7 - 2723078x^6 -$$
$$-13762572x^5 + 1843336x^4 - 3146128x^3 + 5244384x^2 + 1048512x + 2097280,$$
$$\mu_2 = \left(7x^{10} + 8x^9 + 93x^8 + 115x^7 + 511x^6 + 573x^5 + 1441x^4 + 1237x^3 +\right.$$
$$\left.+1998x^2 + 1020x + 1016\right)\left(2x^{13} - x^{12} + 39x^{11} - 2x^{10} + 276x^9 +\right.$$
$$\left.+43x^8 + 959x^7 + 141x^6 + 1717x^5 - 180x^4 + 1291x^3 - 1070x^2 + 4x - 1032\right).$$

Также в поле L *существует фундаментальная* S_h*-единица* u_h *степени* 14, $u_h = u \cdot h^{-14}$.

Приведем контрпример к теореме 5.4.4.4 для гиперэллиптического поля $L = \mathbb{Q}(x)(\sqrt{f})$ с нечетным родом g. Более точно, мы рассмотрим пример гиперэллиптического поля $L = \mathbb{Q}(x)(\sqrt{f})$ рода 3 и многочлена $h \in \mathbb{Q}[x]$, $\deg h = 2$, таких, что в теореме 5.4.4.1 для некоторого $n \in \mathbb{N}$ справедливо равенство $U_0 = U_n$, однако $V_0 \neq V_n$. Если показать, что в этом примере ни для каких $n \in \mathbb{N}$ и $c \in \mathbb{Q}^*$ не справедливы одновременно равенства $U_0 = cU_n$ и $V_0 = V_n$, то в якобиане гиперэллиптического поля L классы дивизоров $\left((h)_\circ^- - \infty^- - \infty^+\right)$ и $\left((h)_\circ^- - (h)_\circ^+\right)$ имеют бесконечный порядок.

Пример 5.4.7.6. *Рассмотрим поле* $K = \mathbb{Q}$, *многочлены* $h = x^2 + 1$ *и*

$$f = x^8 + x^7 + 3x^6 + 3x^5 + 4x^4 + x^3 + 2x^2 + x = \\ = x\left(x^3 + 2x + 1\right)\left(x^4 + x^3 + x^2 + 1\right).$$

Нормирование v_h *поля* $\mathbb{Q}(x)$ *имеет два неэквивалентных продолжения* v_h^- *и* v_h^+ *на поле* $L = \mathbb{Q}(x)(\sqrt{f})$. *Элемент* $\sqrt{f}$ *имеет следующее разложение в* $\Sigma_h((h))$

$$\sqrt{f} = (1 + x) + (-1) \cdot h + \ldots$$

Бесконечное нормирование поля $\mathbb{Q}(x)$ *имеет два неэквивалентных продолжения на поле* $L = \mathbb{Q}(x)(\sqrt{f})$. *Рассмотрим* $D_0 = (h)_\circ^- + \infty^-$. *Находим* $\gamma = 1$ *и*

$$U_0 = h, \quad V_0 = (1 + x) + (-1) \cdot h + 1 \cdot h^2 = x^4 + x^2 + x + 1.$$

Далее строим непрерывную дробь для элемента $\sqrt{f}/h$ *по нормированию* v_h^-:

$$\frac{\sqrt{f}}{h} = \Big[-\tfrac{x(x-1)}{x^2+1};\ -1, 2x, -x, x-1, x-1, \tfrac{2x}{x^2+1}, -x+1, x-1, -1, 2, -1, \\ x-1, -x+1, \tfrac{2x}{x^2+1}, x-1, x-1, -x, 2x, -1, -\tfrac{2x(x-1)}{x^2+1}, 1, 2x, \\ -\tfrac{1}{5}(x+2), 5(x+3), \tfrac{1}{25}(x-1), -\tfrac{25}{2}, -\tfrac{8x}{25}, \tfrac{25}{2}, -\tfrac{1}{25}(x-1), \\ \tfrac{25}{13}(x-5), \tfrac{13}{125}(8x+1), -\tfrac{250}{2197}(4x+7), -\tfrac{2197}{18125}(16x+11), \\ \tfrac{725}{28561}(33x+19), -\tfrac{28561}{862025}(33x+31), \tfrac{34481}{57122}(4x-5), -\tfrac{228488x}{1413721}, \\ -\tfrac{34481}{57122}(4x-5), \tfrac{28561}{862025}(33x+31), \tfrac{21025}{1056757}(x+43), -\tfrac{1056757}{76215625}(73x+6), \ldots\Big].$$

Отметим, что первая часть непрерывной дроби

$$\frac{\sqrt{f}}{h} = \Big[-\tfrac{x(x-1)}{x^2+1};\ -1, 2x, -x, x-1, x-1, \tfrac{2x}{x^2+1}, -x+1, x-1, -1, 2, -1, \\ x-1, -x+1, \tfrac{2x}{x^2+1}, x-1, x-1, -x, 2x, -1, -\tfrac{2x(x-1)}{x^2+1}, \ldots\Big]$$

симетрична и очень похожа на период, так как $U_0 = U_{23} = h$. *Однако* $V_{23} = -x^4 - 3x^2 + x - 1 \neq V_0 = V_{22}$, *то есть условия теоремы 5.4.4.1 для* $n = 23$ *не выполнены. Вычисления показывают, что при* $n > 23$ *коэффициенты многочленов* U_n *и* V_n *растут, и, по-видимому, не существует номера* $n > 23$, *для которого* $V_0 = V_n$.

В данном примере мы не можем пользоваться формулами (5.4.3.14), а также предложением 5.4.3.6, так как g *нечетно. Также отметим, что элемент* α_0 *не будет иметь вид (5.4.3.15), а формулы (5.4.3.13), определяющие* A_j *и* B_j, *должны быть изменены соответствующим образом для случая нечетного* g.

