В.В. Скобелев

Н.М. Глазунов

В.Г. Скобелев

МНОГООБРАЗИЯ НАД КОЛЬЦАМИ

Теория и приложения

ИПММ НАНУ

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК УКРАИНЫ

ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ И МЕХАНИКИ

В.В. Скобелев, Н.М. Глазунов, В.Г. Скобелев

МНОГООБРАЗИЯ НАД КОЛЬЦАМИ

Теория и приложения

Донецк

2011

УДК 512.7+519.7+681.3

Рецензенты:

Академик НАН Украины, зав. отделом теории цифровых автоматов ИК НАН Украины им. В.В. Глушкова *А.А. Летичевский*

Член-корреспондент НАН Украины, декан факультета кибернетики Киевского национального университета имени Тараса Шевченко, *А.В. Анисимов*

Многообразия над кольцами. Теория и приложения
В.В. Скобелев, Н.М. Глазунов, В.Г. Скобелев. ИПММ НАН Украины, Донецк, 2011. – 323 с.

ISBN 978-966-02-6011-5

Монография посвящена дескриптивному, алгоритмическому и метрическому анализу многообразий над конечными кольцами с позиции их возможных применений в процессе исследования автоматно-алгебраических моделей дискретных преобразователей. Решен ряд задач анализа алгебраических кривых, разработаны методы решения систем уравнений с параметрами над кольцами. Показано, каким образом задачи анализа автоматов над кольцами характеризуются в терминах многообразий.

Для специалистов в областях дискретной математики, computer science, прикладной алгебры, защиты информации, а также для студентов и аспирантов, специализирующихся в этих областях.

Утверждено к печати Ученым советом Института прикладной математики и механики НАН Украины

Многовиди над кільцями. Теорія і прикладення
В.В. Скобелєв, М.М. Глазунов, В.Г. Скобелєв. ІПММ НАН України, Донецьк, 2011. – 323 с. (на російській мові)

ISBN 978-966-02-6011-5

Монографія присвячена дескриптивному, алгоритмічному та метричному аналізу многовидів над скінченними кільцями з точки зору їх можливих застосувань у процесі дослідження автоматно-алгебраїчних моделей дискретних перетворювачів. Вирішено низку задач аналізу алгебраїчних кривих, розроблено методи розв'язку систем рівнянь з параметрами над кільцями. Встановлено, яким чином задачі аналізу автоматів над кільцями характеризуються у термінах многовидів.

Для спеціалістів в галузях дискретної математики, computer science, прикладної алгебри, захисту інформації, а також для студентів та аспірантів, які спеціалізуються у цих галузях.

ISBN 978-966-02-6011-5

Светлой памяти

Юлии Владимировны Капитоновой

посвящается

Предисловие

Внедрение информационных технологий практически во все сферы жизни современного общества четко продемонстрировало, что *информация* является стратегическим товаром, от которого зависит не только благополучие, но и существование отдельных индивидуумов, организаций, стран и, вообще, цивилизации в целом. Поэтому проблема защиты информации стала одной из наиболее актуальных на современном этапе развития общества. Как следствие, в течение последних десятилетий наблюдается интенсивное развитие криптографии. Значительное число используемых моделей и методов, совершенно различных по своей структуре, часто недостаточно исследованных теоретически, привело к тому, что основным методом исследования в криптографии является статистический анализ качества используемых конструкций. Просчеты, допускаемые при таком анализе, а также интенсивное развитие средств вычислительной техники являются основными причинами достаточно частого пересмотра криптографических стандартов во всем мире. В настоящее время наблюдается устойчивая тенденция перехода криптографии от чисто комбинаторных моделей к моделям, построенным на основе конечных алгебраических систем (асимметричая криптография на основе теоретико-числовых алгоритмов, фрагментарное использование вычислений в кольцах вычетов практически во всех кандидатах на современные поточные шифры, квантовая криптография, представляющая собой специальный раздел теории унитарных операторов в конечномерных комплексных пространствах и т.д.). Эта тенденция явилась основной причиной формирования на современном этапе раздела теории дискретных преобразователей, предназначенного для исследования автоматно-алгебраических моделей над конечными алгебраическими системами. Для таких моделей решение практически всех задач автоматически сводится к исследованию систем уравнений с параметрами над алгебраической системой. Поэтому в качестве алгебраической системы естественно выбрать конечное кольцо, так как наличие делителей нуля автоматически обеспечивает поиск (перебор) в процессе решения уравнений.

Из сказанного выше вытекает, что понятие *алгебраического многообразия* (и *алгебраической кривой*, как его специального случая) играет определяющую роль в исследовании автоматно-алгебраических моделей над конечным кольцом.

Предметом исследования настоящей монографии является дескриптивный, алгоритмический и метрический анализ многообразий над конечным кольцом, прежде всего, с позиции их возможных применений для исследования соответствующих автоматно-алгебраических моделей дискретных преобразователей.

Монография состоит из шести разделов.

В разделе 1 представлен математический аппарат, необходимый для изложения материала в последующих разделах: основные алгебраические системы (полугруппы,

группы, поля, кольца, кольца многочленов), многообразия над кольцами, полиномиальная и рациональная параметризации многообразия, основные результаты, связанные с плоскими алгебраическими кривыми над конечным кольцом, взаимосвязь между свойствами аффинных и проективных кривых.

В разделе 2 рассмотрены некоторые типы кривых 2-го и 3-го порядков (т.е. коники и кубики) над конечным ассоциативно-коммутативным кольцом с единицей. Найдены множества точек разложимых коник и кубик, а также коник специального вида. Охарактеризовано множество особых точек коники и кубики. Исследуются методы приведения коники к каноническому виду. Установлены условия существования кратных корней многочлена, являющегося правой частью уравнения кубики. Рассмотрены основные свойства эллиптических кривых над полями, а также некоторые приложения эллиптических кривых.

В разделе 3 систематически изложены модели и методы алгебраической геометрии, применяемые в процессе анализа алгебраических кривых, определенных как над конечными полями и кольцами, так и над кольцом целых чисел, над полем p-адических чисел, над полем комплексных чисел. Наряду с непосредственным рассмотрением алгебраических кривых с коэффициентами в конечных кольцах, их анализ осуществляется в результате их локализации по модулям идеалов над более общими кольцами их определения. Необходимость такого подхода возникает при исследовании как теоретических, так и прикладных задач, а его достоинством – возможность применять в процессе анализа алгебраических кривых как локальные, так и глобальные методы. В разделе охарактеризована минимальная модель эллиптической кривой над полем p-адических чисел и над полем рациональных чисел, рассмотрены подходы к представлению гомоморфизмов эллиптических кривых в терминах решеток и в терминах линейных преобразований переменных, показано, как понятие *степень отображения* используется в процессе анализа морфизмов алгебраических кривых, охарактеризовано кольцо эндоморфизмов эллиптической кривой, рассмотрено значение понятия *изогения* при исследовании морфизмов алгебраических кривых, представлена связь модулярных функций и форм с эллиптическими кривыми, изложены основы арифметического моделирования и последующего кодирования специального класса последовательностей, которые строятся, в частности, на основе кубических арифметических поверхностей и накрытий Артина-Шрайера.Эти результаты могут применяться при реализации псевдослучайных генераторов d-ичных ($d \in \mathbf{N}, d \geq 2$) последовательностей.

Раздел 4 посвящен методам решения уравнений и систем уравнений над конечным ассоциативно-коммутативным кольцом с единицей. Исследовано соотношение между множествами отображений абстрактного множества S в полные системы вычетов по конечному набору попарно взаимно простых элементов дедекиндового кольца и множествами отображений множества S в полную систему вычетов по произведению этих элементов. Рассмотрено применение полученных результатов при комбинаторном анализе объектов, построенных в терминах числовых колец, и используемых при решении прикладных задач преобразования информации. Предложена общая схема решения систем полиномиальных уравнений с параметрами над кольцом $\mathcal{K}$. Эта схема детализирована для решения систем полиномиальных уравнений с параметрами над кольцом вычетов $\mathcal{Z}_{p^k}$.

В разделе 5 систематически исследованы автоматы над конечным ассоциативно-

коммутативным кольцом с единицей. Основная цель этого раздела состоит в том, чтобы показать, каким образом решение основных задач анализа для таких автоматов сводится к решению систем уравнений с параметрами над кольцом. В разделе рассмотрена схема анализа конечно-автоматных характеристик исследуемых моделей, охарактеризованы классы их эквивалентных состояний, решены задачи параметрической идентификации и идентификации начального состояния, охарактеризованы множества неподвижных тоечк автоматных отображений, исследуется вариация поведения автомата при вариации параметров или начального состояния, решена задача построения асимптотически точной имитационной модели для нелинейного одномерного автомата с лагом 2.

В разделе 6 изложены основы теории схем А. Гротендика – математического аппарата, предназначенного, в частности, для исследования многообразий над произвольными ассоциативно-коммутативными кольцами с единицей. В разделе представлены понятия *спектр кольца* и *пучек*, охарактеризовано понятие схема, исследовано понятие *векторное расслоение*, кратко рассмотрено применение элементов теории схем к анализу и расширению понятия многообразие, а также применение теории одномерных схем и групповых схем к анализу и расширению понятия алгебраическая кривая.

Монография написана в замкнутой форме, т.е. определяются все, кроме общепринятых, понятия.

Многие результаты были опубликованы авторами ранее (см. список литературы), доложены на семинарах в ИК НАН Украины и ИПММ НАН Украины, а также на многочисленных международных конференциях. Однако настоящая монография представляет собой первую попытку представить все эти результаты с единых позиций.

Вклад авторов в работу над монографией следующий.

Н.М. Глазуновым написаны разделы 3 и 6.

В.В. Скобелевым написаны разделы 2 и 4, а также пп.5.7 и 5.8.

В.Г. Скобелевым написан раздел 1 и пп.5.1-5.6.

Общее редактирование всего текста монографии осуществлено В.Г. Скобелевым.

Все результаты, представленные в разделах 2, 4 и 5 получены В.В. Скобелевым и В.Г. Скобелевым в соответствии с темами научных исследований, проводимых в ИПММ НАН Украины в рамках следующих тем:

1. Сучасні алгебраїчні, логічні та еволюційні методи веріфікації, ідентифікації і керування дискретними та непервними системами (2009-2013) (НДР № 0109U002770).

2. Обернені задачі теорії керування і сучасні комунікаційні технології (2007-2011) (НДР № 0107U000466).

Монография, в первую очередь, предназначена для специалистов в области криптологии, прикладной теории алгоритмов, теории автоматов и дискретной математики, а также для студентов и аспирантов, специализирующихся в этих областях. Кроме того, целью авторов является привлечение внимания специалистов, студентов и аспирантов в области конечных алгебраических систем к задачам, связанным с анализом автоматно-алгебраических моделей дискретных преобразователей информации, а также с теоретическим исследованием целесообразности использования этих моделей в процессе решения задач современной криптографии.

Монография также может быть использована преподавателями ВУЗов при разработке соответствующих спецкурсов. Часть материала, представленного в разделах 1 и 5, использовалась В.Г. Скобелевым при чтении курсов лекций «Введение в криптологию» и «Математические основы криптографии» в Донецком национальном университете для студентов направления 6.080.200 «Прикладна математика», а также при чтении курса лекций «Захист інформації в телекомунікаційних мережах і системах» в Донецком национальном техническом университете для специальности 7.09.24.01 «Телекомунікаційні мережи і системи». Часть материала, представленного в разделах 3 и 6, использовалась Н.М. Глазуновым при чтении курсов лекций «Несанкционированный доступ и защита информации», «Захист інформації в комп'ютерних системах та мережах», «Архівація і стиснення аудіо- і відеозображень» в Институте компьютерных технологий и Факультете компьютерных наук Национального Авиационного Университета.

Авторы считают своим долгом выразить следующие благодарности.

Авторы выражают искреннюю благодарность профессору **Ю.В. Капитоновой** за ее постоянную поддержку и внимание к исследованиям. Ее светлой памяти и посвящена настоящая монография.

Авторы выражают глубокую и искреннюю благодарность академику НАН Украины А.А. Летичевскому, за его внимание, поддержку и, что самое ценное, за его полезные советы и идеи, возможно, не в полной мере, реализованные авторами в процессе выполнения настоящего исследования.

Искренние благодарности научным руководителям на стадии кандидатской диссертации, чьи усилия и терпение, во многом, сформировали сегодняшние позиции и точки зрения авторов на исследуемые в монографии проблемы, а именно: благодарность В.В. Скобелева профессору Ткаченко В.Н., благодарность В.Г. Скобелева профессору **А.М. Богомолову** и академику РАЕН В.Б. Кудрявцеву.

Н.М. Глазунов выражает глубокую признательность учителю по Университету и научному соруководителю кандидатской диссертации **О.Н. Введенскому**, профессору **А.Г. Постникову**, который ввел автора в аналитическую теорию чисел, профессору **А.В. Малышеву**, который ввел автора в геометрию чисел, поддержка и сотрудничество с которыми способствовали написанию аналитической и геометрико-числовой частей докторской диссертации автора, а также члену-корреспонденту НАН Украины и РАН **А.А. Стогнию**.

Авторы выражают благодарность директору ИПММ НАН Украины, чл.-корр. НАНУ Ковалеву А.М. и зам. директора ИПММ НАНУ, д.ф.-м.н. Ковалевскому А.А. за обеспечение условий для появления настоящей монографии.

Написание любой книги требует больших затрат сил и времени. Скобелев В.В. и Скобелев В.Г. выражают искреннюю благодарность маме и жене, Скобелевой Галине, за ее терпение и поддержку в процессе работы над монографией.

Безусловно, что за все недостатки ответственность несут только авторы, которые будут благодарны за любые конструктивные замечания, касающиеся содержания книги.

АВТОРЫ

Апрель, 2011 г.,
Киев, Донецк

СОДЕРЖАНИЕ

1. МОДЕЛИ И МЕТОДЫ

В настоящем разделе представлен математический аппарат, необходимый для изложения материала в последующих разделах.

В п.1.1 охарактеризованы основные алгебраические системы, используемые в дальнейшем, а именно: полугруппы, группы, поля, кольца, а также кольца многочленов. В п.1.2 рассмотренны многообразия над кольцами, а также понятия полиномиальной и рациональной параметризации многообразия над кольцом. Эти параметризации охарактеризованы в терминах специальных колец отображений одного кольца в другое. В п.1.3 изложены основные результаты, связанные с плоскими алгебраическими кривыми над конечным кольцом – специальным случаем многообразия над конечным кольцом. В случае поля рассмотрена взаимосвязь между свойствами аффинных и проективных кривых.

Материал, изложенный в настоящем разделе, основан на монографиях и учебниках [6,29,30,36,39,40,44,47,82].

1.1. Алгебраические системы.

Рассмотрим алгебраические системы, в терминах которых будет осуществляться изложение результатов в последующих разделах.

1.1.1. Группоиды, полугруппы, группы.

Выделяют следующие типы алгебраических систем с одной бинарной операцией.

Группоидом называется алгебраическая система $\mathcal{G} = (G, \diamond)$, где «$\diamond$» – бинарная операция. Если $c = a \diamond b$ $(a, b, c \in G)$, то a и b – *делители* элемента c (говорят также, что c *делится* на a и b). Величина $|G|$ называется *порядком* группоида $\mathcal{G}$.

Пусть $\mathcal{G}_1 = (G_1, \diamond_1)$ и $\mathcal{G}_2 = (G_2, \diamond_2)$ – группоиды. Говорят, что:

1) группоид $\mathcal{G}_2$ – *гомоморфный образ* группоида $\mathcal{G}_1$, если существует такая сюръекция $f : G_1 \to G_2$, что $f(a \diamond_1 b) = f(a) \diamond_2 f(b)$ для любых $a, b \in G_1$ (отображение f – *гомоморфизм* $\mathcal{G}_1$ на $\mathcal{G}_2$);

2) группоиды $\mathcal{G}_1$ и $\mathcal{G}_2$ *изоморфны* (друг другу), если существует такая биекция $f : G_1 \to G_2$, что $f(a \diamond_1 b) = f(a) \diamond_2 f(b)$ для любых $a, b \in G_1$ (отображение f – *изоморфизм* между $\mathcal{G}_1$ и $\mathcal{G}_2$).

Если в группоиде $\mathcal{G} = (G, \diamond)$ существует такой (единственный) элемент $a \in G$, что:

1) $a \diamond x = x \diamond a = x$ для всех $x \in G$, то a называется *нейтральным* элементом группоида $\mathcal{G}$ и обозначается e;

2) $a \diamond x = a$ и $x \diamond a = a$ для всех $x \in G$, то a называется *нулем* группоида $\mathcal{G}$ и обозначается 0.

Пусть $\mathcal{G} = (G, \diamond)$ – группоид с нейтральным элементом e. Для элемента $a \in G$ элемент $b \in G$ называется:

1) *левым обратным* элементом, если $b \diamond a = e$;

2) *правым обратным* элементом, если $a \diamond b = e$.

Замечание 1.1. При любом гомоморфизме f группоида $\mathcal{G}_1 = (G_1, \diamond_1)$ на группоид $\mathcal{G}_2 = (G_2, \diamond_2)$:

1) нейтральный элемент $e_1 \in G_1$ (если он существует) группоида $\mathcal{G}_1$ отображается на нейтральный элемент $e_2 \in G_2$ группоида $\mathcal{G}_2$;

2) нуль $0_1 \in G_1$ (если он существует) группоида $\mathcal{G}_1$ отображается в нуль $0_2 \in G_2$ группоида $\mathcal{G}_2$;

3) левый (правый) обратный для $a \in G_1$ элемент (если он существует) отображается на левый (соответственно, правый) обратный для $f(a) \in G_2$ элемент.

Группоид $\mathcal{G} = (G, \diamond)$ – *абелев*, если «$\diamond$» – *коммутативная* операция, т.е. $a \diamond b = b \diamond a$ $(a, b \in G)$.

Говорят, что в группоиде $\mathcal{G} = (G, \diamond)$ выполняется *закон сокращения*, если

$$(\forall a, b, c \in G)((a \diamond c = b \diamond c \Longrightarrow a = b) \wedge (c \diamond a = c \diamond b \Longrightarrow a = b)).$$

Замечание 1.2. Если $|G| > 1$, то группоид $\mathcal{G} = (G, \diamond)$, удовлетворяющий закону сокращения, не содержит нуля.

Квазигруппой называется группоид $\mathcal{G} = (G, \diamond)$, в котором для любых $a, b \in G$ $(a \neq 0)$ однозначно разрешимы уравнения $a \diamond x = b$ и $y \diamond a = b$. Квазигруппа $\mathcal{G}$ с нейтральным элементом называется *лупой*.

Полугруппой называется такой группоид $\mathcal{G} = (G, \diamond)$, что «$\diamond$» – *ассоциативная* операция, т.е.

$$a \diamond (b \diamond c) = (a \diamond b) \diamond c \ (a, b, c \in G).$$

Степени элемента a полугруппы $\mathcal{G}$ определяются равенствами

$$a^n = \underbrace{a \diamond \cdots \diamond a}_{n} \ (n \in \mathbf{N}).$$

Элементы a^2 $(a \in G)$ называются *квадратами*, а элементом, *свободным от квадратов*, называется любой такой элемент $b \in G \backslash \{0, e\}$, что

равенство $b = v \diamond u^2 \diamond w$ не имеет место ни для каких элементов $u \in G \backslash \{e\}$ и $v, w \in G$.

Замечание 1.3. Таким образом, поиск квадратов полугруппы $\mathcal{G} = (G, \diamond)$ сводится к поиску решений уравнений вида

$$x^2 = b \ (b \in G \backslash \{0, e\}).$$

Пусть $\mathcal{G} = (G, \diamond)$ – полугруппа с нейтральным элементом. Если для элемента $a \in G$ существуют и левый, и правый обратные элементы, то они совпадают. Такой элемент a называется *обратимым* элементом, а обратный ему элемент обозначается a^{-1}. Элементы множества G^{inv} всех обратимых элементов полугруппы $\mathcal{G}$ называются *делителями нейтрального элемента*, а элементы множества $G \setminus G^{inv}$ – *необратимыми* элементами полугруппы $\mathcal{G}$.