Заключение

В диссертационной работе представлено решение актуальных проблем в области алгебраической теории чисел и арифметической геометрии. Нами изучено строение и свойства гиперэллиптических кривых и гиперэллиптических полей, а также связанных с ними теоретико-числовых, алгебраических и геометрических объектов таких, как функциональные непрерывные дроби, функциональные аналоги уравнений Пелля, фундаментальные единицы и S-единицы, якобиевы многообразия, группы классов дивизоров и их подгруппы кручения. Отдельное внимание уделено изучению связей и зависимостей между этими объектами и их ключевыми свойствами. Приведенные объекты рассматривались как над произвольными полями K характеристики, отличной от 2, так и в отдельных случаях над полем рациональных чисел $\mathbb{Q}$ или над полями алгебраических чисел, являющимися конечными расширениями поля $\mathbb{Q}$.

В ходе исследования были использованы как традиционные методы алгебраической теории чисел, классических направлений алгебры и арифметической геометрии, так и возникшие недавно (в том числе в работах автора) новые арифметические методы из теории функциональных непрерывных дробей, теории единиц колец целых или S-целых элементов гиперэллиптических полей, теории дивизоров гиперэллиптических кривых. Ряд результатов получен с использованием систем компьютерной алгебры и символьных компьютерных вычислений.

Основные результаты диссертационной работы заключаются в следующем:

1. найдены точные оценки на длины периодов функциональных непрерывных дробей элементов гиперэллиптического поля, определенного над полем алгебраических чисел;

2. решена проблема классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условием, что поле L определено над полем рациональных чисел;

3. решена проблема классификации эллиптических полей L по принципу периодичности непрерывных дробей ключевых элементов с условиями, что поле L определено над квадратичным расширением поля рациональных чисел, а соответствующая эллиптическая кривая входит в рациональную параметризацию модулярными кривыми;

4. разработана теория функциональных непрерывных дробей обобщенного типа для нормирования первой степени, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

5. разработана теория функциональных непрерывных дробей обобщенного типа для двух несопряженных линейных нормирований, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S;

6. разработана теория функциональных непрерывных дробей обобщенного типа для нормирования второй степени, доказан критерий периодичности функциональных непрерывных дробей обобщенного типа и сформулирован эффективный алгоритм поиска и построения фундаментальных S-единиц для соответствующего множества нормирований S.

Результаты диссертации могут быть использованы в таких теоретических разделах математики, как алгебраическая теория чисел, алгебраическая геометрия, арифметическая геометрия, а также в области защиты информации и в прикладных разделах вычислительной математики.

Публикации автора по теме диссертации

Статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ имени М.В. Ломоносова по специальности 1.1.5 — «Математическая логика, алгебра, теория чисел и дискретная математика»

1. *Платонов В. П.*, *Федоров Г. В.* Непрерывные дроби в гиперэллиптических полях со сколь угодно большой длиной периода // Докл. РАН. Матем., информ., проц. упр. — 2024. — Т. 516. — С. 59—64. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.863 (2023); *Platonov V. P., Fedorov G. V.* Continued fractions in hyperelliptic fields with an arbitrarily large period length // Dokl. Math. — 2024. — Vol. 109, no. 2. — P. 147—151. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.5 (2023), SJR 0.458(2023). Вклад авторов равноценный и неделимый (50%/50%). 0,375 печ. л.

2. *Федоров Г. В.* О последовательностях многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь // Вестн. Моск. ун-та. Сер. 1 Математика. Механика. — 2024. — № 2. — С. 25—30. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.396 (2023); *Fedorov G. V.* On sequences of polynomials f with periodic expansion of $\sqrt{f}$ into continued fractions // Moscow University Mathematics Bulletin. — 2024. — no. 2. — P. 98–102. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.2 (2023), SJR 0.344 (2023). 0,375 печ. л.

3. *Федоров Г. В.* Об оценках длин периодов функциональных непрерывных дробей над алгебраическими числовыми полями // Чебышевский сб. — 2023. — Т. 24, № 3. — С. 162—189. — Журнал индексируется в РИНЦ, Scopus. Импакт фактор: РИНЦ 0.498 (2021), SJR 0.296 (2023). 1,75 печ. л.

4. *Федоров Г. В.* Непрерывные дроби и проблема классификации эллиптических полей над квадратичными полями констант // Матем. заметки. — 2023. — Т. 114, № 6. — С. 873—893. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.796 (2023); *Fedorov G. V.* Continued Fractions and the Classification Problem for Elliptic Fields Over Quadratic Fields of Constants // Math. Notes. — 2023. — Vol. 114, no. 6. — P. 1203–1219. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.6 (2023), SJR 0.418 (2023). 1,3125 печ. л.

5. *Федоров Г. В.* О проблеме описания элементов эллиптических полей с периодическим разложением в непрерывную дробь над квадратичными полями констант // Докл. РАН. Матем., информ., проц. упр. — 2022. — Т. 505. — С. 56—62. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: 0.943(2022); *Fedorov G. V.* On the problem of describing elements of elliptic fields with a periodic expansion into a continued fraction over quadratic fields // Dokl. Math. — 2022. — Vol. 106, no. 1. — P. 259–264. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.6 (2022), SJR 0.444 (2022). 0,4375 печ. л.

6. *Platonov V. P.*, *Fedorov G. V.* Periodicity Criterion for Continued Fractions of Key Elements in Hyperelliptic Fields // Dokl. Math. — 2022. — С. 262—269. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.6 (2022), SJR 0.444 (2022). The contribution of the authors is equal and indivisible (50%/50%). 0,5 печ. л.

7. *Федоров Г. В.* О фундаментальных S-единицах и непрерывных дробях, построенных в гиперэллиптических полях по двум линейным нормированиям // Докл. РАН. Матем., информ., проц. упр. — 2021. — Т. 498. — С. 65—70. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.556 (2021); *Fedorov G. V.* On fundamental S-units and continued fractions constructed in hyperelliptic fields using two linear valuations // Dokl. Math. — 2021. — Vol. 103, no. 3. — P. 151–156. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.486 (2021), SJR 0.385 (2021). 0,375 печ. л.

8. *Платонов В. П.*, *Федоров Г. В.* О проблеме классификации многочленов f с периодическим разложением $\sqrt{f}$ в непрерывную дробь в гиперэллиптических полях // Изв. РАН. Сер. матем. — 2021. — Т. 85, № 5. — С. 152—189. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.804 (2021); *Platonov V. P., Fedorov G. V.* On the classification problem for polynomials f with a periodic continued fraction expansion of $\sqrt{f}$ in hyperelliptic fields // Izv. Math. — 2021. — Vol. 85, no. 5. — P. 972–1007. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.978 (2021), SJR 0.726 (2021). Вклад авторов равноценный и неделимый (50%/50%). 2,375 печ. л.