Группой называется такая полугруппа $\mathcal{G}$, что каждое из уравнений $a \diamond x = b$ и $y \diamond a = b$ однозначно разрешимо при любых $a, b \in G$.

Из этого определения вытекает, что в группе существует нейтральный элемент, а также что для каждого элемента $a \in G$ существует (единственный) *обратный* элемент a^{-1}, т.е.

$$a \diamond a^{-1} = a^{-1} \diamond a = e.$$

Замечание 1.4. Группа $\mathcal{G}$ не содержит нуля, если $|G| > 1$. Если же $|G| = 1$, то единственный элемент множества G одновременно является и нулем, и нейтральным элементом.

Для элемента a группы $\mathcal{G}$ нулевая и отрицательная степени определены равенствами

$$a^0 = e,$$

$$a^{-n} = (a^{-1})^n \ (n \in \mathbf{N}).$$

Элемент a группы $\mathcal{G}$ имеет *бесконечный* порядок, если все элементы a^n $(n \in \mathbf{N})$ попарно различны. В противном случае, *порядок* элемента a – это такое наименьшее число $n_0 \in \mathbf{N}$, что

$$a^{n_0} = e.$$

Если подмножество H $(\emptyset \neq H \subseteq G)$ замкнуто относительно операции «$\diamond$», а система $\mathcal{H} = (H, \diamond)$ является системой того же типа, что и система

$\mathcal{G} = (G, \diamond)$, то имя системы $\mathcal{H}$ образуется из имени системы $\mathcal{G}$ с помощью приставки «под» (т.е. подгруппоид, подполугруппа, подгруппа и т.д.).

Пусть $\mathcal{G} = (G, \diamond)$ – группоид, а Ω – такое семейство отображений множества G в себя, что для любых $\omega \in \Omega$ и $a, b \in G$ истинно равенство

$$\omega(a \diamond b) = \omega(a) \diamond \omega(b).$$

Тогда $\mathcal{G}$ называется Ω-*операторным* группоидом.

Замечание 1.5. Если элементам множества Ω соответствуют *эндоморфизмы* (т.е. гомоморфизмы в себя) группоида $\mathcal{G}$, то понятие «Ω-операторный группоид» дает возможность выделить в $\mathcal{G}$ подгруппоиды, которые отображаются в себя при каждом эндоморфизме $\omega \in \Omega$.

Такие подгруппоиды называются Ω-*допустимыми*. Пересечение любого множества Ω-допустимых подгруппоидов группоида $\mathcal{G}$, если оно не пусто, является Ω-допустимых подгруппоидом.

Таким образом, понятие «Ω-операторный группоид» дает возможность с единых позиций исследовать не только внутренние свойства группоидов, но и различные их представления (достаточно в качестве Ω выбрать ту или иную подполугруппу полугруппы эндоморфизмов группоида $\mathcal{G}$).

Для полугруппы $\mathcal{G} = (G, \diamond)$ с нейтральным элементом подполугруппа $\mathcal{G}^{inv} = (G^{inv}, \diamond)$ является группой.

Пусть $\mathcal{G} = (G, \diamond)$ – абелева полугруппа, а $\mathcal{S}_{\mathcal{G}} = (S_{\mathcal{G}}, \diamond)$ – такая ее подполугруппа, что в $\mathcal{G}$ можно выполнять сокращение на элементы из $S_{\mathcal{G}}$, т.е. если $a \diamond x = b \diamond x$ $(a, b \in G,\ x \in S_{\mathcal{G}})$, то $a = b$. Истинно утверждение: *абелеву полугруппу $\mathcal{G}$ можно изоморфно вложить в такую абелеву полугруппу $\overline{\mathcal{G}} = (\overline{G}, \diamond)$ с нейтральным элементом, что каждый элемент $x \in S_{\mathcal{G}}$ имеет в полугруппе $\overline{\mathcal{G}}$ обратный элемент.*

Замечание 1.6. Абелева полугруппа $\overline{\mathcal{G}} = (\overline{G}, \diamond)$ строится следующим образом.

Множеством *дробей* (говорят также, *множеством частных*) над абелевой полугруппой $\mathcal{G} = (G, \diamond)$ называется множество

$$R_{\mathcal{G}} = \left\{ \frac{a}{x} \middle| a \in G,\ x \in S_{\mathcal{G}} \right\}.$$

При этом *дробь* $\frac{a}{x}$ понимается просто как упорядоченная пара (a, x) элементов a и x.

Определив на множестве $R_{\mathcal{G}}$ операцию «$\diamond$» равенством

$$\frac{a}{x} \diamond \frac{b}{y} = \frac{a \diamond b}{x \diamond y} \quad \left(\frac{a}{x}, \frac{b}{y} \in R_{\mathcal{G}} \right),$$

получим абелеву полугруппу $\mathcal{R}_{\mathcal{G}} = (R_{\mathcal{G}}, \diamond)$.

Обозначим через «$\equiv$» такое отношение эквивалентности на множестве $R_{\mathcal{G}}$, что

$$\frac{a}{x} \equiv \frac{b}{y}$$

тогда и только тогда, когда

$$a \diamond y = b \diamond x.$$

Положим

$$\overline{G} = R_{\mathcal{G}}/_{\equiv},$$

а операцию «$\diamond$» определим на множестве $\overline{G}$ следующим образом: если $H_1, H_2 \in \overline{G}$ ($\frac{a}{x} \in H_1$, $\frac{b}{y} \in H_2$), то $H_1 \diamond H_2 = H$, где $\frac{a \diamond b}{x \diamond y} \in H$.

Получим абелеву полугруппу с единицей

$$\overline{\mathcal{G}} = (\overline{G}, \diamond),$$

которая называется *полугруппой дробей* (говорят также, *полугруппой частных*) над абелевой полугруппой $\mathcal{G}$.

Нейтральным элементом полугруппы $\overline{\mathcal{G}} = (\overline{G}, \diamond)$ является элемент $\{\frac{x}{x} | x \in S_{\mathcal{G}}\}$. Элементу $a \in G$ полугруппы $\mathcal{G}$ соответствует элемент $\{\frac{a \diamond x}{x} | x \in S_{\mathcal{G}}\}$ полугруппы $\overline{\mathcal{G}}$, а элементом полугруппы $\overline{\mathcal{G}}$, обратным элементу $\{\frac{a \diamond x}{x} | x \in S_{\mathcal{G}}\}$ ($a \in S_{\mathcal{G}}$) является элемент $\{\frac{x}{a \diamond x} | x \in S_{\mathcal{G}}\}$.

Пусть $\mathcal{H}$ – подгруппа группы $\mathcal{G}$ (обозначается $\mathcal{H} \leq \mathcal{G}$). *Левые* (соответственно, *правые*) *смежные классы* группы $\mathcal{G}$ по подгруппе $\mathcal{H}$ – это множества $g \diamond H = \{g \diamond h | h \in H\}$ ($g \in G$) (соответственно, множества $H \diamond g = \{h \diamond g | h \in H\}$ ($g \in G$)). При этом, $\pi^l_{\mathcal{H}} = \{g \diamond H | g \in G\}$ и $\pi^r_{\mathcal{H}} = \{H \diamond g | g \in G\}$ – разбиения множества G.

Если $\mathcal{G}$ – конечная группа, то разбиения $\pi^l_{\mathcal{H}}$ и $\pi^r_{\mathcal{H}}$ содержат одно и тоже число блоков. Это число блоков называется *индексом* $\mathcal{H}$ в $\mathcal{G}$. Имеет место теорема Лагранжа: *порядок и индекс любой подгруппы конечной группы являются делителями порядка группы.*

Подгруппа $\mathcal{H}$ группы $\mathcal{G}$ называется *нормальной подгруппой* (обозначается $\mathcal{H} \lhd \mathcal{G}$), если $g \diamond H = H \diamond g$ ($g \in G$). Истинно утверждение: *пересечение любого множества нормальных подгрупп группы $\mathcal{G}$ является нормальной подгруппой группы $\mathcal{G}$.*

Множество $\{g \diamond H | g \in G\}$ называется *множеством смежных классов* группы $\mathcal{G}$ по нормальной подгруппе $\mathcal{H}$. Это множество является группой, если операцию «$*$» композиции смежных классов определить равенством

$$(g_1 \diamond H) * (g_2 \diamond H) = (g_1 \diamond g_2) \diamond H.$$

Такая группа называется *фактор-группой* группы $\mathcal{G}$ по нормальной подгруппе $\mathcal{H}$ и обозначается $\mathcal{G}/_{\mathcal{H}}$.

Существует следующая связь между нормальными подгруппами и гомоморфизмами групп: *если сюръекция $f : G \to H$ является гомоморфизмом группы $\mathcal{G} = (G, \diamond_{\mathcal{G}})$ на группу $\mathcal{H} = (H, \diamond_{\mathcal{H}})$ то алгебраическая*

система $(f^{-1}(e_{\mathcal{H}}), \diamond_{\mathcal{G}})$ *является нормальной подгруппой группы* $\mathcal{G}$ ($e_{\mathcal{H}}$ – нейтральный элемент группы $\mathcal{H}$).

Множество $f^{-1}(e_{\mathcal{H}})$ называется *ядром гомоморфизма* f и обозначается $\ker f$. Истинно утверждение: *если* $\mathcal{H}_1$ *и* $\mathcal{H}_2$ *– такие нормальные подгруппы группы* $\mathcal{G}$, что $\mathcal{H}_1 \lhd \mathcal{H}_2$, *то существует гомоморфизм факторгруппы* $\mathcal{G}/_{\mathcal{H}_1}$ *на фактор-группу* $\mathcal{G}/_{\mathcal{H}_2}$.

Множество всех *подстановок*, определенных на любом множестве X (т.е. биекций $f : X \to X$) вместе с операцией их суперпозиции образует *группу* $\mathcal{S}(X)$.

Если $X = \mathbf{N}_n$, то эта группа называется *симметрической группой* и обозначается $\mathcal{S}(n)$. Имеет место теорема Кэли: *любая конечная группа изоморфна некоторой подгруппе группы* $\mathcal{S}(n)$ *при подходящем выборе числа* n.

Таким образом, симметрические группы $\mathcal{S}(n)$ ($n \in \mathbf{N}$) обеспечивают унифицированное представление конечных групп.

Для любой полугруппы $\mathcal{G} = (G, \diamond)$ абелева подполугруппа $(\langle a \rangle, \diamond)$ ($a \in G$), где

$$\langle a \rangle = \{a^n | n \in \mathbf{N}\},$$

называется *циклической* полугруппой, порожденной элементом a.

Для группы $\mathcal{G} = (G, \diamond)$ *циклической* группой, порожденной элементом $a \in G$ называется абелева подгруппа $(\langle a \rangle, \diamond)$, где

$$\langle a \rangle = \{a^n | n \in \mathbf{Z}\}.$$

В обоих случаях $a \in G$ называется *образующим* элементом.

Отметим следующие свойства подгруппы $(\langle a \rangle, \diamond)$ порядка n:

1) элемент a^k ($k \in \mathbf{N}$) порождает подгруппу порядка $(n, k)^{-1} \cdot n$, где (n, k) – НОД чисел n и k;

2) для каждого делителя d числа n существует единственная подгруппа порядка d и единственная подгруппа индекса d;

3) для каждого делителя d числа n существует в точности $\varphi(d)$ образующих элементов порядка d, где φ – функция Эйлера;

4) существует в точности $\varphi(n)$ образующих элементов.

Пусть $\mathcal{G} = (G, \diamond)$ – абелева полугруппа с нейтральным элементом, удовлетворяющая закону сокращения. Элементы $a, b \in G$ называются

ассоциированными, если каждый из них является делителем для другого. Истинно утверждение: $a, b \in G$ – *ассоциированные элементы тогда и только тогда, когда существует такой элемент* $c \in G^{inv}$, *что* $a = b \diamond c$.

Отсюда вытекает, что множество G разбивается на классы ассоциированных элементов: один из этих классов – множество G^{inv}, а классом элементов, ассоциированных с элементом $a \in G \setminus G^{inv}$ является множество $a \diamond G^{inv}$.

Элемент $p \in G \setminus G^{inv}$ называется *неприводимым*, если из равенства $p = a \diamond b$ вытекает, что один из элементов a, b – делитель нейтрального элемента (следовательно, другой элемент ассоциирован с p).

Определим на множестве классов ассоциированных элементов полугруппы $\mathcal{G}$ следующее отношение «$\leq$» частичного порядка: $A \leq B$ тогда и только тогда, когда хотя бы один (а, следовательно, каждый) элемент класса A является делителем хотя бы одного (а, следовательно, каждого) элемента класса B.

Ясно, что G^{inv} – наименьший элемент этого частично упорядоченного множества, а классы ассоциированных неприводимых элементов – минимальные элементы множества классов ассоциированных элементов, отличных от G^{inv}.

Элемент $p \in G \setminus G^{inv}$ называется *простым*, если из того, что $a \diamond b$ делится на p вытекает, что a или b делится на p. Каждый простой элемент является неприводимым.

Обратное утверждение истинно тогда и только тогда, когда для любых элементов $a, b \in G$ существует их наибольший общий делитель, т.е. такой делитель d элементов a и b, который делится на любой другой делитель d' этих элементов.

Наибольшим общим делителем (если он существует) элементов a и b является любой элемент такого класса D ассоциированных элементов, что D – максимальный элемент множества всех таких классов X ассоциированных элементов, что $X \leq A$ (где $a \in A$) и $X \leq B$ (где $b \in B$).

Гауссовой полугруппой называется абелева полугруппа $\mathcal{G} = (G, \diamond)$ с нейтральным элементом, удовлетворяющая закону сокращения, в которой каждый элемент $a \in G \setminus G^{inv}$ разлагается в произведение неприводимых элементов, причем любые два такие разложения *ассоциированы* между собой, т.е. если $a = b_1 \dots b_m$ и $a = c_1 \dots c_l$ – разложения элемента a в произведения неприводимых элементов, то $l = m$ и существует такая подстановка f, принадлежащая симметрической группе $\mathcal{S}(m)$, что

элементы b_i $(i = 1, \ldots, m)$ и $c_{f(i)}$ ассоциированы.

Отсюда вытекает, что любые два элемента гауссовой полугруппы имеют наибольший общий делитель.

Замечание 1.7. Существует класс конечных абелевых полугрупп $\mathcal{G} = (G, \diamond)$ с нейтральным элементом, которые не являются полугруппами с сокращением (а, следовательно, не являются гауссовыми полугруппами), но которые удовлетворяют следующим условиям:

1) $\mathcal{G}$ – полугруппа с нулем;

2) множества $a \diamond G^{inv}$ $(a \in G)$ – это классы *ассоциированных* элементов;

3) $p \in G \setminus G^{inv}$ – *неприводимый* элемент, если из равенства $p = a \diamond b$ вытекает, что один из элементов a, b – делитель нейтрального элемента;

4) каждый элемент $a \in G \setminus G^{inv}$ разлагается единственным образом (с точностью до ассоциированного разложения) в произведение неприводимых элементов (отсюда, в частности, вытекает равенство множеств неприводимых и простых элементов, а также существование наибольшего общего делителя для любых элементов $a, b \in G$);

Этому классу полугрупп принадлежат полугруппы $\mathcal{Z}_n = (\mathbf{Z}_n, \circ)$ $(n \in \mathbf{N},\ n \geq 2)$, где

$$a \circ b = ab\ (mod\ n).$$

В этом случае $\mathbf{Z}_n^{inv}$ является множеством всех чисел $m \in \mathbf{Z}_n$, взаимно-простых с числом n.

Отметим, что если $n = p^k$ (p – простое число, $k \in \mathbf{N}$ $(k \geq 2)$, то каждый элемент $a \in \mathbf{Z}_{p^k} \setminus \mathbf{Z}_{p^k}^{inv}$ является *нильпотентным*, т.е. существует такое $m \in \mathbf{N}$, что $a^m = 0$.

В дальнейшем, в соответствии с традицией, будем использовать следующие обозначения.

Запись $\mathcal{G} = (G, \cdot)$ (мультипликативное представление) используется для обозначения произвольного группоида, полугруппы или группы. При этом вместо вместо $a \cdot b$ пишут ab, а нейтральный элемент (если он существует) называется *единицей* (обозначается 1).

Запись $\mathcal{G} = (G, +)$ (аддитивное представление) используется, когда хотят подчеркнуть, что $\mathcal{G}$ – абелева группа. Ее нейтральный элемент называется *нулем* (обозначается 0), обратный к $a \in G$ элемент называется *противоположным* элементом (обозначается $-a$), а запись na $(n \in \mathbf{Z},\ a \in G)$ имеет следующий смысл

$$na = \underbrace{a + \cdots + a}_{n}\ (n \in \mathbf{N}),$$

$$0a = 0,$$

$$(-n)a = -(na)\ (n \in \mathbf{N}).$$

Абелева полугруппа $\mathcal{Z}_n = (\mathbf{Z}_n, \circ)$ $(n \in \mathbf{N},\ n \geq 2)$ определена в замечании 1.3.

Запись $\mathcal{Z}_n = (\mathbf{Z}_n, \oplus)$ $(n \in \mathbf{N},\ n \geq 2)$ будет использоваться для абелевой группы, в которой

$$a \oplus b = a + b\,(mod\, n).$$

1.1.2. Кольца.

Кольцом называется такая алгебраическая система $\mathcal{K} = (K, +, \cdot)$, что $(K, \cdot)$ – группоид, $(K, +)$ – абелева группа, а операции «$\cdot$» и «$+$» связаны законами *дистрибутивности*: $a(b+c) = ab + ac$ и $(b+c)a = ba + ca$ для всех $a, b, c \in K$.

Группоид $(K, \cdot)$ называется *мультипликативным* группоидом кольца $\mathcal{K}$, а абелева группа $(K, +)$ – *аддитивной* группой кольца $\mathcal{K}$.

Замечание 1.8. Из законов дистрибутивности непосредственно вытекает, что кольцо $\mathcal{K} = (K, +, \cdot)$ является $(\Omega_1 \cup \Omega_2)$-операторной абелевой группой $(K, +)$, где

$$\Omega_1 = \{\omega_a^{(1)}\ (a \in K) | \omega_a^{(1)}(x) = ax\ (x \in K)\},$$

$$\Omega_2 = \{\omega_a^{(2)}\ (a \in K) | \omega_a^{(2)}(x) = xa\ (x \in K)\}.$$

В кольце $\mathcal{K} = (K, +, \cdot)$ через «$-$» обозначается операция, обратная операции «$+$», т.е. $a - b = c$ $(a, b, c \in K)$ тогда и только тогда, когда $a = b + c$. Для операции «$-$» также истинны законы дистрибутивности: $a(b-c) = ab - ac$ и $(b-c)a = ba - ca$ для всех $a, b, c \in K$.

Замечание 1.9. Для кольца $\mathcal{Z}_n = (\mathbf{Z}_n, \oplus, \circ)$ $(n \in \mathbf{N},\ n \geq 2)$ операция, обратная операции «$\oplus$» обозначается через «$\ominus$».

В любом кольце $\mathcal{K} = (K, +, \cdot)$ нейтральный элемент $0 \in K$ абелевой группы $(K, +)$ обладает тем свойством, что $0a = a0 = 0$ для всех $a \in K$.

Кольцо $\mathcal{K} = (K, +, \cdot)$ называется *кольцом с делением*, если для любых $a, b \in K$ $(a \neq 0)$ уравнения $ax = b$ и $ya = b$ имеют решения (т.е. если $(K, \cdot)$ – квазигруппа).

Подкольцом кольца $\mathcal{K} = (K, +, \cdot)$ называется такая алгебраическая система $\mathcal{K}_1 = (K_1, +, \cdot)$ $(K_1 \subseteq K)$, что $\mathcal{K}_1$ – кольцо.