9. *Федоров Г. В.* О семействах гиперэллиптических кривых над полем рациональных чисел, якобианы которых содержат точки кручения данных порядков // Чебышевский сб. — 2020. — Т. 21, № 1. — С. 322—340. — Журнал индексируется в РИНЦ, Scopus. Импакт фактор: РИНЦ 0.450 (2020), SJR 0.273 (2020). 1,1875 печ. л.

10. *Федоров Г. В.* О длине периода функциональной непрерывной дроби над числовым полем // Докл. РАН. Матем., информ., проц. упр. — 2020. — Т. 495. — С. 78—81. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.904 (2019); *Fedorov G. V.* On the period length of a functional continued fraction over a number field

// Dokl. Math. — 2020. — Vol. 102, no. 3. — P. 513–517. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.619 (2020), SJR 0.765 (2020). 0,25 печ. л.

11. *Федоров Г. В.* Об S-единицах для нормирований второй степени в гиперэллиптических полях // Изв. РАН. Сер. матем. — 2020. — Т. 84, № 2. — С. 197—242. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.958 (2020); *Fedorov G. V.* On S-units for valuations of the second degree in hyperelliptic fields // Izv. Math. — 2020. — Vol. 84, no. 2. — P. 392–435. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 1.189 (2020), SJR 1.057 (2020). 2,875 печ. л.

12. *Платонов В. П.*, *Федоров Г. В.* О проблеме классификации периодических непрерывных дробей в гиперэллиптических полях // Успехи математических наук. — 2020. — Т. 75, 4(454). — С. 211—212. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 1.250 (2020); *Platonov V. P., Fedorov G. V.* On the problem of classification of periodic continued fractions in hyperelliptic fields // Russian Math. Surveys. — 2020. — Vol. 75, no. 4. — P. 785–787. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 1.909 (2020), SJR 0.891 (2020). Вклад авторов равноценный и неделимый (50%/50%). 0,125 печ. л.

13. *Федоров Г. В.* Об ограниченности длин периодов непрерывных дробей ключевых элементов гиперэллиптических полей над полем рациональных чисел // Чебышевский сб. — 2019. — Т. 20, № 4. — С. 357—370. — Журнал индексируется в РИНЦ, Scopus. Импакт фактор: РИНЦ 0.599 (2019), SJR 0.236 (2019). 0,875 печ. л.

14. *Платонов В. П.*, *Федоров Г. В.* Критерий периодичности непрерывных дробей ключевых элементов гиперэллиптических полей // Чебышевский сб. — 2019. — Т. 20, № 1. — С. 248—260. — Журнал индексируется в РИНЦ, Scopus. Импакт фактор: РИНЦ 0.599 (2019), SJR 0.236 (2019). Вклад авторов равноценный и неделимый (50%/50%). 0,75 печ. л.

15. *Платонов В. П.*, *Федоров Г. В.* S-единицы для линейных нормирований и периодичность непрерывных дробей обобщенного типа в гиперэллиптических полях // Докл. РАН. — 2019. — Т. 486, № 3. — С. 280—286. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.904 (2019); *Platonov V. P., Fedorov G. V.* On S-units for linear valuations and the periodicity of continued fractions of generalized type in hyperelliptic fields // Dokl. Math. — 2019. — Vol. 99, no. 3. — P. 277–281. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.548 (2019), SJR 0.607 (2019). Вклад авторов равноценный и неделимый (50%/50%). 0,4375 печ. л.

16. *Федоров Г. В.* Периодические непрерывные дроби и S-единицы с нормированиями второй степени в гиперэллиптических полях // Чебышевский сб. — 2018. — Т. 19, № 3. — С. 282—297. — Журнал индексируется в РИНЦ, Scopus. Импакт фактор: РИНЦ 0.572 (2018), SJR 0.187 (2018). 1,0 печ. л.

17. *Платонов В. П.*, *Федоров Г. В.* О проблеме периодичности непрерывных дробей в гиперэллиптических полях // Матем. сб. — 2018. — Т. 209, № 4. — С. 54—94. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 1.165 (2018); *Platonov V. P., Fedorov G. V.* On the problem of periodicity of continued fractions in hyperelliptic fields // Sb. Math. — 2018. — Vol. 209, no. 4. — P. 519–559. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: SJR 1.158(2020), JCR 1.274(2021). Вклад авторов равноценный и неделимый (50%/50%). 2,5625 печ. л.

18. *Платонов В. П.*, *Федоров Г. В.* О периодичности непрерывных дробей в эллиптических полях // Докл. РАН. — 2017. — Т. 475, № 2. — С. 133—136. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.869 (2017); *Platonov V. P., Fedorov G. V.* On the periodicity of continued fractions in elliptic fields // Dokl. Math. — 2017. — Vol. 96, no. 1. — P. 332–335. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.534 (2017), SJR 0.427 (2017). Вклад авторов равноценный и неделимый (50%/50%). 0,25 печ. л.

19. *Платонов В. П.*, *Федоров Г. В.* О периодичности непрерывных дробей в гиперэллиптических полях // Докл. РАН. — 2017. — Т. 474, № 5. — С. 540—544. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.869 (2017); *Platonov V. P., Fedorov G. V.* On the periodicity of continued fractions in hyperelliptic fields // Dokl. Math. — 2017. — Vol. 95, no. 3. — P. 254–258. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.534 (2017), SJR 0.427 (2017). Вклад авторов равноценный и неделимый (50%/50%). 0,3125 печ. л.

20. *Платонов В. П.*, *Федоров Г. В.* S-единицы и периодичность непрерывных дробей в гиперэллиптических полях // Докл. РАН. — 2015. — Т. 465, № 5. — С. 537—541. — Журнал индексируется в РИНЦ, Scopus, WoS. Импакт фактор: РИНЦ 0.831 (2015); *Platonov V. P., Fedorov G. V.* S-units and periodicity of continued fractions in hyperelliptic fields // Dokl. Math. — 2015. — Vol. 92, no. 3. — P. 752–756. — The journal is indexed in RSCI, Scopus, WoS. Impact factor: JIF 0.445 (2015), SJR 0.358 (2015). Вклад авторов равноценный и неделимый (50%/50%). 0,3125 печ. л.

СПИСОК ЛИТЕРАТУРЫ

21. *Lang S.* Fundamentals of Diophantine geometry. — Springer Science & Business Media, 2013.

22. *Hindry M.*, *Silverman J. H.* Diophantine geometry: an introduction. Vol. 201. — Springer Science & Business Media, 2013.

23. *Chevalley C.* Introduction to the theory of algebraic functions of one variable. — American Mathematical Soc., 1951.

24. *Deuring M.* Lectures on the theory of algebraic functions of one variable. Vol. 314. — Springer, 2006.

25. *Artin E.* Algebraic numbers and algebraic functions. Vol. 358. — American Mathematical Soc., 2005.

26. *Eichler M.* Introduction to the Theory of Algebraic Numbers and Fuctions. — Academic Press, 1966.

27. *Шафаревич И. Р.* Основы алгебраической геометрии. — МЦНМО, 2007.

28. *Stichtenoth H.* Algebraic function fields and codes. Vol. 254. — Springer Science & Business Media, 2009.

29. *Mordell L. J.* On the rational resolutions of the indeterminate equations of the third and fourth degree // Proc. Cambridge Phil. Soc. Vol. 21. — 1922. — P. 179–192.

30. *Faltings G.* Endlichkeitssätze für abelsche Varietäten über Zahlkörpern // Inventiones Mathematicae. — 1983. — Jrg. 73, nr. 3. — P. 349–366. — ISSN 1432-1297.

31. *Weil A.* L'arithmétique sur les courbes algébriques // Oeuvres Scientifiques Collected Papers. — Springer New York, 1979. — P. 11-45. — ISBN 9781475717051.

32. *Weil A.* L'arithmétique sur les courbes algébriques // Acta mathematica. — 1929. — T. 52, n° 1. — P. 281-315.

33. *Mazur B.* Rational points on modular curves // Modular Functions of one Variable V: Proceedings International Conference, University of Bonn, Sonderforschungsbereich Theoretische Mathematik July 2–14, 1976. — Springer. 2006. — P. 107–148.

34. *Mazur B.*, *Goldfeld D.* Rational isogenies of prime degree // Inventiones mathematicae. — 1978. — Vol. 44. — P. 129–162.

35. *Kubert D. S.* Universal bounds on the torsion of elliptic curves // Proceedings of the London Mathematical Society. — 1976. — Vol. s3–33, no. 2. — P. 193–237. — ISSN 0024-6115.

36. *Kenku M. A.*, *Momose F.* Torsion points on elliptic curves defined over quadratic fields // Nagoya Mathematical Journal. — 1988. — Vol. 109. — P. 125–149. — ISSN 2152-6842.

37. *Sutherland A. V.* Constructing elliptic curves over finite fields with prescribed torsion // Mathematics of Computation. — 2011. — Vol. 81, no. 278. — P. 1131–1147. — ISSN 1088-6842.

38. *Rabarison F. P.* Structure de torsion des courbes elliptiques sur les corps quadratiques // Acta Arithmetica. — 2010. — T. 144, n° 1. — P. 17-52. — ISSN 1730-6264.

39. *Kamienny S.*, *Najman F.* Torsion groups of elliptic curves over quadratic fields // Acta Arithmetica. — 2012. — Vol. 152, no. 3. — P. 291–305. — ISSN 1730-6264.

40. *Sutherland A. V.* Torsion subgroups of elliptic curves over number fields // Avalaible on https://math.mit.edu/drew/MazursTheoremSubsequentResults.pdf. — 2012. — Vol. 1. — P. 14.

41. *Howe E. W.* Genus-2 Jacobians with torsion points of large order // Bulletin of the London Mathematical Society. — 2015. — Vol. 47, no. 1. — P. 127–135.

42. *Jacobi C. G. J.* Considerationes generales de transcendentibus Abelianis. — 1832.

43. *Jacobi C. G. J.* De functionibus duarum variabilium quadrupliciter periodicis, quibus theoria transcendentium Abelianarum innititur. — 1835.

44. *Mazur B.*, *Tate J.* Points of order 13 on elliptic curves // Inventiones Mathematicae. — 1973. — Vol. 22, no. 1. — P. 41–49. — ISSN 1432-1297.

45. *Deligne P.* The Weil conjecture. I // Uspekhi Matematicheskikh Nauk. — 1975. — Vol. 30, no. 5. — P. 159–190.

46. *Serre J.-P.* Algebraic groups and class fields. Vol. 117. — Springer Science & Business Media, 2012.

47. *Faltings G.* Erratum: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern // Inventiones Mathematicae. — 1984. — Jrg. 75, nr. 2. — P. 381–381. — ISSN 1432-1297.

48. *Мамфорд Д.* Лекции о тэта-функциях: (Монография). — Мир, 1988. — ISBN 9785030007458.

49. *Cantor D. G.* Computing in the Jacobian of a hyperelliptic curve // Mathematics of computation. — 1987. — Vol. 48, no. 177. — P. 95–101.

50. *Igusa J.-i.* Arithmetic variety of moduli for genus two // Annals of Mathematics. — 1960. — P. 612–649.

51. *Avanzi R. M.*, *Zannier U. M.* Genus one curves defined by separated variable polynomials and a polynomial Pell equation // Acta Arithmetica. — 2001. — Vol. 99. — P. 227–256.

52. *Zannier U.* Hyperelliptic continued fractions and generalized Jacobians // American Journal of Mathematics. — 2019. — Vol. 141, no. 1. — P. 1–40.

53. *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.

54. *Flynn E. V.* Large rational torsion on abelian varieties // Journal of Number Theory. — 1990. — Vol. 36, no. 3. — P. 257–265.

55. *Leprevost F.* Jacobiennes décomposables de certaines courbes de genre 2 : torsion et simplicité // J. Théorie des Nombres de Bordeaux. — 1991. — T. 7, n° 1. — P. 283-306.