Замечание 1.10. Само кольцо $\mathcal{K}$ называется *надкольцом* кольца $\mathcal{K}_1$.

Подкольцами любого кольца $\mathcal{K} = (K, +, \cdot)$ являются *нуль-кольцо* $\mathcal{O} = (\{0\}, +, \cdot)$ и кольцо $\mathcal{K}$. Эти подкольца называются *несобственными*. Все остальные подкольца кольца $\mathcal{K}$ (если такие существуют) называются *собственными*. Истинно утверждение: *пересечение любого множества подколец кольца $\mathcal{K}$ является подкольцом кольца $\mathcal{K}$*. Кольцо, не содержащее ни одного собственного подкольца, называется *простым кольцом*.

Левым (*соответственно, правым*) *идеалом* кольца $\mathcal{K} = (K, +, \cdot)$ называется такое непустое подмножество I множества K, что $(I, +)$ – подгруппа абелевой группы $(K, +)$ и истинно включение $KI \subseteq I$ (соответственно, $IK \subseteq I$).

Замечание 1.11. Если I – левый или правый идеал кольца $\mathcal{K}$, то $\mathcal{I} = (I, +, \cdot)$ – подкольцо кольца $\mathcal{K}$. Обратное утверждение не всегда истинно.

Если множество I одновременно является и левым, и правым идеалом кольца $\mathcal{K}$, то I называется (двусторонним) *идеалом* кольца $\mathcal{K}$. Идеалами любого кольца $\mathcal{K}$ являются $\{0\}$ (*нулевой* идеал) и множество K. Эти идеалы называются *несобственными*. Остальные идеалы (если они существуют) называются *собственными*.

Кольцо $\mathcal{K}$ называется *простым*, если оно не имеет собственных идеалов.

Замечание 1.12. В кольце с делением отсутствуют как левые, так и правые собственные идеалы.

Следовательно, в кольце с делением отсутствуют собственные идеалы.

Отсюда вытекает, что любое кольцо с делением – простое кольцо.

Пусть I – идеал кольца $\mathcal{K} = (K, +, \cdot)$, а «$\equiv_I$» – такое отношение эквивалентности на множестве K, что $a \equiv_I b$ $(a, b \in K)$ тогда и только тогда, когда $a - b \in I$. Тогда кольцом является

$$\mathcal{K}/_{\equiv_I} = (K/_{\equiv_I}, +_I, \cdot_I),$$

где $K/_{\equiv_I} = \{a + I | a \in K\}$, а операции $+_I$ и $\cdot_I$ определены равенствами

$$(a + I) +_I (b + I) = (a + b) + I,$$

$$(a + I) \cdot_I (b + I) = ab + I.$$

Кольцо $\mathcal{K}/_{\equiv_I}$ называется *фактор-кольцом* кольца $\mathcal{K}$ по идеалу I, а элементы множества $K/_{\equiv_I}$ – *классами вычетов* по идеалу I.

Запись $a \equiv b \,(\mathrm{mod}\, I)$ $(a, b \in K)$ означает утверждение о том, что элементы a и b кольца $\mathcal{K}$ принадлежат одному и тому же классу вычетов по идеалу I.

Пусть $\mathcal{K}_1 = (K_1, +_1, \cdot_1)$ и $\mathcal{K}_2 = (K_2, +_2, \cdot_2)$ – кольца. Говорят, что:

1) кольцо $\mathcal{K}_2$ является *гомоморфным образом* кольца $\mathcal{K}_1$, если существует такая сюръекция $f : K_1 \to K_2$, что $f(a+_1 b) = f(a)+_2 f(b)$ и $f(a\cdot_1 b) = f(a)\cdot_2 f(b)$ для любых $a, b \in K_1$ (отображение f называется *гомоморфизмом* $\mathcal{K}_1$ на $\mathcal{K}_2$);

2) кольца $\mathcal{K}_1$ и $\mathcal{K}_2$ *изоморфны* (друг другу), если существует такая биекция $f : K_1 \to K_2$, что $f(a+_1 b) = f(a)+_2 f(b)$ и $f(a\cdot_1 b) = f(a)\cdot_2 f(b)$ для любых $a, b \in K_1$ (отображение f называется *изоморфизмом* между $\mathcal{K}_1$ и $\mathcal{K}_2$).

Существует следующая связь между идеалами и гомоморфизмами колец: *если сюръекция $f : K_1 \to K_2$ – гомоморфизм кольца $\mathcal{K}_1$ на кольцо $\mathcal{K}_2$ то $f^{-1}(0_2)$ – идеал кольца $\mathcal{K}_1$* (где 0_2 – нуль кольца $\mathcal{K}_2$).

Множество $f^{-1}(e_{\mathcal{H}})$ называется *ядром гомоморфизма* f и обозначается $\ker f$. Истинно утверждение: *если I_1 и I_2 – такие идеалы кольца $\mathcal{K} = (K, +, \cdot)$, что $I_1 \subseteq I_2$, то существует гомоморфизм фактор-кольца $\mathcal{K}/_{\equiv_{I_1}}$ на фактор-кольцо $\mathcal{K}/_{\equiv_{I_2}}$*.

В зависимости от свойств мультипликативного группоида выделяют следующие типы колец. Кольцо $\mathcal{K} = (K, +, \cdot)$ называется:

1) *ассоциативным*, если $(K, \cdot)$ – полугрупа, и *неассоциативным*, если группоид $(K, \cdot)$ не является полугруппой;

2) *коммутативным*, если группоид $(K, \cdot)$ – абелев, и *некоммутативным*, если группоид $(K, \cdot)$ не является абелевым;

3) *кольцом с единицей*, если группоид $(K, \cdot)$ содержит единицу, и *кольцом без единицы*, если группоид $(K, \cdot)$ не содержит единицу.

Замечание 1.13. В кольце $\mathcal{K} = (K, +, \cdot)$ равенство $0 = 1$ истинно тогда и только тогда, когда $|K| = 1$.

4) *лиевым кольцом*, если для всех элементов $a, b, c \in K$ выполняются равенства $a^2 = 0$ и $(ab)c + (bc)a + (ca)b = 0$ (*тождество Якоби*).

Замечание 1.14. В лиевом кольце выполняется *закон антикоммутативности*: $ab = -ba$ $(a, b \in K)$.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо с единицей $e \in K$. Положим

$$\mathcal{K}_e = (\{ne | n \in \mathbf{Z}\}, +, \cdot),$$

где

$$n_1 e + n_2 e = (n_1 + n_2)e,$$
$$(n_1 e)(n_2 e) = (n_1 n_2)e$$

для любых $n_1, n_2 \in \mathbf{Z}$.

Кольцо $\mathcal{K}_e$ является наименьшим подкольцом кольца $\mathcal{K}$, содержащим единицу.

Если в кольце $\mathcal{K} = (K, +, \cdot)$ для элементов $a, b \in K \setminus \{0\}$ выполнено равенство $ab = 0$, то a называется *левым*, а b – *правым делителем нуля*. В случае, когда $\mathcal{K}$ – ассоциативно-коммутативное кольцо, указанные элементы a и b называются *делителями нуля*.

Пусть $\mathcal{K}$ – ассоциативно-коммутативное кольцо, а $\mathcal{K}_1$ – подкольцо кольца $\mathcal{K}$. Возможны следующие три различные ситуации:

1. Оба кольца $\mathcal{K}$ и $\mathcal{K}_1$ не содержат единицы.

2. Оба кольца $\mathcal{K}$ и $\mathcal{K}_1$ содержат единицу и эти единицы совпадают. Тогда $\mathcal{K}_1$ называется *унитарным подкольцом* кольца $\mathcal{K}$, а само $\mathcal{K}$ – *унитарным надкольцом* кольца $\mathcal{K}_1$.

3. Кольцо $\mathcal{K}_1$ содержит единицу, а кольцо $\mathcal{K}$ либо не содержит единицы, либо единица кольца $\mathcal{K}$ отлична от единицы кольца $\mathcal{K}_1$. Тогда единица кольца $\mathcal{K}_1$ является делителем нуля в кольце $\mathcal{K}$.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативное кольцо с единицей. *Множеством обратимых элементов кольца* $\mathcal{K}$ называется множество K^{inv} обратимых элементов полугруппы $(K, \cdot)$.

Группа $(K^{inv}, \cdot)$ называется *мультипликативной группой кольца* $\mathcal{K}$. Любой левый или правый делитель нуля кольца $\mathcal{K}$ принадлежит множеству $(K \setminus \{0\}) \setminus K^{inv}$.

Если $K^{inv} = K \setminus \{0\}$, то кольцо $\mathcal{K}$ называется *телом*.

Коммутативное тело называется *полем*.

Замечание 1.15. В кольце $\mathcal{Z}_n = (\mathbf{Z}_n, \oplus, \circ)$ $(n \in \mathbf{N},\ n \geq 2)$ множество $\mathbf{Z}_n^{inv}$ состоит из всех чисел $a \in \mathbf{Z}_n$, взаимно-простых с числом n (см. замечание 1.7).

Следовательно, $\mathcal{Z}_n$ $(n \in \mathbf{N},\ n \geq 2)$ является полем тогда и только тогда, когда n – простое число.

Если для кольца $\mathcal{K} = (K, +, \cdot)$ существует такое число $n \in \mathbf{N}$, что $nx = 0$ для всех $x \in K$, то наименьшее из таких чисел $n \in \mathbf{N}$ называется *характеристикой* кольца $\mathcal{K}$. Если же указанное число $n \in \mathbf{N}$ не существует, то говорят, что $\mathcal{K}$ – кольцо *характеристики* 0.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо. Обозначим через $S_{\mathcal{K}}$ множество всех элементов $x \in K \backslash \{0\}$, на которые допустимы сокращения в кольце $\mathcal{K}$. Истинно утверждение: *ассоциативно-коммутативное кольцо $\mathcal{K}$ можно изоморфно вложить в такое ассоциативно-коммутативное кольцо $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ с единицей, что каждый элемент $x \in S_{\mathcal{K}}$ имеет в кольце $\overline{\mathcal{K}}$ обратный элемент.*

Замечание 1.16. Ассоциативно-коммутативное кольцо $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ с единицей строится в соответствии со схемой, представленной в замечании 1.6.

Действительно, пусть $R_{\mathcal{K}} = \{\frac{a}{x} | a \in K,\ x \in S_{\mathcal{K}}\}$ – множество *дробей* (*частных*) над кольцом $\mathcal{K}$.

Положив

$$\frac{a}{x} + \frac{b}{y} = \frac{ay + bx}{xy}$$

и

$$\frac{a}{x} \cdot \frac{b}{y} = \frac{ab}{xy}$$

для любых $\frac{a}{x}, \frac{b}{y} \in R_{\mathcal{K}}$, получим алгебраическую систему $\mathcal{R}_{\mathcal{K}} = (R_{\mathcal{K}}, +, \cdot)$.

Пусть «$\equiv$» – такое отношение эквивалентности на множестве $R_{\mathcal{K}}$, что $\frac{a}{x} \equiv \frac{b}{y}$ тогда и только тогда, когда $ay = bx$. Положим $\overline{K} = R_{\mathcal{K}}/_{\equiv}$ и определим на множестве $\overline{K}$ операции «$+$» и «$\cdot$» следующим образом: если $H_1, H_2 \in \overline{K}$ ($\frac{a}{x} \in H_1, \frac{b}{y} \in H_2$), то $H_1 + H_2 = H$, где $\frac{ay+bx}{xy} \in H$ и $H_1 H_2 = H$, где $\frac{ab}{xy} \in H$.

Получим ассоциативно-коммутативное кольцо с единицей $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$, которое называется *кольцом дробей* (*кольцом частных*) над кольцом $\mathcal{K}$.

Единицей кольца $\overline{\mathcal{K}}$ является элемент $\{\frac{x}{x} | x \in S_{\mathcal{K}}\}$. Элементу $a \in K$ кольца $\mathcal{K}$ соответствует элемент $\{\frac{ax}{x} | x \in S_{\mathcal{K}}\}$ кольца $\overline{\mathcal{K}}$, а элементом кольца $\overline{\mathcal{K}}$, обратным элементу $\{\frac{ax}{x} | x \in S_{\mathcal{K}}\}$ ($a \in S_{\mathcal{K}}$) является элемент $\{\frac{x}{ax} | x \in S_{\mathcal{K}}\}$.

Областью целостности называется ассоциативно-коммутативное кольцо $\mathcal{K} = (K, +, \cdot)$ без делителей нуля. Истинно утверждение: *если $\mathcal{K} = (K, +, \cdot)$ – область целостности, то кольцо частных $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ – поле.* Это поле называется *полем частных* (или *полем дробей*) над областью целостности $\mathcal{K}$.

Для любых идеалов I_1 и I_2 ассоциативно-коммутативного кольца $\mathcal{K}$ множество $I = I_1 I_2$ является идеалом. Если при этом $I \neq I_1$ и $I \neq I_2$, то говорят, что идеал I *разложим* (в произведение идеалов I_1 и I_2).

Простым идеалом ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ называется такой его собственный идеал I, что если $ab \in I$ $(a, b \in K)$, то $a \in I$ или

$b \in I$. Истинно утверждение: *собственный идеал I кольца $\mathcal{K}$ является простым тогда и только тогда, когда для любых идеалов A, B кольца $\mathcal{K}$ из $AB \subseteq I$ следует, что $A \subseteq I$ или $B \subseteq I$*. Отсюда вытекает, что:

1) каждый максимальный (по включению) собственный идеал ассоциативного кольца является простым идеалом;

2) если ассоциативно-коммутативное кольцо $\mathcal{K}$ содержит единицу, а I – простой идеал, то $\mathcal{K}/\equiv_I$ – поле.

Пример 1.1. Если число $n \in \mathbf{N}$ ($n \geq 2$) не является простым, а $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ ($\alpha_1, \dots \alpha_m \in \mathbf{N}$) – каноническое разложение числа n, то кольцо $\mathcal{Z}_n = (\mathbf{Z}_n, \oplus, \circ)$ содержит m простых идеалов, а именно: $(p_1), \dots, (p_m)$.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо. *Радикалом* идеала I кольца $\mathcal{K}$ называется идеал $\sqrt{I}$ кольца $\mathcal{K}$, состоящий из всех таких элементов $a \in K$, что $a^n \in I$ для некоторого $n \in \mathbf{N}$. Идеал $\sqrt{(0)}$ состоит из всех нильпотентных элементов кольца $\mathcal{K}$ и называется *радикалом кольца $\mathcal{K}$*.

Ясно, что $I \subseteq \sqrt{I}$ и $\sqrt{\sqrt{I}} = \sqrt{I}$ для любого идеала I кольца $\mathcal{K}$. Истинно утверждение: *если I_1 и I_2 – такие идеалы кольца $\mathcal{K}$*, что $I_1^n \subseteq I_2$ *для некоторого $n \in \mathbf{N}$, то*

$$\sqrt{I_1} \subseteq \sqrt{I_2},$$

$$\sqrt{I_1 I_2} = \sqrt{I_1 \cap I_2}\ (= \sqrt{I_1} \cap \sqrt{I_2}),$$

$$\sqrt{I_1 + I_2} = \sqrt{\sqrt{I_1} + \sqrt{I_2}}.$$

Идеал I ассоциативно-коммутативного кольца $\mathcal{K} = (K, +, \cdot)$ называется *радикальным*, если он удоветворяет следующему условию:

$$(\forall a \in K)((\exists n \in \mathbf{N})(a^n \in I) \Rightarrow a \in I).$$

Дедекиндовым кольцом называется область целостности с единицей, в которой каждый собственный идеал единственным образом разложим в произведение конечного числа простых идеалов.

Базисом идеала I ассоциативно-коммутативного кольца $\mathcal{K} = (K, +, \cdot)$ называется любое такое подмножество $M \subseteq I$, что $M \not\subseteq I_1$ для любого идеала $I_1 \subset I$.

Идеал называется *конечно-порожденным*, если он имеет конечный базис. Если $M = \{a_1, \ldots, a_n\}$ – базис идеала I (в этом случае пишут $I = (a_1, \ldots, a_n)$), то

$$I = \sum_{i=1}^{n} Ka_i + \sum_{i=1}^{n} \mathbf{Z}a_i.$$

В частности, если $\mathcal{K}$ – кольцо с единицей, то истинно равенство

$$I = \sum_{i=1}^{n} Ka_i.$$

Замечание 1.17. Пусть I – конечно-порожденный идеал ассоциативно-коммутативного кольца $\mathcal{K}$. Базис $M = \{a_1, \ldots, a_n\}$ идеала I называется *минимальным*, если никакое собственное подмножество множества M не является базисом идеала I. Идеал I может иметь минимальные базисы, состоящие из различного числа элементов.

Нетеровым кольцом называется ассоциативно-коммутативное кольцо с единицей, в котором каждый идеал имеет конечный базис.

Замечание 1.18. Любое конечное ассоциативно-коммутативное кольцо с единицей – нетерово кольцо.

Ассоциативно-коммутативное кольцо с единицей называется *примарным*, если оно содержит единственный простой идеал.

Пример 1.2. Так как в кольце $\mathcal{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ (p – простое число, $k \in \mathbf{N}$ ($k \geq 2$)) единственным простым идеалом является (p), то $\mathcal{Z}_{p^k}$ – примарное кольцо.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо. *Главным идеалом*, порождаемым элементом a называется идеал

$$(a) = \{ax + na | x \in K,\ n \in \mathbf{Z}\}.$$

Замечание 1.19. Ясно, что нулевой идеал является главным идеалом любого ассоциативно-коммутативного кольца.

Для любого элемента $a \in K$ главный идеал (a) является наименьшим идеалом, содержащим элемент a. Если кольцо $\mathcal{K}$ содержит единицу, то

$$(a) = aK.$$

Пример 1.3. Существует $k-1$ собственный идеал кольца $\mathcal{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ (p – простое число, $k \in \mathbf{N}$ $(k \geq 2)$), а именно: $(p), (p^2), \ldots, (p^{k-1})$, т.е. каждый собственный идеал кольца $\mathcal{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ – главный идеал.

Замечание 1.20. Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо с единицей, не содержащее делителей нуля, а ненулевой элемент $a \in K \backslash K^{inv}$ представлен в виде $a = a_1^{\alpha_1} \ldots a_l^{\alpha_l}$ $(\alpha_1, \ldots, \alpha_l \in \mathbf{N})$, где $a_1, \ldots, a_l$ – попарно неассоциированные неприводимые элементы кольца $\mathcal{K}$. Тогда

$$\sqrt{(a)} = (a_1 \ldots, a_l).$$

Кроме того, если $a = a_1^{\alpha_1} \ldots a_l^{\alpha_l}$ $(\alpha_1, \ldots, \alpha_l \in \mathbf{Z}_+)$ и $b = a_1^{\beta_1} \ldots a_l^{\beta_l}$ $(\beta_1, \ldots, \beta_l \in \mathbf{Z}_+)$ – разложения элементов $a, b \in K \backslash K^{inv}$ в произведения попарно неассоциированных неприводимых элементов кольца $\mathcal{K}$, то

$$(a) \cap (b) = (c),$$

где $c = a_1^{\gamma_1} \ldots a_l^{\gamma_l}$, а $\gamma_i = \max\{\alpha_i, \beta_i\}$ $(i = 1, \ldots, l)$.

Гауссовым кольцом называется такая область целостности с единицей $\mathcal{K} = (K, +, \cdot)$, что $(K \setminus \{0\}, \cdot)$ гауссова полугруппа.

Кольцом главных идеалов называется область целостности с единицей, в котором каждый собственный идеал – главный. Истинно утверждение: *каждое кольцо главных идеалов – гауссово кольцо.*

В кольце $\mathcal{K} = (K, +, \cdot)$ главных идеалов простыми идеалами являются такие идеалы (p), что p – простой элемент абелевой полугруппы $(K, \cdot)$. При этом, если $a \in (K \setminus \{0\}) \setminus K^{inv}$ и $a = p_1 \ldots p_n$ – разложение элемента a в произведение простых множителей, то

$$(a) = (p_1) \ldots (p_n).$$

Замечание 1.21. Кольцо $\mathcal{Z}_n = (\mathbf{Z}_n, \oplus, \circ)$ не является кольцом главных идеалов, если число $n \in \mathbf{N}$ $(n \geq 2)$ не является простым.