56. *Leprevost F.* Famille de courbes de genre 2 munies d une classe de diviseurs rationnels d ordre 13 // C. R. Acad. Sci. Paris Ser. I Math. — 1991. — T. 313. — P. 451-454.

57. *Leprevost 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 Ser. I Math. — 1991. — Vol. 313. — P. 771–774.

58. *Leprévost F.* Points rationnels de torsion de jacobiennes de certains courbes de genre 2 // Comptes rendus de l'Académie des sciences. Série 1, Mathématique. — 1993. — Vol. 316, no. 8. — P. 819–821.

59. *Ogawa H.* Curves of genus 2 with a rational torsion divisor of order 23 // Proc. Japan Acad. Ser. A Math. Sci. — 1994. — Vol. 70. — P. 295–298.

60. *Poonen B.* Computational aspects of curves of genus at least 2 // Algorithmic Number Theory. — Springer Berlin Heidelberg, 1996. — P. 283–306. — ISBN 9783540706328.

61. *Adams W. W.*, *Razar M. J.* Multiples of points on elliptic curves and continued fractions // Proceedings of the London Mathematical Society. — 1980. — Vol. 3, no. 3.

62. *Berry T. G.* On periodicity of continued fractions in hyperelliptic function fields // Archiv der Mathematik. — 1990. — Vol. 55, no. 3. — P. 259–266. — ISSN 1420-8938.

63. *Berry T. G.* Continued Fractions in Hyperelliptic Function Fields // Coding Theory, Cryptography and Related Areas. — Springer Berlin Heidelberg, 2000. — P. 29–41. — ISBN 9783642571893.

64. *Berry T. G.* A Type of Hyperelliptic Continued Fraction // Monatshefte für Mathematik. — 2005. — Vol. 145, no. 4. — P. 269–283. — ISSN 1436-5081.

65. *Stein A.* Introduction to continued fraction expansions in real quadratic function fields // Faculty of Mathematics. — University of Waterloo, 2002. — P. 1–23.

66. *Jacobson M. J.*, *Scheidler R.*, *Stein A.* Fast arithmetic on hyperelliptic curves via continued fraction expansions // Advances in Coding Theory and Cryptography. — World Scientific, 2007. — P. 200–243.

67. *Sadek M.* Periodic continued fractions and elliptic curves over quadratic fields // Journal of Symbolic Computation. — 2016. — Vol. 76. — P. 200–218.

68. *Poorten A. J. van der*, *Tran X. C.* Quasi-Elliptic Integrals and Periodic Continued Fractions // Monatshefte fur Mathematik. — 2000. — Vol. 131, no. 2. — P. 155–169. — ISSN 1436-5081.

69. *Poorten A. J. van der*, *Tran X. C.* Periodic Continued Fractions in Elliptic Function Fields // Algorithmic Number Theory. — Springer Berlin Heidelberg, 2002. — P. 390–404. — ISBN 9783540454557.

70. *Poorten A. van der.* Periodic continued fractions and elliptic curves. — 2004.

71. *Pappalardi F.*, *Van Der Poorten A. J.* Pseudo-elliptic integrals, units, and torsion // Journal of the Australian Mathematical Society. — 2005. — Vol. 79, no. 3. — P. 335–347. — ISSN 1446-8107.

72. *Scherr Z. L.* Rational Polynomial Pell Equations : PhD thesis / Scherr Zachary L. — The University of Michigan, 2013.

73. *Kronberg M.* Explicit construction of rational torsion divisors on Jacobians of curves : PhD thesis / Kronberg Max. — Universit at Oldenburg, 2016.

74. *Daowsud K.* Continued fractions and the divisor at infinity on a hyperelliptic curve: Examples and order bounds : PhD thesis / Daowsud Katthaleeya. — Oregon State University, 2013.

75. *Merkert O.* Reduction and specialization of hyperelliptic continued fractions : PhD thesis / Merkert Olaf. — Scuola Normale Superiore, 2017.

76. *Malagoli F.* Continued fractions in function fields: polynomial analogues of McMullen's and Zaremba's conjectures : PhD thesis / Malagoli Francesca. — Università di Pisa, 2017.

77. *Петрунин М. М.* S-единицы и функциональные непрерывные дроби в гиперэллиптических полях : PhD thesis / Петрунин Максим Максимович. — НИИСИ РАН, 2019.

78. *Arul V.* Explicit division and torsion points on superelliptic Curves and jacobians : PhD thesis / Arul Vishal. — Massachusetts Institute of Technology, 2020.

79. *Richman D.* Weierstrass points and torsion points on tropical curves : PhD thesis / Richman David. — The University of Michigan, 2020.

80. *Kalaydzhieva N. D.* On problems related to multiple solutions of Pell's equation and continued fractions over function fields : PhD thesis / Kalaydzhieva Nikoleta Dianova. — University College London, 2020.

81. *Lindner S. A.* Improvements to Divisor Class Arithmetic on Hyperelliptic Curves : PhD thesis / Lindner Sebastian A. — University of Calgary, 2020.

82. *Gužvić T.* Torsion of elliptic curves with rational j-invariant over number fields : PhD thesis / Gužvić Tomislav. — University of Zagreb, 2021.

83. *Dobson S.* Key Exchange and Zero-Knowledge Proofs from Isogenies and Hyperelliptic Curves : PhD thesis / Dobson Samuel. — The University of Auckland, 2022.

84. *Nowell S. C.* Models of hyperelliptic curves over p-adic fields : PhD thesis / Nowell Sarah Catherine. — University College London, 2022.

85. *Green H.* The Parity Conjecture for Hyperelliptic Curves : PhD thesis / Green Holly. — University College London, 2023.

86. *Платонов В. П., Петрунин М. М.* О проблеме кручения в якобианах кривых рода 2 над полем рациональных чисел // Докл. РАН. — 2012. — Т. 446, № 3. — С. 263—264.

87. *Stoll M.* On the height constant for curves of genus two // Acta Arithmetica. — 1999. — Vol. 90, no. 2. — P. 183–201.

88. *Stoll M.* An explicit theory of heights for hyperelliptic Jacobians of genus three // Algorithmic and experimental methods in algebra, geometry, and number theory. — 2017. — P. 665–715.