Пусть $n = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$ $(\alpha_1, \ldots \alpha_m \in \mathbf{N})$ – каноническое разложение, а каноническое разложение числа $a \in (\mathbf{Z}_n \setminus \{0\}) \setminus \mathbf{Z}_n^{inv}$ имеет вид

$$a = \alpha p_{i_1}^{\beta_1} \ldots p_{i_r}^{\beta_r} \ (1 \leq i_1 < \cdots < i_r \leq m,\ 1 \leq \beta_j \leq \alpha_{i_j}\ (j = 1, \ldots, r)).$$

где $\alpha \in \mathbf{Z}_n^{inv}$. Тогда

$$(a) = (p_{i_1})^{\beta_1} \ldots (p_{i_r})^{\beta_r},$$

т.е. в кольце $\mathcal{Z}_n$ каждый ненулевой главный идеал единственным образом представим в виде произведения простых идеалов.

Евклидовым кольцом называется область целостности $\mathcal{K} = (K, +, \cdot)$ с единицей, в которой каждому элементу $x \in K \setminus \{0\}$ можно поставить в соответствие такое число $n(x) \in \mathbf{Z}_+$, что:

1) если $b \in K$ – делитель элемента $a \in K \setminus \{0\}$, то $n(b) \leq n(a)$;

2) для любых элементов $a, b \in K$ $(b \neq 0)$ существуют такие элементы $q, r \in K$, что $a = bq + r$, причем либо $r = 0$, либо $n(r) < n(b)$.

Истинно утверждение: *любое евклидово кольцо является кольцом главных идеалов.*

Замечание 1.22. В любом евклидовом кольце $\mathcal{K} = (K, +, \cdot)$ для поиска наибольшего общего делителя элементов $a, b \in K \setminus \{0\}$ применим алгоритм Евклида.

Пусть $\mathcal{K} = (K, +, \cdot)$ – область целостности с единицей, а $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ – поле частных. *Дробным идеалом* кольца $\mathcal{K}$ называется такое множество $A \subseteq \overline{K}$, что выполнены следующие три условия:

1) $(A, +)$ – подгруппа абелевой группы $(\overline{K}, +)$;

2) если $a \in A$ и $x \in K$, то $ax \in A$;

3) существует такой элемент $d \in K \setminus \{0\}$ и такой идеал A_0 кольца $\mathcal{K}$, что $A = \frac{1}{d}A_0$ (т.е. каждый элемент множества A – это дробь с знаменателем d).

Замечание 1.23. Идеалы области целостности с единицей $\mathcal{K}$ (их называют *целыми идеалами*) принадлежат множеству дробных идеалов.

Множество всех дробных идеалов области целостности с единицей $\mathcal{K}$ является абелевой полугруппой, если операцию умножения определить следующим образом: если $A = \frac{1}{c}A_0$ и $B = \frac{1}{d}B_0$, то $AB = \frac{1}{cd}A_0B_0$.

Подполугруппой этой полугруппы является множество всех ненулевых дробных идеалов.

Ненулевой дробный идеал – *обратимый*, если существует такой дробный идеал A^{-1}, что $AA^{-1} = K$, а каждый ненулевой главный дробный идеал $\frac{1}{d}(a) = \left(\frac{a}{d}\right)$ обратим, так как $\left(\frac{a}{d}\right)^{-1} = \left(\frac{d}{a}\right)$.

Каждый обратимый дробный идеал порождается конечным множеством элементов. Истинно утверждение: *область целостности с единицей является дедекиндовым кольцом тогда и только тогда, когда полугруппа ее ненулевых дробных идеалов является группой.*

Отсюда вытекает, что каждый ненулевой дробный идеал дедекиндового кольца раскладывается в произведение положительных или отрицательных степеней простых идеалов.

Кольцом дискретного нормирования называется примарное кольцо $\mathcal{K} = (K, +, \cdot)$ главных идеалов (т.е. кольцо главных идеалов, имеющее

единственный простой идеал). Если (t) – простой идеал кольца $\mathcal{K}$, то каждый элемент $x \in K \setminus \{0\}$ единственным образом представим в виде $x = t^r y$ $(r \in \mathbf{Z}_+)$, где $y \in K^{inv}$, а $t^0 = 1$. Элемент t называется *локальным параметром*, и говорят, что кольцо $\mathcal{K}$ допускает *локальную параметризацию*.

Замечание 1.24. Хотя кольцо $\mathcal{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ (p – простое число, $k \in \mathbf{N}$ $(k \geq 2)$) не является кольцом дискретного нормирования, оно допускает локальную параметризацию, так как любой элемент $x \in \mathbf{Z}_{p^k} \setminus \{0\}$ может быть представлен в виде $x = p^r y$, где $r \in \mathbf{Z}_k$ и $y \in \mathbf{Z}_{p^k}^{inv}$.

Учитывая это обстоятельство, в [52] следующим образом определен *p-тип* $\mathtt{t}_p(z)$ элемента $z \in \mathbf{Z}_{p^k}$

$$\mathtt{t}_p(z) = \begin{cases} 0, & \text{если } z \in \mathbf{Z}_{p^k}^{inv} \\ r \ (1 \leq r \leq k-1), & \text{если } z \equiv 0 \,(mod\, p^r) \text{ и } z \not\equiv 0 \,(mod\, p^{r+1}) \\ k, & \text{если } z = 0 \end{cases}. \qquad (1.1)$$

Из (1.1) вытекает, что:

1) $\mathtt{t}_p(u \circ v) = \min\{k, \mathtt{t}_p(u) + \mathtt{t}_p(v)\}$ $(u, v \in \mathbf{Z}_{p^k})$;

2) $\mathtt{t}_p(u \oplus v) = \min\{\mathtt{t}_p(u), \mathtt{t}_p(v)\}$ $(u, v \in \mathbf{Z}_{p^k})$, если $u \oplus v \neq 0$;

3) если $\mathtt{t}_p(u \oplus v) = 0$ $(u, v \in \mathbf{Z}_{p^k})$, то $\min\{\mathtt{t}_p(u), \mathtt{t}_p(v)\} = 0$;

4) $\mathtt{t}_p(u) = \mathtt{t}_p(v)$ $(u, v \in \mathbf{Z}_{p^k})$ тогда и только тогда, когда элементы u и v принадлежат одному и тому же классу ассоциированных элементов кольца $\mathcal{Z}_{p^k}$.

В силу последнего свойства понятие «p-тип $\mathtt{t}_p(z)$ элемента кольца $\mathcal{Z}_{p^k}$» определяет биекцию классов ассоциированных элементов кольца $\mathcal{Z}_{p^k}$ на множество $\mathbf{Z}_{k+1}$.

Поэтому для того, чтобы задать класс ассоциированных элементов кольца $\mathcal{Z}_{p^k}$, достаточно зафиксировать p-тип $\mathtt{t}_p(z)$ элемента, принадлежащего этому классу.

В разделе 4 будет показано, что именно это обстоятельство дает возможность сокращать перебор в процессе решения уравнений над конечными кольцами.

Любой ненулевой элемент x поля частных $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ кольца дискретного нормирования $\mathcal{K}$ также представим в виде $x = t^r y$, где $r \in \mathbf{Z}$, а $y \in K^{inv}$. Элемент $t \in K$ называется *локальным параметром*, а число r – *порядком* (или *нормой*) ненулевого элемента $x \in \overline{K}$ и обозначается $\mathtt{ord}_{\mathcal{K}}(x)$.

Говорят, что ненулевой элемент $x \in K \setminus \{0\}$ имеет при данном нормировании:

1) *нуль*, если $\mathtt{ord}_{\mathcal{K}}(x) > 0$;

2) *полюс*, если $\mathtt{ord}_{\mathcal{K}}(x) < 0$.

Следующая детализация операторного группоида в терминах теории колец приводит к понятию «*модуль*» – одному из основных понятий, предназначенных для унифицированного исследования внутренних свойств и представлений алгебраических систем.

Пусть $\mathcal{G} = (G, +)$ – абелева группа, а $\mathcal{K} = (K, +, \cdot)$ – кольцо отображений множества G в себя. Множество G называется $\mathcal{K}$-*модулем*, если выполнены следующие условия:

1) единица кольца $\mathcal{K}$, если она существует, является тождественным отображением множества G;

2) равенство $(a+b)(g) = a(g)+b(g)$ истинно для всех $a, b \in K$ и $g \in G$;

3) равенство $a(u+v) = a(u)+a(v)$ истинно для всех $a \in K$ и $u, v \in G$;

4) равенство $(ab)(g) = a(b(g))$ истинно для всех $a, b \in K$ и $g \in G$.

Замечание 1.25. В определении модуля первое свойство имеет значение только для колец с единицей. Модули над такими кольцами называются *унитарными*.

Подмодулем $\mathcal{K}$-модуля G называется такое подмножество $G_1 \subseteq G$, что $\mathcal{G} = (G_1, +)$ – подгруппа группы $\mathcal{G} = (G, +)$, причем $a(g) \in G_1$ для всех $a \in K$ и $g \in G_1$.

При этом множество

$$G/_{G_1} = \{g + G_1 | g \in G\}$$

называется *фактор-модулем*, а действие элементов кольца $\mathcal{K}$ на элементы множества $G/_{G_1}$ определяется равенством

$$a(g + G_1) = a(g) + G_1.$$

Пусть U и V – $\mathcal{K}$-модули. $\mathcal{K}$-*гомоморфизмом* U в V называется такое отображение $\sigma : U \to V$, что $\sigma(u_1 + u_2) = \sigma(u_1) + \sigma(u_2)$ $(u_1, u_2 \in U)$ и $\sigma(a(u)) = a(\sigma(u))$ $(a \in K, u \in U)$. Истинно утверждение: *если отображение* $\sigma : U \to V$ *является* $\mathcal{K}$-*гомоморфизмом* U в V, *то*

$$\ker \sigma = \{u \in U | \sigma(u) = 0\}$$

является подмодулем модуля U.

Пример 1.4. 1. Любой левый (соответственно, правый) идеал I ассоциативного кольца $\mathcal{K} = (K, +, \cdot)$ является K-модулем, если действие элементов кольца на элементы идеала I определить равенством $a(x) = ax$ (соответственно, равенством $a(x) = xa$) для всех $a \in K$ и $x \in I$.

2. По определению, *векторным* (или *линейным*) пространством называется унитарный модуль над телом (в частности, над полем).

Для любого кольца $\mathcal{K} = (K, +, \cdot)$ абелевой группой является $(K^n, +)$ $(n \in \mathbf{N})$, где

$$\mathbf{a} + \mathbf{b} = (a_1 + b_1, \ldots, a_n + b_n)$$

для любых $\mathbf{a} = (a_1, \ldots, a_n) \in K^n$ и $\mathbf{b} = (b_1, \ldots, b_n) \in K^n$.

Определим действие элементов кольца на элементы абелевой группы равенством

$$a(\mathbf{a}) = (aa_1, \ldots, aa_n) \ (a \in K, \mathbf{a} = (a_1, \ldots, a_n) \in K^n).$$

В этом случае вместо $a(\mathbf{a})$ $(\mathbf{a} \in K^n)$ пишут $a\mathbf{a}$.

Если $\mathcal{K}$ – ассоциативное кольцо, то множество K^n является $\mathcal{K}$-модулем (но не векторным пространством, если $\mathcal{K}$ не является телом).

3. Если $\mathcal{K} = (K, +, \cdot)$ – поле, то $\mathcal{K}$-модуль K^n $(n \in \mathbf{N})$ называется *n-мерным аффинным пространством* над полем $\mathcal{K}$.

В частности, $K^1 = K$ – *аффинная прямая*, а K^2 – *аффинная плоскость*.

1.1.3. Кольца многочленов и рядов.

В настоящем пункте под кольцом $\mathcal{K} = (K, +, \cdot)$ понимается ассоциативно-коммутативное кольцо.

Многочленом над кольцом $\mathcal{K}$ от переменной x называется выражение

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \ (m \in \mathbf{Z}_+),$$

где $a_0, a_1, \ldots, a_m \in K$ – *коэффициенты*. Если

$$a_0 = a_1 = \cdots = a_m = 0,$$

то $f(x)$ – *нулевой* многочлен, а если хотя бы один из коэффициентов отличен от нуля, то $f(x)$ – *ненулевой* многочлен.

Степень нулевого многочлена не определена, а степень ненулевого многочлена – такое максимальное число k, что $a_k \neq 0$ (a_k называется *старшим коэффициентом*, а a_0 – *свободным членом* многочлена $f(x)$).

Замечание 1.26. Всюду в дальнейшем предполагается, что для ненулевого многочлена в записи

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m$$

коэффициент a_m – старший член, а нулевой многочлен будет обозначаться 0.

Обозначим через $K[x]$ множество всех многочленов от переменной x над кольцом $\mathcal{K}$.

Два многочлена называются равными, если их коэффициенты совпадают.

Определив обычным образом сложение и умножение многочленов, получим ассоциативно-коммутативное *кольцо*

$$\mathcal{K}[x] = (K[x], +, \cdot)$$

многочленов от переменной x над кольцом $\mathcal{K}$.

Само кольцо $\mathcal{K}$ является подкольцом кольца $\mathcal{K}[x]$ (элементам множества $K \setminus \{0\}$ соответствуют многочлены 0-й степени, а элементу $0 \in K$ – нулевой многочлен).

Если в кольце $\mathcal{K}$ отсутствуют делители нуля, то и в кольце $\mathcal{K}[x]$ отсутствуют делители нуля. В частности, если $\mathcal{K}$ – область целостности, то $\mathcal{K}[x]$ – область целостности.

Многочлен $f(x) \in K[x]$ степени $m \in \mathbf{N}$ называется *разложимым* (в кольце $\mathcal{K}[x]$), если существуют такие многочлены $f_i(x) \in K[x]$ $(i = 1, 2)$ степени $m_i \in \mathbf{N}$ $(m_i < m\,(i = 1, 2))$, что

$$f(x) = f_1(x) f_2(x).$$

В противном случае говорят, что многочлен $f(x) \in K[x]$ *неразложим* (в кольце $\mathcal{K}[x]$).

Замечание 1.27. Если $\mathcal{K}$ – область целостности, то $m = m_1 + m_2$. В противном случае можно только утверждать, что $m \leq m_1 + m_2$.

Подставив в многочлен $f(x) \in K[x]$ вместо переменной x элемент $a \in K$ и выполнив действия, получим элемент $f(a) \in K$.

Таким образом, каждый многочлен $f(x) \in K[x]$ определяет некоторое отображение множества K в себя.

Замечание 1.28. Существуют такие кольца $\mathcal{K}$, что различные многочлены $f_1(x), f_2(x) \in K[x]$ определяют одно и то же отображение множества K в себя.

Пусть «$\equiv$» – отношение эквивалентности, определенное на множестве $K[x]$ следующим образом: $f_1(x) \equiv f_2(x)$ $(f_1(x), f_2(x) \in K[x])$ тогда и только тогда, когда многочлены $f_1(x)$ и $f_2(x)$ определяют одно и то же отображение множества K в себя.

Тогда

$$\mathcal{K}[x]/_{\equiv} = (K[x]/_{\equiv}, +, \cdot)$$

представляет собой ассоциативно-коммутативное фактор-кольцо всех полиномиальных отображений (от одной переменной) множества K в себя.

Элемент $a \in K$ называется *корнем* многочлена $f(x) \in \mathcal{K}[x]$, если $f(a) = 0$. Истинно утверждение: *$a \in K$ – корень многочлена $f(x)$ тогда и только тогда, когда*

$$f(x) = (x - a)g(x),$$

где $g(x) \in K[x]$ – многочлен, степень которого на единицу меньше степени многочлена $f(x)$.

Если

$$f(x) = (x - a)^k g(x) \ (k \in \mathbf{N}),$$

где $g(x) \in K[x]$ – такой многочлен, что $g(a) \neq 0$, то число k называется *кратностью* корня a, а корень a называется *кратным*, если $k \geq 2$. Истинно утверждение: *если $\mathcal{K}$ – область целостности, то любой многочлен $f(x) \in K[x]$ степени $m \in \mathbf{N}$ имеет не больше, чем m корней* (с учетом их кратности).

Производная $\mathsf{D}f(x)$ многочлена

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \in K[x]$$

определяется равенством

$$\mathsf{D}f(x) = a_1 + 2a_2 x + \cdots + m a_m x^{m-1}.$$

Ясно, что $a \in K$ – кратный корень многочлена $f(x) \in K[x]$ тогда и только тогда, когда a – корень многочлена $\mathsf{D}f(x)$.

Замечание 1.29. Для любых двух ненулевых многочленов $f(x), g(x) \in K[x]$ наличие общего корня можно проверить с использованием *результанта* этих многочленов, определяемого следующим образом.

Пусть $f(x) = \sum\limits_{i=0}^{n} a_i x^i \in K[x]$ $(n \in \mathbf{N})$ и $g(x) = \sum\limits_{i=0}^{m} b_i x^i \in K[x]$ $(m \in \mathbf{N})$.

Матрицей Сильвестра многочленов $f(x)$ и $g(x)$ по отношению к x называется $(n + m) \times (n + m)$-матрица

$$\mathrm{Syl}(f, g, x) = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(m)}, \mathbf{b}^{(1)}, \ldots, \mathbf{a}^{(n)}),$$

где

$$\mathbf{a}^{(i)} = (\underbrace{0, \ldots, 0}_{i-1}, a_n, \ldots, a_0, \underbrace{0, \ldots, 0}_{m-i})^T \ (i = 1, \ldots, m),$$

$$\mathbf{b}^{(j)} = (\underbrace{0, \ldots, 0}_{j-1}, b_m, \ldots, b_0, \underbrace{0, \ldots, 0}_{n-i})^T \ (j = 1, \ldots, n).$$

Результантом $\mathrm{Res}(f, g, x)$ многочленов $f(x)$ и $g(x)$ по отношению к x называется определитель матрицы Сильвестра, т.е.

$$\mathrm{Res}(f,g,x) = \det(\mathrm{Syl}(f,g,x)). \tag{1.2}$$

Определитель $k \times k$-матрицы $A = (a_{ij})$ над кольцом $\mathcal{K}$ определяется равенством

$$\det(A) = \sum_{\sigma \in \mathcal{S}(k)} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \dots a_{k\sigma(k)}, \tag{1.3}$$

где $\mathrm{sgn}(\sigma) = 1$, если σ – четная перестановка и $\mathrm{sgn}(\sigma) = -1$, если σ – нечетная перестановка.

Если многочлены $f(x)$ и $g(x)$ имеют общий корень, то $\mathrm{Res}(f,g,x) = 0$.

В случае, когда $\mathcal{K}$ – поле, равенство

$$\mathrm{Res}(f,g,x) = 0$$

истинно тогда и только тогда, когда многочлены $f(x)$ и $g(x)$ имеют общий корень.

Дискриминант $\mathrm{disc}(f)$ многочлена $f(x) = \sum\limits_{i=0}^{n} a_i x^i \in K[x]$ ($\mathcal{K}$ – кольцо с единицей) определяется равенством

$$a_n \mathrm{disc}(f) = (-1)^{0.5n(n-1)} \mathrm{Res}(f, \mathsf{D}f, x). \tag{1.4}$$

Пусть $\mathcal{K}$ – кольцо с единицей. Ясно, что $\mathrm{disc}(f)$ определен однозначно тогда и только тогда, когда старший коэффициент a_n многочлена $f(x)$ не является делителем нуля. При этом, если $a_n \in K^{inv}$, то

$$\mathrm{disc}(f) = a_n^{-1} (-1)^{0.5n(n-1)} \mathrm{Res}(f, \mathsf{D}f, x). \tag{1.5}$$

Из (1.4) вытекает, что если многочлен $f(x) \in K[x]$ со старшим коэффициентом, не являющимся делителем нуля, имеет кратный корень, то $\mathrm{disc}(f) = 0$.