89. *Müller J. S., Reitsma B.* Computing torsion subgroups of Jacobians of hyperelliptic curves of genus 3 // Research in Number Theory. — 2023. — Vol. 9, no. 2. — P. 23.

90. *Elkies N. D.* Curves of genus 2 over $\mathbb{Q}$ whose Jacobians are absolutely simple abelian surfaces with torsion points of high order. — URL: https://people.math.harvard.edu/~elkies/g2_tors.html#bkgd (дата обр. 17.03.2024).

91. *Платонов В. П., Петрунин М. М.* Новые порядки точек кручения в якобианах кривых рода 2 над полем рациональных чисел // Докл. РАН. — 2012. — Т. 443, № 6. — С. 664—664.

92. *Платонов В. П.* Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // Успехи математических наук. — 2014. — Т. 69, 1 (415. — С. 3—38.

93. *Платонов В. П.*, *Петрунин М. М.* Новые кривые рода 2 над полем рациональных чисел, якобианы которых содержат точки кручения больших порядков // Докл. РАН. Матем., информ., проц. упр. — 2015. — Т. 461, № 6. — С. 638—638.

94. *Nicholls C.* Descent methods and torsion on Jacobians of higher genus curves : PhD thesis / Nicholls Christopher. — University of Oxford, 2018.

95. *Платонов В. П.*, *Петрунин М. М.*, *Жгун В. С.* К вопросу о простоте якобианов кривых рода 2 над полем рациональных чисел с точками кручения больших порядков // Докл. РАН. Матем., информ., проц. упр. — 2013. — Т. 450, № 4. — С. 385—388.

96. *Платонов В. П.* Арифметика квадратичных полей и кручение в якобианах // Докл. РАН. — 2010. — Т. 430, № 3. — С. 318—320.

97. *Koblitz N.* Algebraic aspects of cryptography. Vol. 3. — Springer Science & Business Media, 2012.

98. Handbook of elliptic and hyperelliptic curve cryptography / H. Cohen [et al.]. — CRC press, 2005.

99. *Galbraith S. D.* Mathematics of public key cryptography. — Cambridge University Press, 2012.

100. *Wollinger T.* Software and hardware implementation of hyperelliptic curve cryptosystems. — Ruhr University Bochum, 2004.

101. *Koblitz N.* Hyperelliptic cryptosystems // Journal of cryptology. — 1989. — Vol. 1. — P. 139–150.

102. Novel efficient implementations of hyperelliptic curve cryptosystems using degenerate divisors / M. Katagi [et al.] // Information Security Applications: 5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, 2004, Revised Selected Papers 5. — Springer. 2005. — P. 345–359.

103. *Lange T.* Formulae for arithmetic on genus 2 hyperelliptic curves // Applicable Algebra in Engineering, Communication and Computing. — 2005. — Vol. 15. — P. 295–328.

104. *Wiener M. J.* Cryptanalysis of short RSA secret exponents // IEEE Transactions on Information theory. — 1990. — Vol. 36, no. 3. — P. 553–558.

105. *Pollard J. M.* A Monte Carlo method for factorization // BIT Numerical Mathematics. — 1975. — Vol. 15, no. 3. — P. 331–334.

106. *Shanks D.* The infrastructure of a real quadratic field and its applications // Proceedings of the Number Theory Conference. — University of Colorado, Boulder, 1972. — P. 217–224.

107. *Нечаев В.* Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и педвузов. — М.: Высшая школа, 1999.

108. *Shoup V.* Lower bounds for discrete logarithms and related problems // Advances in Cryptology—EUROCRYPT'97: International Conference on the Theory and Application of Cryptographic Techniques Konstanz, Germany, May 11–15, 1997 Proceedings 16. — Springer. 1997. — P. 256–266.

109. *Gaudry P.* Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem // Journal of Symbolic computation. — 2009. — Vol. 44, no. 12. — P. 1690–1702.

110. *Faure C.*, *Minder L.* Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes // Proceedings of the 11th international workshop on Algebraic and Combinatorial Coding Theory, ACCT. Vol. 2008. — 2008. — P. 99–107.

111. *Joyner D.*, *Kim J.-L.* Selected unsolved problems in coding theory. — Springer Science & Business Media, 2011.

112. *Niederreiter H.* Sequences with almost perfect linear complexity profile // Advances in Cryptology—EUROCRYPT'87: Workshop on the Theory and Application of Cryptographic Techniques Amsterdam, The Netherlands, April 13–15, 1987 Proceedings 6. — Springer. 1988. — P. 37–51.

113. *Schinzel A.* On some problems of the arithmetical theory of continued fractions // Acta Arithmetica. — 1961. — Vol. 6, no. 4. — P. 393–413.

114. *Schinzel A.* On some problems of the arithmetical theory of continued fractions II // Acta Arithmetica. — 1962. — Vol. 7, no. 3. — P. 287–298. — ISSN 1730-6264.

115. *Ленг С.* Введение в теорию диофантовых приближений. — Мир, 1970.

116. *Rosen M.* Number theory in function fields. Vol. 210. — Springer Science & Business Media, 2013.

117. *Lasjaunias A.* A survey of diophantine approximationin fields of power series // Monatshefte für Mathematik. — 2000. — Vol. 130. — P. 211–229.

118. *Schmidt W.* On continued fractions and diophantine approximation in power series fields // Acta Arithmetica. — 2000. — Vol. 95, no. 2. — P. 139–166. — ISSN 1730-6264.

119. *Serret J.* Cours d'algèbre supérieure. — Mallet-Bachelier, 1854.

120. *Korkine A.*, *Zolotareff G.* Sur les formes quadratiques // Mathematische Annalen. — 1873. — T. 6, n° 3. — P. 366-389.

121. *Hurwitz A.* Über die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche // Mathematische Annalen. — 1891. — Jrg. 39, nr. 2. — P. 279–284.

122. *Cassels J. W. S.* Simultaneous Diophantine Approximation // Journal of the London Mathematical Society. — 1955. — Vol. s1–30, no. 1. — P. 119–121. — ISSN 0024-6107.

123. *Герман О. Н.* Диофантовы экспоненты решеток // Современные проблемы математики. — 2016. — Т. 23. — С. 35—42.

124. *Быковский В. А.*, *Фроленков Д. А.* О средней длине конечных цепных дробей с фиксированным знаменателем // Матем. сб. — 2017. — Т. 208, № 5. — С. 63—102.

125. *Добровольский Н. М.*, *Добровольский Н. Н.* О минимальных многочленах остаточных дробей для алгебраических иррациональностей // Чебышевский сб. — 2015. — Т. 16, 3 (55). — С. 147—182.

126. *Добровольский Н. Н.* Дзета-функции моноидов натуральных чисел и смежные вопросы : PhD thesis / Добровольский Николай Николаевич. — МГУ имени М.В. Ломоносова, 2024.

127. *Abel N. H.* Ueber die Integration der Differential-Formel $\frac{\rho\,\mathrm{d}x}{\sqrt{R}}$, wenn R und ρ ganze Functionen sind. — 1826.

128. *Tchebichef P.* Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynome du troisieme ou du quatrieme degré' // Journal de Mathématiques Pures et Appliquées. — 1857. — T. 2. — P. 168-192.

129. *Tchebichef P.* Sur l'intégration de la différentielle $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}}\,\mathrm{d}x$ // Journal de Mathématiques Pures et Appliquées. — 1864. — T. 9. — P. 225-241.

130. *Платонов В. П.*, *Беняш-Кривец В. В.* Группы S-единиц в гиперэллиптических полях и непрерывные дроби // Матем. сб. — 2009. — Т. 200, № 11. — С. 15—44.

131. *Artin E.* Quadratische Körper im Gebiete der höheren Kongruenzen. I, II. Arithmetischer Teil // Mathematische Zeitschrift. — 1924. — Jrg. 19, nr. 1. — P. 153–246.

132. *Fulton W.* Algebraic Curves: An Introduction To Algebraic Geometry. Third edition. — Benjamin, New York, 2008.

133. *Galbraith S. D.* Mathematics of public key cryptography. — Cambridge University Press, 2012.

134. *Silverman J. H.* The arithmetic of elliptic curves. Vol. 106. — Springer, 2009.

135. *Mumford D.*, *Ramanujam C. P.*, *Manin J. I.* Abelian varieties. Vol. 5. — Oxford university press Oxford, 1974.

136. *Харрис Д.* Алгебраическая геометрия. Начальный курс. — 2005.

137. *Griffiths P.*, *Harris J.* Principles of algebraic geometry. — John Wiley & Sons, 2014.

138. *Hartshorne R.* Algebraic geometry. Vol. 52. — Springer Science & Business Media, 2013.

139. *Paulus S.*, *Stein A.* Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves // Algorithmic Number Theory. — Springer Berlin Heidelberg, 1998. — P. 576–591. — ISBN 9783540691136.

140. *Платонов В. П.*, *Петрунин М. М.* S-единицы и периодичность в квадратичных функциональных полях // Успехи математических наук. — 2016. — Т. 71, 5 (431). — С. 181—182.

141. *Петрунин М. М.* S-единицы и периодичность квадратного корня в гиперэллиптических полях // Докл. РАН. Матем., информ., проц. упр. — 2017. — Т. 474, № 2. — С. 155—158.

142. *Платонов В. П.*, *Петрунин М. М.* Группы S-единиц и проблема периодичности непрерывных дробей в гиперэллиптических полях // Труды Математического института имени В.А. Стеклова. — 2018. — Т. 302. — С. 354—376.

143. *Платонов В. П.*, *Жгун В. С.*, *Петрунин М. М.* О проблеме периодичности разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов f над полями алгебраических чисел // Матем. сб. — 2022. — Т. 213, № 3. — С. 139—170.

144. *Платонов В. П.*, *Петрунин М. М.* О конечности числа периодических разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов над полями алгебраических чисел // Докл. РАН. Матем., информ., проц. упр. — 2020. — Т. 495. — С. 48—54.

145. *Платонов В. П.*, *Жгун В. С.*, *Петрунин М. М.* О проблеме периодичности разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов над числовыми полями // Докл. РАН. Матем., информ., проц. упр. — 2020. — Т. 493. — С. 32—37.

146. *Menezes A.*, *Zuccherato R.*, *Wu Y.-H.* An elementary introduction to hyperelliptic curves. — 1996.

147. *Lockhart P.* On the discriminant of a hyperelliptic curve // Transactions of the American Mathematical Society. — 1994. — Vol. 342, no. 2. — P. 729–752.

148. *Bekker B.*, *Zarhin Y.* Torsion points of order $2g + 1$ on odd degree hyperelliptic curves of genus g // Transactions of the American Mathematical Society. — 2020. — Vol. 373, no. 11. — P. 8059–8094.

149. *Lang S.* Algebraic number theory. Vol. 110. — Springer Science & Business Media, 1994.

150. *Вейль А.* Основы теории чисел. — Мир, 1972.

151. *Платонов В. П.*, *Петрунин М. М.* Фундаментальные S-единицы в гиперэллиптических полях и проблема кручения в якобианах гиперэллиптических кривых // Докл. РАН. Матем., информ., проц. упр. — 2015. — Т. 465, № 1. — С. 23—23.

152. *Lang S.* Introduction to algebraic and abelian functions. Vol. 89. — Springer Science & Business Media, 2012.

153. *Федоров Г. В.* О гиперэллиптических кривых нечетной степени и рода g с 6 точками кручения порядка $2g+1$ // Докл. РАН. Матем., информ., проц. упр. — 2024. — Т. 518, № 4. — С. 10—17.

154. *Платонов В. П.*, *Жгун В. С.*, *Федоров Г. В.* О конечности множества обобщенных якобианов с нетривиальным кручением над полями алгебраических чисел // Докл. РАН. Матем., информ., проц. упр. — 2023. — Т. 513. — С. 66—70.

155. *Платонов В. П.*, *Федоров Г. В.* Бесконечное семейство кривых рода 2 над полем рациональных чисел, якобиевы многообразия которых содержат рациональные точки порядка 28 // Докл. РАН. — 2018. — Т. 482, № 4. — С. 385—388.

156. *Платонов В. П.*, *Жгун В. С.*, *Федоров Г. В.* Непрерывные дроби в гиперэллиптических полях и представление Мамфорда // Докл. РАН. — 2016. — Т. 471, № 6. — С. 640—644.