Пусть $\mathcal{K}_1 = (K_1, +, \cdot)$ – унитарное надкольцо кольца $\mathcal{K} = (K, +, \cdot)$. Элемент $a \in K_1$ называется *алгебраическим* над $\mathcal{K}$, если существует такой ненулевой многочлен $f(x) \in K[x]$, что $f(a) = 0$. В противном случае $a \in K_1$ – *трансцендентный* элемент над кольцом $\mathcal{K}$.

Для любого элемента $a \in K_1$ множество

$$\{f(a) | f(x) \in K[x]\}$$

определяет наименьшее подкольцо кольца $\mathcal{K}_1$, содержащее кольцо $\mathcal{K}$ и элемент a.

Замечание 1.30. Таким образом, для любого кольца $\mathcal{K}$ с единицей кольцо многочленов $\mathcal{K}[x]$ представляет собой наименьшее унитарное надкольцо, содержащее кольцо $\mathcal{K}$ и трансцендентный элемент x.

Истинно утверждение: *если $\mathcal{K}_1$ – унитарное надкольцо области целостности $\mathcal{K}$, то для любого элемента $a \in K_1$, алгебраического над $\mathcal{K}$, многочлен $f(x) \in K[x]$ наименьшей степени, корнем которого является элемент a, неразложим в кольце $\mathcal{K}[x]$.*

Пусть $\mathcal{K}$ – гауссово кольцо. Многочлен $f(x) \in K[x]$ положительной степени называется *примитивным*, если его коэффициенты не имеют общих делителей, отличных от обратимых элементов. Истинно утверждение: *любой многочлен $f(x) \in K[x]$ степени $m \in \mathbf{N}$ единственным образом (с точностью до обратимых множителей, являющихся элементами кольца $\mathcal{K}$) может быть представлен в виде*

$$f(x) = a \prod_{i=1}^{k} f_i(x),$$

где $a \in K$, а *$f_i(x) \in K[x]$ $(i = 1, \ldots, k)$ – неразложимые примитивные многочлены, сумма степеней которых равна m.*

Таким образом, если $\mathcal{K}$ – гауссово кольцо, то $\mathcal{K}[x]$ – гауссово кольцо.

Замечание 1.31. В гауссовом кольце $\mathcal{K}[x]$ разложение

$$f(x) = a \prod_{i=1}^{k} f_i(x)$$

многочлена $f(x) \in K[x]$ положительной степени в произведение неразложимых примитивных многочленов называется *каноническим разложением* $f(x)$.

Если $\mathcal{K}$ – поле, то $\mathcal{K}[x]$ – евклидово кольцо (и, следовательно, $\mathcal{K}[x]$ – кольцо главных идеалов), так как в этом случае число $n(f(x))$ – это степень многочлена $f(x)$. Многочлен $f(x) \in K[x]$ положительной степени называется *приведенным*, если его старший коэффициент равен единице. Истинно утверждение: *любой многочлен $f(x) \in K[x]$ степени $m \in \mathbf{N}$ единственным образом может быть представлен в виде*

$$f(x) = a \prod_{i=1}^{k} f_i(x),$$

где $a \in K$ – старший коэффициент многочлена $f(x)$, а $f_i(x) \in K[x]$ $(i = 1, \ldots, k)$ – неразложимые приведенные многочлены, сумма степеней которых равна m.

Поле $\mathcal{K}$ называется *алгебраически замкнутым*, если каждый неразложимый многочлен $f(x) \in K[x]$ имеет степень 1. Это означает, что любой

многочлен положительной степени $f(x) \in K[x]$ раскладывается в $\mathcal{K}[x]$ в произведение многочленов 1-й степени.

Замечание 1.32. Известно, что алгебраически замкнутое поле – бесконечное поле.

Поэтому, никакое конечное поле не является алгебраически замкнутым.

В кольце $\mathcal{K}[x] = (K[x], +, \cdot)$ допустимо сокращение на многочлены, принадлежащие множеству

$$S_{\mathcal{K}[x]} = \{f(x) \in K[x] | \mathrm{Val}\, f \subseteq S_{\mathcal{K}}\}.$$

Это означает, что кольцо многочленов $\mathcal{K}[x]$ можно изоморфно вложить в такое ассоциативно-коммутативное кольцо

$$\overline{\mathcal{K}[x]} = (\overline{K[x]}, +, \cdot)$$

с единицей, что каждый элемент $f(x) \in S_{\mathcal{K}[x]}$ имеет в кольце $\overline{\mathcal{K}[x]}$ обратный элемент.

Замечание 1.33. Ассоциативно-коммутативное кольцо $\overline{\mathcal{K}[x]} = (\overline{K[x]}, +, \cdot)$ с единицей строится в соответствии со схемой, представленной в замечании 1.16.

Действительно, пусть $R_{\mathcal{K}[x]} = \{\frac{f(x)}{g(x)} | f(x) \in K[x],\ g(x) \in S_{\mathcal{K}[x]}\}$ – множество *дробей* (*частных*) над кольцом $\mathcal{K}[x]$.

Положив

$$\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)g_2(x) + f_2(x)g_1(x)}{g_1(x)g_2(x)}$$

и

$$\frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}$$

для любых $\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)} \in S_{\mathcal{K}[x]}$, получим алгебраическую систему

$$\mathcal{R}_{\mathcal{K}[x]} = (R_{\mathcal{K}[x]}, +, \cdot).$$

Обозначим через «$\equiv$» такое отношение эквивалентности на множестве $R_{\mathcal{K}[x]}$, что

$$\frac{f_1(x)}{g_1(x)} \equiv \frac{f_2(x)}{g_2(x)}$$

тогда и только тогда, когда

$$f_1(x)g_2(x) = f_2(x)g_1(x).$$

Положим $\overline{K[x]} = R_{\mathcal{K}[x]}/_{\equiv}$ и определим на множестве $\overline{K[x]}$ операции «$+$» и «$\cdot$» следующим образом: если $H_1, H_2 \in \overline{K[x]}$ ($\frac{f_1(x)}{g_1(x)} \in H_1, \frac{f_2(x)}{g_2(x)} \in H_2$), то $H_1 + H_2 = H$, где $\frac{f_1(x)g_2(x)+f_2(x)g_1(x)}{g_1(x)g_2(x)} \in H$ и $H_1H_2 = H$, где $\frac{f_1(x)f_2(x)}{g_1(x)g_2(x)} \in H$.

Получим ассоциативно-коммутативное *кольцо* (*с единицей*) *рациональных дробей от неизвестного* x

$$\overline{\mathcal{K}[x]} = (\overline{K[x]}, +, \cdot),$$

над кольцом $\mathcal{K}$.

Единицей кольца $\overline{\mathcal{K}[x]}$ является элемент $\{\frac{f(x)}{f(x)} | f(x) \in S_{\mathcal{K}[x]}\}$. Элементу $f(x) \in K[x]$ кольца $\mathcal{K}[x]$ соответствует элемент $\{\frac{f(x)g(x)}{g(x)} | g(x) \in S_{\mathcal{K}[x]}\}$ кольца $\overline{\mathcal{K}[x]}$, а элементом кольца $\overline{\mathcal{K}[x]}$, обратным элементу $\{\frac{f(x)g(x)}{g(x)} | g(x) \in S_{\mathcal{K}[x]}\}$ $(f(x) \in S_{\mathcal{K}[x]})$ является элемент $\{\frac{g(x)}{f(x)g(x)} | g(x) \in S_{\mathcal{K}[x]}\}$.

В частности, если $\mathcal{K}$ – область целостности, то $\overline{\mathcal{K}[x]}$ – *поле рациональных дробей от неизвестного* x над полем $\mathcal{K}$.

Подставив в элемент $\frac{f(x)}{g(x)} \in \overline{K[x]}$ вместо переменной x любой элемент $a \in K$, получим элемент $\frac{f(a)}{g(a)} \in \overline{K}$, т.е. каждый элемент $\frac{f(x)}{g(x)} \in \overline{K[x]}$ определяет некоторое отображение множества K в множество $\overline{K}$.

Определим на множестве $\overline{K[x]}$ отношение эквивалентности «$\equiv$» следующим образом: $\frac{f_1(x)}{g_1(x)} \equiv \frac{f_2(x)}{g_2(x)}$ $(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)} \in \overline{K[x]})$ тогда и только тогда, когда дроби $\frac{f_1(x)}{g_1(x)}$ и $\frac{f_2(x)}{g_2(x)}$ определяют одно и то же отображение множества K в множество $\overline{K}$. Получим ассоциативно-коммутативное факторкольцо

$$\overline{\mathcal{K}[x]}/_{\equiv} = (\overline{K[x]}/_{\equiv}, +, \cdot)$$

всех рациональных отображений (от одной переменной) множества K в множество $\overline{K}$.

Замечание 1.34. Иногда приходится рассматривать над кольцом $\mathcal{K}$ множество дробей

$$\widetilde{R}_{\mathcal{K}[x]} = \Big\{ \frac{f(x)}{g(x)} \Big| f(x), g(x) \in K[x],\ (\mathrm{Val}\ g) \backslash \{0\} \neq \emptyset \Big\}$$

от переменной x.

В этом случае элемент $\frac{f(x)}{g(x)}$ – это такое частичное рациональное отображение (от одной переменной) множества K в множество

$$\widetilde{K} = \{\frac{a}{b} | a \in K, b \in K \backslash \{0\}\},$$

что

$$\mathrm{Dom} \frac{f(x)}{g(x)} = \{a \in K | g(a) \neq 0\}.$$

При этом истинны включения

$$\mathrm{Dom} \frac{f_1(x)g_2(x) + f_2(x)g_1(x)}{g_1(x)g_2(x)} \subseteq \mathrm{Dom} \frac{f_1(x)}{g_1(x)} \cap \mathrm{Dom} \frac{f_2(x)}{g_2(x)},$$

$$\mathrm{Dom}\frac{f_1(x)f_2(x)}{g_1(x)g_2(x)} \subseteq \mathrm{Dom}\frac{f_1(x)}{g_1(x)} \cap \mathrm{Dom}\frac{f_2(x)}{g_2(x)},$$

причем эти включения могут быть строгими.

Степенным рядом над кольцом $\mathcal{K}$ от переменной x называется выражение

$$f(x) = a_0 + a_1x + \cdots + a_mx^m + \ldots,$$

где $a_i \in K$ $(i \in \mathbf{Z}_+)$.

Обозначим через $K\{x\}$ множество всех степенных рядов от переменной x над кольцом $\mathcal{K}$. Определив обычным образом операции сложения и умножения рядов, получим ассоциативно-коммутативное *кольцо рядов*

$$\mathcal{K}\{x\} = (K\{x\}, +, \cdot)$$

от переменной x над кольцом $\mathcal{K}$.

Ясно, что $\mathcal{K}$ и $\mathcal{K}[x]$ – подкольца кольца $\mathcal{K}\{x\}$. Истинно утверждение: *если $\mathcal{K}$ – область целостности, то $\mathcal{K}\{x\}$ – область целостности.*

Следовательно, может быть построено поле частных $\overline{\mathcal{K}\{x\}}$ области целостности $\mathcal{K}\{x\}$.

В частности, если $\mathcal{K}$ – поле, то поле $\overline{\mathcal{K}\{x\}}$ изоморфно полю лорановых рядов над $\mathcal{K}$, т.е. рядов вида

$$a_nx^n + a_{n+1}x^{n+1} + \ldots,$$

где $n \in \mathbf{Z}$, а все коэффициенты $a_n, a_{n+1}, \ldots$ – элементы поля $\mathcal{K}$.

Кольцо

$$\mathcal{K}[x_1, \ldots, x_n] = (K[x_1, \ldots, x_n], +, \cdot)\ (n \in \mathbf{N},\ n \geq 2)$$

многочленов от переменных $x_1, \ldots, x_n$ над кольцом $\mathcal{K}$ может быть определено индуктивно, а именно: $\mathcal{K}[x_1, \ldots, x_n]$ – это кольцо многочленов от переменной x_n над кольцом многочленов $\mathcal{K}[x_1, \ldots, x_{n-1}]$, т.е.

$$\mathcal{K}[x_1, \ldots, x_n] = \mathcal{K}[x_1, \ldots, x_{n-1}][x_n].$$

Замечание 1.35. Кольца степенных рядов от переменных $x_1, \ldots, x_n$ $(n \geq 2)$ также могут быть определены индуктивно.

Многочлен $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ может быть представлен в виде конечной суммы одночленов, т.е. в виде

$$f(x_1, \ldots, x_n) = a_0 + \sum_{1 \leq i_1 < \ldots i_r \leq n} a_{i_1 \ldots i_r} x_{i_1}^{\alpha_1} \ldots x_{i_r}^{\alpha_r}\ (\alpha_1, \ldots, \alpha_r \in \mathbf{N}), \quad (1.6)$$

где $a_0, a_{i_1 \ldots i_r} \in K$ – коэффициенты.

Замечание 1.36. Из (1.6) вытекает, что $\mathcal{K}$ и $\mathcal{K}[x_{i_1}, \ldots, x_{i_r}]$ $(1 \leq i_1 < \ldots i_r \leq n)$ – подкольца кольца $\mathcal{K}[x_1, \ldots, x_n]$.

Степень ненулевого многочлена (1.6) определяется следующим образом. Если все коэффициенты $a_{i_1 \ldots i_r}$ равны нулю, то $f(x_1, \ldots, x_n)$ – многочлен 0-й степени, иначе степень многочлена $f(x_1, \ldots, x_n)$ равна такому максимальному числу $\alpha_1 + \cdots + \alpha_r$, что $a_{i_1 \ldots i_r} \neq 0$.

В кольце $\mathcal{K}[x_1, \ldots, x_n]$ производная $\mathsf{D}_{x_i} f(x_1, \ldots, x_n)$ $(i = 1, \ldots, n)$ многочлена $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ по переменной x_i определяется обычным образом, т.е. многочлен $f(x_1, \ldots, x_n)$ рассматривается как многочлен только от одной переменной x_i, и применяется правило дифференцирования, сформулированное для кольца многочленов от одной переменной.

Подставив в (1.6) вместо каждой переменной x_i $(i = 1, \ldots, n)$ элемент $a_i \in K$ и выполнив действия, получим элемент $f(a_1, \ldots, a_n) \in K$. Таким образом, кольцо $\mathcal{K}[x_1, \ldots, x_n]$ определяет кольцо отображений множества K^n в множество K.

Пусть $\mathcal{K}_1 = (K_1, +, \cdot)$ – унитарное надкольцо кольца $\mathcal{K} = (K, +, \cdot)$. Для любых элементов $a_1, \ldots, a_n \in K_1$ множество

$$\{f(a_1, \ldots, a_n) | f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]\}$$

определяет наименьшее подкольцо кольца $\mathcal{K}_1$, содержащее кольцо $\mathcal{K}$ и элементы $a_1, \ldots, a_n$.

Элементы $a_1, \ldots, a_n \in K$ *алгебраически зависимы* над кольцом $\mathcal{K}$, если существует такой ненулевой многочлен $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, что $f(a_1, \ldots, a_n) = 0$. В противном случае элементы $a_1, \ldots, a_n \in K$ называются *алгебраически независимыми* над кольцом $\mathcal{K}$.

Замечание 1.37. Для любого кольца $\mathcal{K}$ с единицей кольцо многочленов $\mathcal{K}[x_1, \ldots, x_n]$ представляет собой наименьшее унитарное надкольцо, содержащее кольцо $\mathcal{K}$ и алгебраически независимые элементы $x_1, \ldots, x_n$.

Кольцо $\mathcal{K}[x_1, \ldots, x_n]$ $(n \geq 2)$ (в отличие от кольца $\mathcal{K}[x]$) не является кольцом главных идеалов.

Пример 1.5. В кольце $\mathcal{K}[x_1, \ldots, x_n]$ $(n \geq 2)$ множество всех многочленов, у которых свободный член равен нулю, является собственным идеалом, но не является главным идеалом.

Для любого набора $\mathbf{a} = (a_1, \ldots, a_n) \in K^n$ $(n \in \mathbf{N})$ множество

$$I_{\mathbf{a}} = \{f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] | f(a_1, \ldots, a_n) = 0\}$$

является конечно порожденным идеалом кольца $\mathcal{K}[x_1, \ldots, x_n]$.

Замечание 1.38. Множество $M = \{x_1 - a_1, \ldots, x_n - a_n\}$ – базис идеала $I_{\mathbf{a}}$.

Идеал $I_{\mathbf{a}}$ – простой, если кольцо $\mathcal{K} = (K, +, \cdot)$ не содержит делителей нуля.

Однако, для любых $\mathbf{a} \neq \mathbf{b}$ $(\mathbf{a}, \mathbf{b} \in K^n)$ идеал $I_{\mathbf{a}} \cap I_{\mathbf{b}}$ не является простым идеалом кольца $\mathcal{K}[x_1, \ldots, x_n]$.

Имеет место теорема Гильберта о базисе: *если* $\mathcal{K}$ *– нетерово кольцо, то* $\mathcal{K}[x_1, \ldots, x_n]$ $(n \in \mathbf{N})$ *– нетерово кольцо* (т.е. каждый идеал кольца $\mathcal{K}[x_1, \ldots, x_n]$ $(n \in \mathbf{N})$ является конечно порожденным).

Замечание 1.39. Пусть $\mathcal{K} = (K, +, \cdot)$ – кольцо с единицей, не содержащее делителей нуля.

Многочлен $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n])$ положительной степени – *неприводимый*, если он не может быть разложен в произведение двух многочленов положительной степени.

Для разложения

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{l} f_i^{\alpha_i}(x_1, \ldots, x_n) \ (\alpha_1, \ldots, \alpha_n \in \mathbf{N})$$

многочлена $f(x_1, \ldots, x_n)$ на попарно неассоциированные неприводимые многочлены $f_i(x_1, \ldots, x_n)$ $(i = 1, \ldots, l)$, истинны следующие равенства

$$(f(x_1, \ldots, x_n)) = \prod_{i=1}^{l} (f_i(x_1, \ldots, x_n))^{\alpha_i}$$

и

$$\sqrt{(f(x_1, \ldots, x_n))} = (\prod_{i=1}^{l} (f_i(x_1, \ldots, x_n))).$$

Рациональные дроби от переменных $x_1, \ldots, x_n$ $(n \in \mathbf{N})$ над кольцом $\mathcal{K} = (K, +, \cdot)$ определяются обычным образом.

Обозначим через

$$\overline{\mathcal{K}[x_1, \ldots, x_n]} = (\overline{K[x_1, \ldots, x_n]}, +, \cdot)$$

кольцо рациональных дробей от неизвестных $x_1, \ldots, x_n$ над кольцом $\mathcal{K}$ (в частности, если $\mathcal{K}$ – область целостности, то $\overline{\mathcal{K}[x_1, \ldots, x_n]}$ – поле рациональных дробей от неизвестных $x_1, \ldots, x_n$ над кольцом $\mathcal{K}$).

Подставив в элемент $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)} \in \overline{K[x_1, \ldots, x_n]}$ вместо переменных $x_1, \ldots, x_n$ любой набор значений $(a_1, \ldots, a_n) \in K^n$, получим элемент $\frac{f(a_1,\ldots,a_n)}{g(a_1,\ldots,a_n)} \in \overline{K}$, т.е. каждый элемент $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)} \in \overline{K[x_1, \ldots, x_n]}$ определяет некоторое отображение множества K^n в множество $\overline{K}$.

Определим на множестве $\overline{K[x_1, \ldots, x_n]}$ отношение эквивалентности «$\equiv$» следующим образом

$$\frac{f_1(x_1, \ldots, x_n)}{g_1(x_1, \ldots, x_n)} \equiv \frac{f_2(x_1, \ldots, x_n)}{g_2(x_1, \ldots, x_n)}$$

тогда и только тогда, когда дроби $\frac{f_1(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)}$ и $\frac{f_2(x_1,\ldots,x_n)}{g_2(x_1,\ldots,x_n)}$ определяют одно и то же отображение множества K^n в множество $\overline{K}$.

Получим ассоциативно-коммутативное фактор-кольцо

$$\overline{\mathcal{K}[x_1, \ldots, x_n]}/_{\equiv} = (\overline{K[x_1, \ldots, x_n]}/_{\equiv}, +, \cdot)$$

всех рациональных отображений (от n переменных) множества K^n в множество $\overline{K}$.

Замечание 1.40. Иногда приходится рассматривать над кольцом $\mathcal{K}$ множество дробей

$$\widetilde{R}_{\mathcal{K}[x_1,\ldots,x_n]} = \left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \middle| f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \ (\mathrm{Val}\, g) \backslash \{0\} \neq \emptyset \right\}$$

от переменных $x_1, \ldots, x_n$.

В этом случае элемент $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)} \in \widetilde{R}_{\mathcal{K}[x_1,\ldots,x_n]}$ представляет собой такое частичное рациональное отображение (от n переменных) множества K^n в множество $\widetilde{K}$, что

$$\mathrm{Dom} \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} = \{(a_1, \ldots, a_n) \in K^n | g(a_1, \ldots, a_n) \neq 0\}.$$

При этом истинны включения

$$\mathrm{Dom} \frac{f_1(x_1, \ldots, x_n) g_2(x_1, \ldots, x_n) + f_2(x_1, \ldots, x_n) g_1(x_1, \ldots, x_n)}{g_1(x_1, \ldots, x_n) g_2(x_1, \ldots, x_n)} \subseteq$$

$$\subseteq \mathrm{Dom} \frac{f_1(x_1, \ldots, x_n)}{g_1(x_1, \ldots, x_n)} \cap \mathrm{Dom} \frac{f_2(x_1, \ldots, x_n)}{g_2(x_1, \ldots, x_n)},$$

$$\mathrm{Dom}\frac{f_1(x_1,\ldots,x_n)f_2(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)g_2(x_1,\ldots,x_n)} \subseteq \mathrm{Dom}\frac{f_1(x_1,\ldots,x_n)}{g_1(x_1,\ldots,x_n)} \cap \mathrm{Dom}\frac{f_2(x_1,\ldots,x_n)}{g_2(x_1,\ldots,x_n)},$$

причем эти включения могут быть строгими.

1.2. Многообразия над кольцами.

В настоящем пункте под кольцом $\mathcal{K} = (K, +, \cdot)$ понимается ассоциативно-коммутативное кольцо. Для упрощения обозначений вместо записи «$f(x_1, \ldots, x_n)$» будем использовать запись «f» там, где это не вызывает недоразумений.

1.2.1. Общие понятия.

Многообразием в множестве K^n ($n \in \mathbf{N}$), порожденным (ненулевыми) многочленами $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ ($m \in \mathbf{N}$) называется множество

$$V(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in K^n | f_i(a_1, \ldots, a_n) = 0 \text{ для всех } i = 1, \ldots, m\}. \tag{1.7}$$

Если $\mathcal{K}$ – поле, то (1.7) называется *аффинным* многообразием.

Гиперповерхностью называется многообразие, порождаемое одним многочленом (если $m = 1$ и $n = 2$, то гиперповерхность называется *кривой* над кольцом $\mathcal{K}$).

Таким образом, любое многообразие $V(f_1, \ldots, f_m)$ ($m \geq 2$) является пересечением гиперповерхностей $V(f_i)$ ($i = 1, \ldots, m$).

Пример 1.6. 1. Для любго кольца $\mathcal{K} = (K, +, \cdot)$ при всех значениях $m, n \in \mathbf{N}$ система линейных уравнений

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

определяет в множестве K^n *линейное многообразие.*

2. Для любого кольца $\mathcal{K} = (K, +, \cdot)$, не содержащего делителей нуля, каждое непустое конечное множество $S = \{a_1, \ldots, a_n\} \subseteq K$ является многообразием в K. Действительно,

$$S = V(\prod_{i=1}^{n}(x - a_i)).$$

3. Если $\mathcal{K} = (K, +, \cdot)$ – конечное кольцо, то

$$K = V(\prod_{a \in K}(x - a)),$$

т.е. множество K – многообразие в K.

4. Для любого кольца $\mathcal{K} = (K, +, \cdot)$ при любых $n, r \in \mathbf{N}$ $(r < n)$ множество K^r является многообразием в множестве K^n.

Действительно, рассмотрим многообразие $V(x_1, x_2, \ldots, x_l)$ $(1 \leq l \leq n)$ в K^n. Его точки – векторы

$$\mathbf{a} = (\underbrace{0, \ldots, 0}_{l}, x_{l+1}, \ldots, x_n) \ (x_{l+1}, \ldots, x_n \in K).$$

Отождествив каждый такой вектор $\mathbf{a}$ с вектором

$$\mathbf{b} = (x_{l+1}, \ldots, x_n) \in K^{n-l},$$

мы тем самым отождествим многообразие $V(x_{l+1}, \ldots, x_n)$ с множеством K^{n-l}.

Положив $r = n - l$, получим требуемое.

Поэтому в дальнейшем, при необходимости, будем рассматривать множество K^r $(r \in \mathbf{N})$ как многообразие, без всяких уточнений, в каком множестве оно рассматривается.

Замечание 1.41. Из (1.7) вытекает, что для любых многообразий $V(f_1, \ldots, f_s)$ и $V(g_1, \ldots, g_t)$ в K^n равенство

$$V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$$

истинно тогда и только тогда, когда над кольцом $\mathcal{K}$ эквивалентны системы полиномиальных уравнений

$$f_i(x_1, \ldots, x_n) = 0 \ (i = 1, \ldots, s)$$

и

$$g_i(x_1, \ldots, x_n) = 0 \ (i = 1, \ldots, t).$$

Таким образом, для любого кольца $\mathcal{K}$ любое многообразие в K^n – это множество решений класса всех эквивалентных над кольцом $\mathcal{K}$ систем полиномиальных уравнений от n неизвестных.

Если $\{f_1, \ldots, f_s\}$ и $\{g_1, \ldots, g_t\}$ – базисы одного и того же конечно-порожденного идеала кольца $\mathcal{K}[x_1, \ldots, x_n]$, то

$$V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t).$$

Поэтому корректно говорить о многообразии $V(I)$ в K^n, ассоциированном с конечно-порожденным идеалом I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$.

Следовательно, для любого кольца $\mathcal{K}$ отображение $\mathbf{v}_{\mathcal{K},n}$ ($n \in \mathbf{N}$), определенное на множестве всех конечно-порожденных идеалов кольца $\mathcal{K}[x_1, \ldots, x_n]$ равенством

$$\mathbf{v}_{\mathcal{K},n}(I) = V(I)$$

является сюръекцией этого множества на множество всех многообразий в K^n, т.е. на множество классов эквивалентных над кольцом $\mathcal{K}$ систем полиномиальных уравнений от n неизвестных.

Следует отметить, что отображение $\mathbf{v}_{\mathcal{K},n}$ может не быть инъекцией, так как в кольце $\mathcal{K}[x_1, \ldots, x_n]$ могут существовать такие конечно-порожденные идеалы I_1 и I_2 ($I_1 \neq I_2$), что $\mathbf{v}_{\mathcal{K},n}(I_1) = \mathbf{v}_{\mathcal{K},n}(I_2)$.

Для любых многообразий $V_1 \subseteq K^{n_1}$ и $V_2 \subseteq K^{n_2}$ многообразием является множество

$$V_1 \times V_2 = \{(a_1, \ldots, a_{n_1+n_2}) | (a_1, \ldots, a_{n_1}) \in V_1, (a_{n_1+1}, \ldots, a_{n_1+n_2}) \in V_2\}.$$

Замечание 1.42. Отсюда, в частности вытекает, что если $\mathcal{K} = (K, +, \cdot)$ – конечное кольцо, то K^n ($n \in \mathbf{N}$) – многообразие в K^n.

Если $V_1 = V(f_1, \ldots, f_{m_1}) \subseteq K^n$ и $V_2 = V(g_1, \ldots, g_{m_2}) \subseteq K^n$, то

$$V_1 \cap V_2 = V(f_1, \ldots, f_{m_1}, g_1, \ldots, g_{m_2}) \tag{1.8}$$

и

$$V_1 \cup V_2 \subseteq V(\{f_i g_j | i = 1, \ldots, m_1;\ j = i = 1, \ldots, m_2\}). \tag{1.9}$$

Замечание 1.43. Если кольцо $\mathcal{K}$ не содержит делителей нуля, то в (1.9) имеет место знак равенства, т.е.

$$V_1 \cup V_2 = V(\{f_i g_j | i = 1, \ldots, m_1;\ j = 1, \ldots, m_2\}). \tag{1.10}$$

Из (1.10) вытекает, что если кольцо $\mathcal{K}$ не содержит делителей нуля, то для любых конечно-порожденных идеалов I_1 и I_2 кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ истинно равенство

$$\mathbf{v}_{\mathcal{K},n}(I_1) \cup \mathbf{v}_{\mathcal{K},n}(I_2) = \mathbf{v}_{\mathcal{K},n}(I_1 I_2) \tag{1.11}$$

Многообразие $V \subseteq K^n$ называется *неприводимым*, если для любых многообразий $V_1, V_2 \subseteq K^n$ из равенства $V = V_1 \cup V_2$ вытекает, что $V_1 = V$ или $V_2 = V$.

Если кольцо $\mathcal{K}$ не содержит делителей нуля, то, в силу (1.11), для любого конечно-порожденного идеала I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ многообразие $\mathbf{v}_{\mathcal{K},n}(I)$ неприводимо тогда и только тогда, когда I – простой идеал.

Пример 1.7. Пусть кольцо $\mathcal{K} = (K, +, \cdot)$ не содержит делителей нуля. Рассмотрим кольцо многочленов $\mathcal{K}[x, y, z]$ от трех переменных x, y и z.

Многообразие $V(z)$ определяет в K^3 *плоскость* (x, y), а многообразие $V(x, y)$ определяет в K^3 *ось* z.

Следовательно, многообразие

$$V(xz, yz) = V(x, y) \cup V(z) \subseteq K^3$$

представляет собой объединение плоскости (x, y) с осью z.

Идеалом многообразия (1.7) называется идеал

$$I(V(f_1, \ldots, f_m)) = \{f \in K[x_1, \ldots, x_n] | f(a_1, \ldots, a_n) = 0 \text{ для всех } (a_1, \ldots, a_n) \in V(f_1, \ldots, f_m)\}. \quad (1.12)$$

Ясно, что

$$(f_1, \ldots, f_m) \subseteq I(V(f_1, \ldots, f_m)). \quad (1.13)$$

Замечание 1.44. Из (1.12) вытекает, что для любого кольца $\mathcal{K} = (K, +, \cdot)$ при всех $n \in \mathbf{N}$ с каждым многообразием $V \subseteq K^n$ (т.е. с каждым множеством решений класса всех эквивалентных над кольцом $\mathcal{K}$ систем полиномиальных уравнений от n неизвестных) ассоциируется идеал $I(V)$ кольца $\mathcal{K}[x_1, \ldots, x_n]$ $(n \in \mathbf{N})$.

Поэтому корректно говорить об отображении $\mathbf{i}_{\mathcal{K},n}$ $(n \in \mathbf{N})$ множества всех многообразий $V \subseteq K^n$ в множество всех идеалов кольца $\mathcal{K}[x_1, \ldots, x_n]$, определенном равенством

$$\mathbf{i}_{\mathcal{K},n}(V) = I(V).$$

Таким образом, для любого кольца $\mathcal{K}$ при всех $n \in \mathbf{N}$ определено отображение $\mathbf{i}_{\mathcal{K},n} \circ \mathbf{v}_{\mathcal{K},n}$ множества конечно-порожденных идеалов кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ в множество всех идеалов этого кольца.

Возникает естественный вопрос:

Какими свойствами обладает отображение $\mathbf{i}_{\mathcal{K},n} \circ \mathbf{v}_{\mathcal{K},n}$?

Во-первых, из (1.13) вытекает, что для любого конечно-порожденного идеала I кольца $\mathcal{K}[x_1, \ldots, x_n]$ истинно включение

$$I \subseteq \mathbf{i}_{\mathcal{K},n} \circ \mathbf{v}_{\mathcal{K},n}(I).$$

Во-вторых, если $f \in \mathbf{i}_{\mathcal{K},n} \circ \mathbf{v}_{\mathcal{K},n}(I)$ $(f \in K[x_1, \ldots, x_n])$, то $f^m \in \mathbf{i}_{\mathcal{K},n} \circ \mathbf{v}_{\mathcal{K},n}(I)$ для всех $m \in \mathbf{N}$. Следовательно, для любого конечно-порожденного идеала I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ истинно включение

$$\mathbf{i}_{\mathcal{K},n} \circ \mathbf{v}_{\mathcal{K},n}(I) \subseteq \sqrt{I}.$$

В частности, если $\mathcal{K}$ – алгебраически замкнутое поле, то имеет место равенство

$$\mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I) = \sqrt{I}.$$

Это равенство называется теоремой Гильберта о нулях.

В-третьих, если $\mathcal{K}$ – кольцо, не содержащее делителей нуля и $f^m \in \mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I)$ ($f \in K[x_1, \ldots, x_n]$) для некоторого $m \in \mathbf{N}$, то $f \in \mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I)$.

Отсюда вытекает, что если кольцо $\mathcal{K}$ не содержит делителей нуля, то для любого конечно-порожденного идеала I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ идеал $\mathsf{i}_{\mathcal{K},n} \circ \mathsf{v}_{\mathcal{K},n}(I)$ является радикальным идеалом.

1.2.2. Параметризация многообразия.

Формула (1.7), как правило, представляет многообразие $V \subseteq K^n$ в *неявном* виде. Возникает естественный вопрос:

Можно ли многообразие (1.7) *представить набором формул того или иного вида, предназначенных для вычисления координат точки многообразия, соответствующей заданным допустимым значениям параметров*?

Именно для ответа на этот вопрос и используется понятие «параметризация многообразия».

Рассмотрим основные типы параметризации многообразий над конечными кольцами.

Полиномиальной параметризацией многообразия (1.7) называется такой набор многочленов $h_1, \ldots, h_n \in K[t_1, \ldots, t_l]$, что точки с координатами

$$\begin{cases} x_1 = h_1(t_1, \ldots, t_l) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = h_n(t_1, \ldots, t_l) \end{cases} \qquad ((t_1, \ldots, t_l) \in K^l) \tag{1.14}$$

принадлежат многообразию (1.7).

Замечание 1.45. Из этого определения вытекает, что построение полиномиальной параметризации многообразия $V \subseteq K^n$ эквивалентно построению такого отображения $\mathsf{h} : K^l \to K^n$, определенного равенством

$$\mathsf{h}(t_1, \ldots, t_l) = (h_1(t_1, \ldots, t_l), \ldots, h_n(t_1, \ldots, t_l)) \ ((t_1, \ldots, t_l) \in K^l), \tag{1.15}$$

где $h_1, \ldots, h_n \in K[t_1, \ldots, t_l]$, что истинно включение

$$\mathrm{Val}\ \mathsf{h} \subseteq V. \tag{1.16}$$

Само множество $\mathrm{Val}\,\mathsf{h}$ может не быть многообразием в K^n.

Кроме того, не для всякого многообразия $V \subseteq K^n$ существует полиномиальная параметризация h, удовлетворяющая условию

$$\mathrm{Val}\,\mathsf{h} = V.$$

Ясно, что для любого многообразия $V(f_1, \ldots, f_m) \subseteq K^n$ построение таких полинимиальных параметризаций $\mathsf{h}_j : K^l \to K^n$ $(j = 1, \ldots, r)$, что истинно равенство

$$\bigcup_{j=1}^{r} \mathrm{Val}\,\mathsf{h}_j = V(f_1, \ldots, f_m) \tag{1.17}$$

эквивалентно построению представления (в неявном виде) полиномами множества решений системы полиномиальных уравнений

$$f_i(x_1, \ldots, x_n) = 0 \ \ (i = 1, \ldots, m)$$

над кольцом $\mathcal{K}$.

Пример 1.8. Пусть $\mathcal{K} = (K, +, \cdot)$ – кольцо с единицей, не содержащее делителей нуля. Тогда $x^2 - yz \in K[x, y, z]$.

Найдем полиномиальную параметризацию многообразия $V(x^2 - yz) \in K^3$.

Положив

$$x = uvw$$

в уравнении $x^2 = yz$, получим

$$yz = u^2v^2w^2.$$

Следовательно, отображение $\mathsf{h} : K^3 \to K^3$, определяемое системой уравнений

$$\begin{cases} x = uvw \\ y = u^2v \\ z = w^2v \end{cases}, \tag{1.18}$$

является полинимиальной параметризацией многообразия $V(x^2 - yz) \in K^3$.

Для полиномиальной параметризации (1.18) можно только утверждать, что

$$\mathrm{Val}\,\mathsf{h} \subseteq V(x^2 - yz).$$

Действительно, в кольце $\mathcal{K} = (K, +, \cdot)$ могут существовать такие свободные от квадратов элементы $v_1, v_2 \in K$ $(v_1 \neq v_2)$, что v_1v_2 – квадрат.

Тогда $(uv_1v_2w, u^2v_1, w^2v_2) \in V(x^2 - yz)$ и $(uv_1v_2w, u^2v_1, w^2v_2) \notin \mathrm{Val}\,\mathsf{h}$.

Естественно возникает задача построения по полиномиальной параметризации h (т.е. по системе уравнений (1.14)) наименьшего многообразия $V \subseteq K^n$, удовлетворяющего включению (1.16).

Содержательно эта задача означает построение над кольцом $\mathcal{K}$ системы уравнений от n неизвестных, множество решений которой – наименьшее множество, содержащее множество $\operatorname{Val}\mathsf{h}$.

Решение этой задачи основано на (последовательном) исключении параметров $t_1, \ldots, t_l$ в системе уравнений (1.14).

Пример 1.9. Пусть $\mathcal{K} = (K, +, \cdot)$ – кольцо с единицей, а отображение $\mathsf{h} : K^1 \to K^3$ определено системой уравнений

$$\begin{cases} x = t^2 \\ y = t^3 \\ z = t^4 \end{cases}.$$

Возводя 1-е уравнение в куб, а 2-е уравнение в квадрат, получим $x^3 - y^2 = 0$, а из 1-го и 3-го уравнений находим, что $z - x^2 = 0$.

Следовательно, для многообразия $V(x^3 - y^2, z - x^2) \subseteq K^3$ истинно включение

$$\operatorname{Val}\mathsf{h} \subseteq V(x^3 - y^2, z - x^2).$$

Замечание 1.46. Если $\mathcal{K} = (K, +, \cdot)$ – поле, то существует унифицированный метод решения рассматриваемой задачи в кольце многочленов $\mathcal{K}[x_1, \ldots, x_n]$, основанный на выделении в идеалах специального вида базисов, построенных с помощью операции деления многочленов.

Для выполнения этой операции необходимо упорядочить в порядке «убывания» одночлены, входящие в многочлен $f \in K[x_1, \ldots, x_n]$.

Последнее осуществляется следующим образом.

Линейное упорядочение переменных $x_1, \ldots, x_n$ по их значимости (для определенности считаем, что $x_1 > \cdots > x_n$) дает возможность определить на множестве мономов $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ $(\alpha_1, \ldots, \alpha_n \in \mathbf{Z}_+^n)$ отношение линейного порядка «$\succ$», *совместимое с алгебраической структурой кольца* $\mathcal{K}[x_1, \ldots, x_n]$.

Последнее означает, что отношение линейного порядка «$\succ$» должно быть определено только в терминах векторов

$$\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}_+^n,$$

т.е.