157. *Fedorov G. V.* On the Periodicity of Continued Fractions in Hyperelliptic Fields // Advances in Dynamical Systems and Control. — Springer, 2016. — С. 141—157.

158. *Le Brigand D.* Decoding of codes on hyperelliptic curves // Lecture Notes in Computer Science. — Springer Berlin Heidelberg, 1991. — P. 125–134. — ISBN 9783540475460.

159. *Adleman L. M.*, *Huang M.-D. A.* Primality Testing and Abelian Varieties Over Finite Fields. — Springer Berlin Heidelberg, 1992. — ISBN 9783540470212.

160. *Adleman L. M.*, *DeMarrais J.*, *Huang M.-D.* A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields // Algorithmic Number Theory. — Springer Berlin Heidelberg, 1994. — P. 28–40. — ISBN 9783540490449.

161. *Lange T.* Efficient arithmetic on genus 2 hyperelliptic curves over finite fields via explicit formulae // Cryptology ePrint Archive. — 2002.

162. *Lange T.* Inversion-free arithmetic on genus 2 hyperelliptic curves // Cryptology EPrint Archive. — 2002.

163. *Хинчин А. Я.* Цепные дроби. — ГИТТЛ, 1949.

164. *Olds C. D.* Continued fractions. — The Mathematical Association of America, 1963.

165. *Арнольд В. И.* Цепные дроби. Учебное пособие. — МЦНМО, 2013.

166. *Платонов В. П.*, *Петрунин М. М.* S-единицы в гиперэллиптических полях и периодичность непрерывных дробей // Докл. РАН. Матем., информ., проц. упр. — 2016. — Т. 470, № 3. — С. 260—265.

167. *Жгун В. С.* Обобщенные якобианы и непрерывные дроби в гиперэллиптических полях // Чебышевский сб. — 2017. — Т. 18, 4 (64). — С. 208—220.

168. *Daowsud K.*, *Schmidt T. A.* Continued fractions for rational torsion // Journal of Number Theory. — 2018. — Vol. 189. — P. 115–130.

169. *Hickerson D.* Length of period simple continued fraction expansion of $\sqrt{d}$ // Pacific Journal of Mathematics. — 1973. — Vol. 46, no. 2. — P. 429–432. — ISSN 0030-8730.

170. *Cohn J.* The length of the period of the simple continued fraction of $d^{1/2}$ // Pacific Journal of Mathematics. — 1977. — Vol. 71, no. 1. — P. 21–32. — ISSN 0030-8730.

171. *Mkaouar M.* Sur les fractions continues des séries formelles quadratiques sur $F_q(X)$ // Acta Arithmetica. — 2001. — T. 97, n° 3. — P. 241-251. — ISSN 1730-6264.

172. *Hbaib M.*, *Mkaouar M.*, *Tounsi K.* Un critere de transcendance dans le corps des series formelles $\mathbb{F}_q((X^{-1}))$ // J. Number Theory. — 2006. — T. 116. — P. 140-149.

173. *Basma A.* On the continued fraction period for a square root of polynomial in $\mathbb{F}_q[X]$ // Journal for Algebra and Number Theory Academia. — 2015. — Vol. 5, no. 3. — P. 81–89.

174. *Poorten A. J. van der.* Some facts that should be better known, especially about rational functions // Number theory and applications (Banff, AB, 1988). — Kluwer Acad. Publ., Dordrecht, 1989. — P. 497–528.

175. Классификация чисто-вещественных алгебраических иррациональностей / Н. М. Добровольский [и др.] // Чебышевский сб. — 2017. — Т. 18, 2 (62). — С. 98—128.

176. *Добровольский Н. М.*, *Добровольский Н. Н.*, *Юшина Е. И.* О матричной форме теоремы Галуа о чисто периодических цепных дробях // Чебышевский сб. — 2012. — Т. 13, 3 (43). — С. 47—52.

177. *Rosenlicht M.* Equivalence relations on algebraic curves // Annals of Mathematics. — 1952. — P. 169–191.

178. *Rosenlicht M.* Generalized jacobian varieties // Annals of Mathematics. — 1954. — P. 505–530.

179. *Landau E.* Über den Verlauf der zahlentheoretischen Funktion φ (x) // Archiv der Mathematik und Physik. — 1902. — Jrg. 5. — P. 86–91.

180. *Золотарев Е.* Приложение эллиптических функций к вопросам о функциях, наименее и наиболее отклоняющихся от нуля //. Т. 2. — 1932. — С. 1—59.

181. *Платонов В. П.*, *Петрунин М. М.* Новые результаты о проблеме периодичности непрерывных дробей элементов гиперэллиптических полей // Труды Математического института имени В.А. Стеклова. — 2023. — Т. 320. — С. 278—286.

182. *Платонов В. П.*, *Жгун В. С.*, *Федоров Г. В.* О периодичности непрерывных дробей в гиперэллиптических полях над квадратичным полем констант // Докл. РАН. — 2018. — Т. 482, № 2. — С. 137—141.

183. *Платонов В. П.*, *Петрунин М. М.*, *Штейников Ю. Н.* О конечности числа эллиптических полей с заданными степенями S-единиц и периодическим разложением $\sqrt{f}$ // Докл. РАН. Матем., информ., проц. упр. — 2019. — Т. 488, № 3. — С. 237—242.

184. О конечности гиперэллиптических полей со специальными свойствами и периодическим разложением $\sqrt{f}$ / В. П. Платонов [и др.] // Докл. РАН. Матем., информ., проц. упр. — 2018. — Т. 483, № 6. — С. 603—608.

185. SymPy: symbolic computing in Python / A. Meurer [et al.] // PeerJ Computer Science. — 2017. — Vol. 3. — e103.

186. SymPy 1.12 documentation. — URL: https://docs.sympy.org/latest/index.html (дата обр. 09.05.2023).

187. *Hone A. N. W.* Continued Fractions and Hankel Determinants from Hyperelliptic Curves // Communications on Pure and Applied Mathematics. — 2020. — Vol. 74, no. 11. — P. 2310–2347. — ISSN 1097-0312.