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} \succ x_1^{\beta_1} \ldots x_n^{\beta_n} \Leftrightarrow (\alpha_1, \ldots, \alpha_n) \succ (\beta_1, \ldots, \beta_n)),$$

причем должны быть выполнены следующие два условия:

1) если $\overrightarrow{\alpha} \succ \overrightarrow{\beta}$ $(\overrightarrow{\alpha}, \overrightarrow{\beta} \in \mathbf{Z}_+^n)$, то $\overrightarrow{\alpha} + \overrightarrow{\gamma} \succ \overrightarrow{\beta} + \overrightarrow{\gamma}$ для любого $\overrightarrow{\gamma} \in \mathbf{Z}_+^n$;

2) каждое непустое подмножество множества $\mathbf{Z}_+^n$ имеет наименьший по отношению к линейному порядку «$\succ$» элемент (т.е. отношение линейного порядка «$\succ$» удовлетворяет условию обрыва убывающих цепей).

Как правило, в качестве отношения линейного порядка «$\succ$» выбирается одно из следующих трех отношений (ниже предполагается, что $\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}_+^n$ и $\overrightarrow{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbf{Z}_+^n$):

1) *отношение лексикографического порядка* «$\succ_{\text{lex}}$», где $\overrightarrow{\alpha} \succ_{\text{lex}} \overrightarrow{\beta}$ тогда и только тогда 1-я слева ненулевая компонента вектора $\overrightarrow{\alpha} - \overrightarrow{\beta}$ – положительное число;

2) *градуированное отношение лексикографического порядка* «$\succ_{\text{grlex}}$», где $\overrightarrow{\alpha} \succ_{\text{grlex}} \overrightarrow{\beta}$ тогда и только тогда, когда $\sum\limits_{i=1}^{n} \alpha_i > \sum\limits_{i=1}^{n} \beta_i$ или $\sum\limits_{i=1}^{n} \alpha_i = \sum\limits_{i=1}^{n} \beta_i$ и $\overrightarrow{\alpha} \succ_{\text{lex}} \overrightarrow{\beta}$ (т.е. вначале мономы упорядочиваются по степеням, а при равенстве степеней используется лексикографичесое упорядочение);

3) *градуированное обратное отношение лексикографического порядка* «$\succ_{\text{grevlex}}$», где $\overrightarrow{\alpha} \succ_{\text{grevlex}} \overrightarrow{\beta}$ тогда и только тогда, когда $\sum\limits_{i=1}^{n} \alpha_i > \sum\limits_{i=1}^{n} \beta_i$ или $\sum\limits_{i=1}^{n} \alpha_i = \sum\limits_{i=1}^{n} \beta_i$ и самая правая ненулевая компонента вектора $\overrightarrow{\alpha} - \overrightarrow{\beta}$ – отрицательное число.

Пусть на множестве мономов зафиксировано отношение линейного порядка «$\succ$».

Обозначим через $\text{LT}(f)$ старший член многочлена $f \in \mathcal{K}[x_1, \ldots, x_n]$, а через $\text{LT}(I)$ – множество старших членов многочленов, принадлежащих идеалу I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$.

Базисом Гребнера идеала I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ называется такое конечное множество $G = \{g_1, \ldots, g_l\} \subseteq I$, что

$$(\text{LT}(g_1), \ldots, \text{LT}(g_l)) = (\text{LT}(I))$$

т.е. старший член любого многочлена, принадлежащего идеалу I, делится хотя бы на один старший член $\text{LT}(g_i)$ $(i = 1, \ldots, l)$.

Используя операцию деления многочленов, любой многочлен $f \in \mathcal{K}[x_1, \ldots, x_n]$ можно представить в виде

$$f = h_1 g_1 + \cdots + h_l g_l + r,$$

где ни один из одночленов многочлена r не делится ни ни на один из старших членов $\text{LT}(g_1), \ldots, \text{LT}(g_l)$ (в этом случае говорят, что r – *остаток от деления* f *на* G). Истинно утверждение: *базис Гребнера идеала* I *является базисом идеала* I.

Отсюда вытекает, что если G – базис Гребнера идеала I, то $f \in I$ тогда и только тогда, когда $r = 0$.

Для любого идеала $I \neq \{0\}$ кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ существует единственный *редуцированный базис Гребнера* G, т.е. такой, что старший коэффициент каждого многочлена $g \in G$ равен единицы и никакой моном никакого многочлена $g \in G$ не принадлежит идеалу $(G \backslash \{g\})$.

Отсюда вытекает, что проверка равенства двух идеалов кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ сводится к проверке равенства их редуцированных базисов Гребнера.

Во многих современных системах компьютерной алгебры реализованы алгоритмы построения базисов Гребнера.

Как правило, это тот или иной вариант алгоритма Бухбергера, результат которого – базис Гребнера элементы которого отличаются от элементов редуцированного базиса Гребнера только постоянными множителями.

Существенным моментом построения базиса Гребнера $G = \{g_1, \ldots, g_l\}$ идеала I кольца многочленов $\mathcal{K}[x_1, \ldots, x_n]$ является последовательное исключение переменных, входящих в многочлены $g_1, \ldots, g_l$.

Отсюда вытекает, что если $\mathcal{K}$ – поле, то:

1) построение по заданной полиномиальной параметризации h (т.е. по системе уравнений (1.14)) наименьшего многообразия $V \subseteq K^n$, удовлетворяющего включению (1.16), сводится к построению при лексикографической упорядоченности «$\succ_{\text{lex}}$» базиса Гребнера G для идеала $(x_1 - h_1(t_1, \ldots, t_l), \ldots, x_n - h_n(t_1, \ldots, t_l))$ кольца многочленов $\mathcal{K}[t_1, \ldots, t_l, x_1, \ldots, x_n]$, и выбору из G всех тех многочленов, которые не содержат ни одной из переменных $t_1, \ldots, t_l$;

2) решение системы полиномиальных уравнений

$$f_i(x_1, \ldots, x_n) = 0 \ \ (i = 1, \ldots, m)$$

над полем $\mathcal{K}$ сводится к построению базиса Гребнера

$$G = \{g_1, \ldots, g_l\}$$

для идеала

$$I = (f_1, \ldots, f_m).$$

Эти вычисления называются (*прямым ходом*. После чего осуществляется последовательное решение уравнений

$$g_j = 0 \ \ (j = l, l-1, \ldots, 1).$$

Эти вычисления называются (*обратным ходом*.

Корректность этого метода обусловлена тем обстоятельством, что при лексикографической упорядоченности «$\succ_{\text{lex}}$» переменных для всех $r = 0, 1, \ldots, n$ множество

$$G_r = G \cap K[x_{r+1}, \ldots, x_n]$$

является базисом Гребнера идеала $I \cap K[x_{r+1}, \ldots, x_n]$ (этот идеал называется r-м *исключающим идеалом* идеала I).

Понятие «полиномиальная параметризация» допускает следующее естественное обобщение.

Для частичного рационального отображения

$$r(t_1, \ldots, t_l) = \frac{f(t_1, \ldots, t_l)}{g(t_1, \ldots, t_l)} \in \widetilde{R}_{\mathcal{K}[t_1, \ldots, t_l]}$$

положим

$$\mathsf{S}_r = \{(a_1, \ldots, a_l) \in K^l | r(a_1, \ldots, a_l) \in K\}.$$

Ясно, что

$$\mathsf{S}_r \subseteq \operatorname{Dom} r,$$

причем включение может быть строгим.

Замечание 1.47. Если $\mathcal{K}$ – поле, то

$$\mathtt{S}_r = \{(a_1, \ldots, a_l) \in K^l | g(a_1, \ldots, a_l) \neq 0\}$$

и, следовательно, $\mathtt{S}_r = \operatorname{Dom} r$.

Рациональной параметризацией многообразия $V \subseteq K^n$ назовем такой набор частичных рациональных отображений $r_1, \ldots, r_n \in \widetilde{R}_{\mathcal{K}[t_1,\ldots,t_l]}$, что точки с координатами

$$\begin{cases} x_1 = r_1(t_1, \ldots, t_l) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = r_n(t_1, \ldots, t_l) \end{cases} \qquad ((t_1, \ldots, t_l) \in \bigcap_{i=1}^{n} \mathtt{S}_{r_i}) \tag{1.19}$$

принадлежат многообразию V.

Таким образом, построение рациональной параметризации многообразия $V \subseteq K^n$ эквивалентно построению такого частичного отображения $\mathsf{r} : K^l \to \widetilde{K}^n$, определенного равенством

$$\mathsf{r}(t_1, \ldots, t_l) = (r_1(t_1, \ldots, t_l), \ldots, r_n(t_1, \ldots, t_l)) \; ((t_1, \ldots, t_l) \in K^m), \tag{1.20}$$

что истинно включение

$$\operatorname{Val}\left(\mathsf{r}|_{\bigcap_{i=1}^{n} \mathtt{S}_{r_i}}\right) \subseteq V. \tag{1.21}$$

Отметим, что само множество $\operatorname{Val}\left(\mathsf{r}|_{\bigcap_{i=1}^{n} \mathtt{S}_{r_i}}\right)$ может не быть многообразием в K^n.

Кроме того, не для всякого многообразия $V \subseteq K^n$ существует рациональная параметризация r, удовлетворяющая условию

$$\operatorname{Val}\left(\mathsf{r}|_{\bigcap_{i=1}^{n} \mathtt{S}_{r_i}}\right) = V.$$

Замечание 1.48. В том случае, когда $\mathcal{K} = (K, +, \cdot)$ – поле, построение по рациональной параметризации (1.19) (где $r_i = \frac{f_i}{g_i}$ $(i = 1, \ldots, n)$) наименьшего многообразия $V \subseteq K^n$, удовлетворяющего включению (1.21), сводится к построению при лексикографической упорядоченности «$\succ_{\text{lex}}$» базиса Гребнера G для идеала $(x_1 g_1 - f_1, \ldots, x_n g_n - f_n, g_1 \ldots g_n y - 1)$ кольца многочленов $\mathcal{K}[y, t_1, \ldots, t_l, x_1, \ldots, x_n]$ (переменная y исключает обращение знаменателей в нуль), после чего осуществляется выбор из G всех тех многочленов, которые не содержат ни одной из переменных $y, t_1, \ldots, t_l$.

1.2.3. Алгебраические отображения на многообразии.

Понятие «параметризация многообразия» естественно приводит к алгебраическим системам, представляющим собой специальные кольца отображений одного кольца в другое. Рассмотрим кратко эти конструкции.

Рассмотрим вначале конструкцию, характеризующую понятие «полиномиальная параметризация многообразия».

Отображение $\mathsf{f} : K^l \to K^m$ $(l, m \in \mathbf{N})$ называется *полиномиальным* (*регулярным*) отображением, если

$$\mathsf{f}(a_1, \ldots, a_l) = (f_1(a_1, \ldots, a_l), \ldots, f_m(a_1, \ldots, a_l)) \, ((a_1, \ldots, a_l) \in K^l),$$

где $f_1, \ldots, f_m \in K[t_1, \ldots, t_l]$ – фиксированные многочлены. В этом случае говорят, что отображение f представлено в виде $\mathsf{f} = (f_1, \ldots, f_m)$.

Обозначим через $P_{K^l \to K^m}$ $(l, m \in \mathbf{N})$ множество всех полиномиальных отображений $\mathsf{f} : K^l \to K^m$. Определив сумму и произведение отображений $\mathsf{f} = (f_1, \ldots, f_m) \in P_{K^l \to K^m}$ и $\mathsf{g} = (g_1, \ldots, g_m) \in P_{K^l \to K^m}$ равенствами

$$\mathsf{f} + \mathsf{g} = (f_1 + g_1, \ldots, f_m + g_m)$$

и

$$\mathsf{fg} = (f_1 g_1, \ldots, f_m g_m),$$

получим кольцо

$$\mathcal{P}_{K^l \to K^m} = (P_{K^l \to K^m}, +, \cdot),$$

состоящее из всех полиномиальных отображений кольца $\mathcal{K}^l = (K^l, +, \cdot)$ в кольцо $\mathcal{K}^m = (K^m, +, \cdot)$.

Говорят, что отображения $\mathsf{f}, \mathsf{g} \in P_{K^l \to K^m}$ представляют одно и то же полиномиальное отображение многообразия $V \subseteq K^l$ в множество K^m, если $\mathsf{f}|_V = \mathsf{g}|_V$, т.е. если $\mathsf{f}(\mathbf{a}) = \mathsf{g}(\mathbf{a})$ для всех $\mathbf{a} \in V$.

Пусть $P_{V \to K^m}$ – множество всех полиномиальных отображений многообразия V в множество K^m.

Тогда

$$\mathcal{P}_{V \to K^m} = (P_{V \to K^m}, +, \cdot)$$

представляет собой кольцо всех полиномиальных отображений многообразия V в множество K^m.

Замечание 1.49. Зафиксируем многообразие $V \subseteq K^l$ и конечно-порожденный идеал J – кольца $\mathcal{P}_{V \to K}$. Множество

$$\mathsf{v}_{V,l}(J) = \{(a_1, \ldots, a_l) \in V | f(a_1, \ldots, a_l) = 0 \text{ для всех } f \in J\}$$

называется *подмногообразием* многообразия V.

Для любого непустого множества $W \subseteq V$ положим

$$\mathsf{i}_{V,l}(W) = \{f \in P_{V\to K} | f(a_1,\ldots,a_l) = 0 \text{ для всех } (a_1,\ldots,a_l) \in W\}.$$

Ясно, что $\mathsf{i}_{V,l}(W)$ – идеал кольца $\mathcal{P}_{V\to K}$. При этом:

1) $J \subseteq \mathsf{i}_{V,l} \circ \mathsf{v}_{V,l}(J)$ для любого конечно-порожденного идеала J кольца $\mathcal{P}_{V\to K}$;

2) $W \subseteq \mathsf{v}_{V,l} \circ \mathsf{i}_{V,l}(W)$ для любого подмногообразия W многообразия V (если $\mathcal{K}$ – алгебраически замкнутое поле, то $W = \mathsf{v}_{V,l} \circ \mathsf{i}_{V,l}(W)$).

Истинно утверждение: *отображения* $\mathsf{f}_i = (f_1^{(i)},\ldots,f_m^{(i)}) \in P_{K^l\to K^m}$ $(i = 1,2)$ *представляют одно и то же полиномиальное отображение* $\mathsf{f} \in P_{V\to K^m}$ *тогда и только тогда, когда*

$$f_j^{(1)} \equiv f_j^{(2)} \pmod{\mathsf{i}_{\mathcal{K},l}(V)}$$

для всех $j = 1,\ldots,l$.

Отсюда вытекает, что построение любого отображения

$$\mathsf{f} = (f_1,\ldots,f_m) \in P_{V\to K^m},$$

сводится, по своей сути, к выбору компонент f_j $(j = 1,\ldots,l)$ из классов фактор-множества $K[t_1,\ldots,t_l]/_{\mathsf{i}_{\mathcal{K},l}(V)}$.

По этой причине фактор-кольцо

$$\mathcal{K}[t_1,\ldots,t_l]/_{\equiv_{\mathsf{i}_{\mathcal{K},l}(V)}} = (K[t_1,\ldots,t_l]/_{\mathsf{i}_{\mathcal{K},l}(V)},+,\cdot)$$

называется *координатным кольцом многообразия* V.

В терминах координатного кольца могут быть сформулированы алгебраические характеристики многообразия V.

При этом, сравнение многообразия $V \subseteq K^l$ с многообразием $W \subseteq K^m$ может быть осуществлено в терминах сравнения их координатных колец $\mathcal{K}[t_1,\ldots,t_l]/_{\equiv_{\mathsf{i}_{\mathcal{K},l}(V)}}$ и $\mathcal{K}[t_1,\ldots,t_m]/_{\equiv_{\mathsf{i}_{\mathcal{K},m}(W)}}$.

Замечание 1.50. Если $\mathcal{K}$ – поле, то кольцо $\mathcal{K}[t_1,\ldots,t_l]/_{\equiv_{\mathsf{i}_{\mathcal{K},l}(V)}}$, рассматриваемое как векторное пространство, изоморфно векторному пространству $\mathrm{Span}(\{t_1^{\alpha_1}\ldots t_l^{\alpha_l} | t_1^{\alpha_1}\ldots t_l^{\alpha_l} \notin (\mathrm{LT}(\mathsf{i}_{\mathcal{K},l}(V))\})$, где Span – линейная оболочка.

Поэтому, если $\mathcal{K}$ – поле, то выбор представителей $f_j \in K[t_1,\ldots,t_l]/_{\mathsf{i}_{\mathcal{K},l}(V)}$ $(j = 1,\ldots,l)$ может быть осуществлен на основе построения базиса Гребнера идеала $\mathsf{i}_{\mathcal{K},l}(V)$.

Обозначим через $P_{V\to W}$ множество всех полиномиальных отображений $\mathsf{f} \in P_{V\to K^m}$, осуществляющих отображение многообразия $V \subseteq K^l$ в многообразие $W \subseteq K^m$.

Многообразия $V \subseteq K^l$ и $W \subseteq K^m$ называются *изоморфными*, если существуют такие полиномиальные отображения $\mathsf{f} \in P_{V \to W}$ и $\mathsf{g} \in P_{W \to V}$, что отображение $\mathsf{f} \circ \mathsf{g}$ является тождественным отображением на многообразии W, а отображение $\mathsf{g} \circ \mathsf{f}$ – тождественным отображением на многообразии V.

Замечание 1.51. Понятие «изоморфизм многообразий» играет существенную роль при характеристике свойств полиномиальной параметризации многообразия.

В частности, если многообразие $W \subseteq K^m$ изоморфно многообразию $V = K^l$, то существует биекция $\mathsf{f} \in P_{K^l \to W}$, т.е. существует полиномиальная параметризация многообразия W, обладающая «хорошими свойствами».

Рассмотрим теперь конструкцию, характеризующую понятие «рациональная параметризация многообразия».

Частичное отображение $\mathsf{r} : K^l \mapsto \widetilde{K}^m$ $(l, m \in \mathbf{N})$ с непустой областью определения называется *частичным рациональным отображением*, если

$$\mathsf{r}(a_1, \ldots, a_l) = (r_1(a_1, \ldots, a_l), \ldots, r_m(a_1, \ldots, a_l)) \; ((a_1, \ldots, a_l) \in K^l),$$

где $r_i = \frac{f_i}{g_i} \in \widetilde{R}_{\mathcal{K}[x_1,\ldots,x_n]}$ $(i = 1, \ldots, m)$. В этом случае говорят, что частичное рациональное отображение r представлено в виде $\mathsf{r} = \left(\frac{f_1}{g_1}, \ldots, \frac{f_m}{g_m}\right)$.

Обозначим через $R_{K^l \mapsto \widetilde{K}^m}$ $(l, m \in \mathbf{N})$ множество всех частичных рациональных отображений отображений $\mathsf{r} : K^l \mapsto \widetilde{K}^m$.

Определим сумму и произведение частичных рациональных отображений $\mathsf{r}_1 = \left(\frac{f_1^{(1)}}{g_1^{(1)}}, \ldots, \frac{f_m^{(1)}}{g_m^{(1)}}\right)$ и $\mathsf{r}_2 = \left(\frac{f_1^{(2)}}{g_1^{(2)}}, \ldots, \frac{f_m^{(2)}}{g_m^{(2)}}\right)$ равенствами

$$\mathsf{r}_1 + \mathsf{r}_2 = \left(\frac{f_1^{(1)}}{g_{(1)}^1} + \frac{f_1^{(2)}}{g_1^{(2)}}, \ldots, \frac{f_m^{(1)}}{g_m^{(1)}} + \frac{f_m^{(2)}}{g_m^{(2)}}\right),$$

$$\mathsf{r}_1\mathsf{r}_2 = \left(\frac{f_1^{(1)}}{g_1^{(1)}} \cdot \frac{f_1^{(2)}}{g_1^{(2)}}, \ldots, \frac{f_m^{(1)}}{g_m^{(1)}}) \cdot \frac{f_m^{(2)}}{g_m^{(2)}}\right).$$

В кольце $\mathcal{K}$ с делителями нуля следует учитывать обстоятельства, указанные в замечаниях 1.34 и 1.40, которые возникают при сложении и умножении дробей по обычным правилам.

Из-за этих осложнений при построении рациональной параметризации многообразия, как правило, ограничиваются множеством $R_{K^l \mapsto \overline{K}^m}$

$(l, m \in \mathbf{N})$ частичных рациональных отображений. Это дает возможность действовать в рамках кольца

$$\mathcal{R}_{K^l \mapsto \overline{K}^m} = (R_{K^l \to \overline{K}^m}, +, \cdot)$$

всех частичных рациональных отображений кольца $\mathcal{K}^l = (K^l, +, \cdot)$ в кольцо $\overline{\mathcal{K}}^m = (\overline{K}^m, +, \cdot)$.

Если $\mathcal{K}$ – область целостности, то $\mathcal{R}_{K^l \mapsto \overline{K}^m}$ – поле всех частичных рациональных отображений кольца $\mathcal{K}^l$ в поле $\overline{\mathcal{K}}^m$.

Говорят, что частичные рациональные отображения $\mathsf{r}_1, \mathsf{r}_2 \in R_{K^l \mapsto \overline{K}^m}$ представляют одно и то же частичное рациональное отображение многообразия $V \subseteq K^l$ в множество $\overline{K}^m$, если $\mathsf{r}_1|_V = \mathsf{r}_2|_V$, т.е. если $\mathrm{Dom}\,(\mathsf{r}_1|_V) = \mathrm{Dom}\,(\mathsf{r}_2|_V) = V' \subseteq V$ и $\mathsf{r}_1(\mathbf{a}) = \mathsf{r}_2(\mathbf{a})$ для всех $\mathbf{a} \in V'$.

Пусть $R_{V \mapsto \overline{K}^m}$ – множество всех частичных рациональных отображений многообразия $V \subseteq K^l$ в множество $\overline{K}^m$. Истинно утверждение: *частичные отображения* $\mathsf{r}_i = \left(\frac{f_1^{(i)}}{g_1^{(i)}}, \ldots, \frac{f_m^{(i)}}{g_m^{(i)}}\right) \in R_{K^l \mapsto \overline{K}^m}$ $(i = 1, 2)$ *представляют одно и то же частичное рациональное отображение* $\mathsf{r} \in R_{V \mapsto \overline{K}^m}$ *тогда и только тогда, когда* $\mathrm{Dom}\,(\mathsf{r}_1|_V) = \mathrm{Dom}\,(\mathsf{r}_2|_V)$ и $f_j^{(1)} g_j^{(2)} \equiv f_j^{(2)} g_j^{(1)} \pmod{\mathbf{i}_{\mathcal{K},l}(V)}$ для всех $j = 1, \ldots, l$.

Пусть $V \subseteq K^l$ и $W \subseteq K^m$ – непустые неприводимые многообразия, а $R_{V \to W}$ – множество всех таких частичных рациональных отображений $\mathsf{r} \in R_{V \mapsto \overline{K}^m}$, что $\mathsf{r}(V \cap \mathrm{Dom}\,\mathsf{r}) \subseteq W$. Многообразия $V \subseteq K^l$ и $W \subseteq K^m$ называются *бирационально эквивалентными*, если существуют такие отображения $\mathsf{r}_1 \in P_{V \to W}$ и $\mathsf{r}_2 \in P_{W \to V}$, что $\mathsf{r}_1 \circ \mathsf{r}_2$ – тождественное отображение на непустом подмножестве

$$\mathsf{r}_1(\mathsf{r}_2(W \cap \mathrm{Dom}\,\mathsf{r}_2) \cap \mathrm{Dom}\,\mathsf{r}_1) \subseteq W,$$

а $\mathsf{r}_2 \circ \mathsf{r}_1$ – тождественное отображение на непустом подмножестве

$$\mathsf{r}_2(\mathsf{r}_1(V \cap \mathrm{Dom}\,\mathsf{r}_1) \cap \mathrm{Dom}\,\mathsf{r}_2) \subseteq V.$$

Неприводимое многообразие $W \subseteq K^m$ называется *рациональным многообразием*, если существует такое $l \in \mathbf{N}$, что W бирационально эквивалентно множеству K^l. Именно для таких многообразий существуют «хорошие» рациональные параметризации.

Замечание 1.52. Понятие «бирациональная эквивалентность» является более слабым, по сравнению с понятием «изоморфизм многообразий» в том смысле, что

класс бирационально эквивалентных многообразий может содержать неизоморфные многообразия.

Исторически, именно проблема классификации многообразий с точностью до бирациональной эквивалентности сыграла роль мощного катализатора в развитии *алгебраической геометрии* (начиная с XIX-го столетия). По-видимому, это связано с тем обстоятельством, что (по крайней мере, для поля действительных чисел) построение рациональных отображений на многообразиях оказалась более легкой задачей, чем построение полиномиальных отображений.

1.3. Кривые над кольцами.

В настоящем пункте под кольцом $\mathcal{K} = (K, +, \cdot)$ понимается ассоциативно-коммутативное кольцо с единицей. В соответствии с традицией кольцо многочленов от двух переменных над кольцом $\mathcal{K}$ будем обозначать через $\mathcal{K}[x, y] = (K[x, y], +, \cdot)$.

1.3.1. Общие понятия.

Плоской алгебраической кривой Γ над кольцом $\mathcal{K} = (K, +, \cdot)$ называется многообразие $V(f)$ в K^2, где $f \in K[x, y]$ – многочлен положительной степени. В дальнейшем будем рассматривать только плоские алгебраические кривые. Поэтому, для краткости, словосочетание «плоская алгебраическая» будет опускаться.

Замечание 1.53. Если $\mathcal{K}$ – поле, то множество K^2 называется *аффинной плоскостью*, а кривая $\Gamma = V(f)$ $(f \in K[x, y])$ – *аффинной кривой*.

Для кривой $\Gamma = V(f)$ $(f \in K[x, y])$ любое уравнение $g(x, y) = 0$ $(g \in \mathsf{i}_{K,2}(V(f)))$ называется *уравнением кривой* Γ.

Замечание 1.54. Пусть кольцо $\mathcal{K} = (K, +, \cdot)$ не содержит делителей нуля.
Если существует разложение

$$g(x, y) = \prod_{i=1}^{l} g_i^{\alpha_i}(x, y) \ \ (\alpha_1, \ldots, \alpha_n \in \mathbf{N})$$

многочлена $g(x, y)$ на попарно неассоциированные неприводимые многочлены $g_i(x, y)$ $(i = 1, \ldots, l)$, то кривая $V(g)$ является объединением кривых $V(g_i)$ $(i = 1, \ldots, l)$.

Если же $g \in K[x, y]$ – неприводимый многочлен, то говорят, что кривая $V(g)$ – *неприводимая*.

В дальнейшем предполагается, что кривая $\Gamma = V(f)$ $(f \in K[x,y])$ задана таким уравнением $g(x,y) = 0$, что $g \in \mathsf{i}_{K,2}(V(f))$ – многочлен наименьшей положительной степени. Поэтому будем писать $\Gamma = V(g)$.

Степень многочлена g называется *степенью кривой* $\Gamma = V(g)$.

Любой корень $A = (x_0, y_0)$ уравнения $g(x,y) = 0$ называется *точкой* кривой Γ.

Пример 1.10. Рассмотрим над кольцом $\mathcal{K} = (K, +, \cdot)$ кривую 1-й степени Γ, т.е. кривую, определяемую линейным многообразием $V(y - ax)$, где $a \in K \backslash \{0\}$ – фиксированный элемент кольца $\mathcal{K}$.

Для любого кольца $\mathcal{K}$ точка $A = (0,0)$ принадлежит кривой Γ.

Если $\mathcal{K}$ – поле, то отображение $y = ax$ – биекция (множества K на себя).

Если же кольцо $\mathcal{K}$ не является полем, то отображение $y = ax$ не является биекцией для любого делителя нуля $a \in K$.

Кривая $\Gamma = V(g)$ $(g \in K[x,y])$ называется *коникой*, если g – многочлен 2-й степени, и *кубикой*, если g – многочлен 3-й степени.

Замечание 1.55. Общее уравнение коники над кольцом $\mathcal{K} = (K, +, \cdot)$ имеет вид

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \ \ (a, b, c, d, e, f \in K).$$

В зависимости от значений параметров $a, b, c, d, e, f \in K$ можно выделить различные типы коник над кольцом $\mathcal{K}$.

В случае поля $\mathcal{R}$ действительных чисел, стандартная классификация имеет вид: эллипс, парабола, гипербола, изолированная точка, пустое множество, прямая, пара пересекающихся прямых, параллельные прямые, двойная прямая.

В случае произвольного кольца $\mathcal{K}$, классификация коник существенно зависит от структуры этого кольца.

Эта задача является сложной в случае конечного кольца $\mathcal{K}$, так как в этом случае классификации коник, чаще всего, осуществляется в зависимости от контекста решаемых задач.

Значительно сложнее ситуация с кубикой. Известна некоторая классификация кубик (с точностью до бирациональной эквивалентности многообразий) в случае, когда $\mathcal{K} = (K, +, \cdot)$ – поле.

Но даже в этом случае, чаще всего (особенно в прикладных задачах) рассматривают кубики вида

$$y^2 = f(x),$$

где $f \in K[x]$ - многочлен 3-й степени.

Это обусловлено тем, что над алгебраически замкнутым полем неприводимая кубика бирационально эквивалентна кривой именно этого вида.

При этом, кривые $y^2 = f(x)$, для которых многочлен $f(x)$ не имеет кратных корней, называются *эллиптическими кривыми*.

Кривая $\Gamma = V(g)$ ($g \in K[x,y]$) называется *рациональной кривой*, если для многообразия $V(g)$ существует рациональная параметризация

$$\mathsf{r} : K^1 \mapsto \overline{K}^2 \ (\mathsf{r} = (\psi, \chi),\ \psi, \chi \in R_{K \mapsto \overline{K}}),$$

т.е.

$$g(\psi(t), \chi(t)) = 0 \ (t \in \operatorname{Dom}\psi \cap \operatorname{Dom}\chi).$$

Пример 1.11. Пусть $\mathcal{K} = (K, +, \cdot)$ – область целостности.

1. Покажем, что кривая Γ, определяемая уравнением

$$y^2 = x^2 + x^3,$$

является рациональной кривой.

Подставив $y = tx$ в уравнение кривой Γ, получим

$$t^2x^2 = x^2 + x^3 \Leftrightarrow x^2(x + 1 - t^2) = 0 \Leftrightarrow \begin{cases} x = 0 \\ x = t^2 - 1 \end{cases}.$$

Значение $x = 0$ соответстует точке $(0, 0)$ кривой Γ, а положив $x = t^2 - 1$ в выражении $y = tx$, получим полиномиальную параметризацию

$$\begin{cases} x = t^2 - 1 \\ y = t(t^2 - 1) \end{cases} \tag{1.22}$$

кривой Γ, т.е. Γ – рациональная кривая.

Отметим, что точка $(0, 0) \in \Gamma$ получается из (1.22), если положить $t = 1$.

2. Покажем, что кривая Γ, определяемая уравнением

$$y^2 + x^2 = 1,$$

является рациональной кривой.

Подставив $x = \frac{2t}{t^2+1}$ в уравнение кривой Γ, получим

$$y^2 = 1 - \left(\frac{2t}{t^2+1}\right)^2 = \frac{t^4 + 2t^2 + 1 - 4t^2}{(t^2+1)^2} = \frac{t^4 - 2t^2 + 1}{(t^2+1)^2} = \frac{(t^2-1)^2}{(t^2+1)^2} = \left(\frac{t^2-1}{t^2+1}\right)^2.$$

Положив $y = \frac{t^2-1}{t^2+1}$, получим, что

$$\begin{cases} x = \frac{2t}{t^2+1} \\ y = \frac{t^2-1}{t^2+1} \end{cases} \quad \left(t \in \mathsf{S}_{\frac{2t}{t^2+1}} \cap \mathsf{S}_{\frac{t^2-1}{t^2+1}}\right) \tag{1.23}$$

является рациональной параметризацией кривой Γ.

Аналогичным образом, Положив $y = -\frac{t^2-1}{t^2+1}$, получим, что

$$\begin{cases} x = \frac{2t}{t^2+1} \\ y = -\frac{t^2-1}{t^2+1} \end{cases} \quad \left(t \in \mathtt{S}_{\frac{2t}{t^2+1}} \cap \mathtt{S}_{\frac{t^2-1}{t^2+1}} \right) \tag{1.24}$$

является рациональной параметризацией кривой Γ.

Отметим,что рациональная параметризация (1.23) не содержит точку $(0,1) \in \Gamma$, а рациональная параметризация (1.24) не содержит точку $(0,-1) \in \Gamma$.

Замечание 1.56. В том случае, когда $\mathcal{K} = (K, +, \cdot)$ – поле, один из стандартных методов построения рациональной параметризации неприводимой рациональной кривой $\Gamma = V(g)$ ($g \in K[x,y]$) состоит в следующем.

Зафиксируем точку (x_0, y_0) кривой Γ. Точке $(x,y) \neq (x_0,y_0)$ кривой Γ сопоставим угловой коэффициент t прямой, проходящей через точки (x_0,y_0) и (x,y).

Этот метод, в частности, применим при поиске решений обычного рационального уравнения $f(x,y) = 0$ ($x, y \in \mathbf{Q}$) в случае, когда известно одно из его решений.

Однако, для произвольного кольца $\mathcal{K}$, не являющегося полем, семейство отображений $y = ax$ ($a \in K$) не может рассматриваться как проектирование из точки (x_0,y_0) на множество K. Именно в силу этого обстоятельства и возникают существенные трудности при попытках установить соответствие между значениями параметра и точками исследуемой кривой.

Пусть Γ – кривая, заданная над кольцом $\mathcal{K} = (K, +, \cdot)$ уравнением $g(x,y) = 0$. Точка (x_0,y_0) кривой Γ называется

1) *особой* точкой, если $\mathsf{D}_x g(x,y)|_{(x_0,y_0)} = 0$ и $\mathsf{D}_y g(x,y)|_{(x_0,y_0)} = 0$;

2) *простой* точкой, если она не является особой точкой.

Кривая Γ над кольцом $\mathcal{K} = (K, +, \cdot)$, все точки которой – простые, называется *гладкой* кривой.

Любая неприводимая кривая над любым кольцом $\mathcal{K}$ без делителей нуля может иметь только конечное число особых точек.

Пример 1.12. Пусть $\mathcal{K} = (K, +, \cdot)$ – поле, характеристика которого не равна 2.

1. Для кривой Γ, заданной уравнением

$$y^2 + x^2 = 1,$$

получим

$$\begin{cases} \mathsf{D}_x(y^2+x^2-1) = 0 \\ \mathsf{D}_y(y^2+x^2-1) = 0 \end{cases} \Leftrightarrow \begin{cases} 2x = 0 \\ 2y = 0 \end{cases} \Leftrightarrow (x,y) = (0,0).$$

Так как $(0,0) \notin \Gamma$, то Γ – гладкая кривая.

2. Любая неприводимая коника над любым полем $\mathcal{K}$ является гладкой кривой.

3. Для кривой Γ, заданной уравнением

$$y^2 = x^2 + x^3,$$

получим

$$\begin{cases} \mathsf{D}_x(x^2 + x^3 - y^2) = 0 \\ \mathsf{D}_y(y^2 - x^2 - x^3) = 0 \end{cases} \Leftrightarrow \begin{cases} x(2 + 3x) = 0 \\ 2y = 0 \end{cases} .$$

Ясно, что если $\mathcal{K}$ – поле характеристики 3, то кривая Γ имеет единственную особую точку $(0, 0) \in \Gamma$.

Пример 1.13. Для кривой Γ, заданной уравнением

$$y^2 = f(x),$$

где $f(x)$ – многочлен 3-й степени, получим

$$\begin{cases} \mathsf{D}_x(y^2 - f(x)) = 0 \\ \mathsf{D}_y(y^2 - f(x)) = 0 \end{cases} \Leftrightarrow \begin{cases} \mathsf{D}_x f(x) = 0 \\ 2y = 0 \end{cases} \Leftrightarrow \begin{cases} \mathsf{D}_x f(x) = 0 \\ y = 0 \end{cases} .$$

Это означает, что кривая Γ имеет особую точку тогда и только тогда, когда многочлен $f(x)$ имеет кратный корень.

Отсюда вытекает, что эллиптическая кривая является гладкой кривой.

Замечание 1.57. Пусть (x_0, y_0) – особая точка неприводимой кривой $\Gamma = V(g)$ над областью целостности $\mathcal{K} = (K, +, \cdot)$.

При замене $x \to x - x_0$, $y \to y - y_0$ (т.е. при сдвиге начала координат в точку (x_0, y_0)) особой точкой кривой Γ становится точка $(0, 0)$.

При этом в уравнении кривой Γ младшие члены многочлена имеют степень r $(r \geq 2)$. В этом случае говорят, что точка $(0, 0)$ является *r-кратной* особой точкой кривой Γ.

Рассмотрим следующие случаи.

1. Пусть $r = 2$, т.е. $(0, 0)$ – 2-кратная особая точка.

Тогда в уравнении неприводимой кривой Γ младшие члены многочлена имеют вид $ax^2 + bxy + cy^2$. Если при переходе к алгебраически замкнутому полю $\mathcal{K}' \supseteq \mathcal{K}$ многочлен $ax^2 + bxy + cy^2$:

1) разлагается на два различных линейных множителя, то особая точка $(0, 0)$ называется *узлом*;

2) является полным квадратом, то особая точка $(0, 0)$ называется *острием*.

2. Пусть Γ – неприводимая кривая степени $n \in \mathbf{N}$, а точка $(0, 0)$ является $(n-1)$-кратной особой точкой.

При переходе к алгебраически замкнутому полю $\mathcal{K}' \supseteq \mathcal{K}$ кривая Γ является рациональной кривой.

3. Пусть Γ – неприводимая кривая степени $n \in \mathbf{N}$, а точка $(0,0)$ является $(n-2)$-кратной особой точкой.

Тогда кривая Γ называется *гиперэллиптической кривой*.

Результаты, связанные с алгебраическими отображениями на многообразии (см. п.1.2.3), могут быть следующим образом проинтерпретированы для неприводимой кривой $\Gamma = V(g)$ $(g \in K[x,y])$ над кольцом $\mathcal{K} = (K, +, \cdot)$.

Частичное рациональное отображение

$$r(x,y) = \frac{p(x,y)}{q(x,y)} \in R_{K^2 \mapsto \overline{K}}$$

определено во всех таких точках $(x_0, y_0) \in K^2$, что $q(x_0, y_0) \neq 0$.

Такие точки $(x_0, y_0) \in K^2$ называются *регулярными* для частичного рационального отображения r.

Ниже под частичным рациональным отображением, определенным на неприводимой кривой $\Gamma = V(g)$ $(g \in K[x,y])$ над кольцом $\mathcal{K} = (K, +, \cdot)$, понимается такое частичное не равное тождественно нулю на своей области определения рациональное отображение

$$r(x,y) = \frac{p(x,y)}{q(x,y)} \in R_{K^2 \mapsto \overline{K}},$$

что $p, q \in K[x,y]$, $\mathrm{Val}\,(q|_\Gamma) \subseteq S_\mathcal{K}$, причем многочлен q не делится на многочлен g.

Отсюда, в частности, вытекает, что многочлен q не является нулевым многочленом на рассматриваемой неприводимой кривой $\Gamma = V(g)$.

Пусть (x_0, y_0) – простая точка неприводимой кривой Γ.

Если частичное рациональное отображение r на кривой Γ может быть представлено в виде

$$r = t^k r_1, \tag{1.25}$$

где $k \in \mathbf{Z}$, а t – частичное рациональное отображение, удовлетворяющее условию $t(x_0, y_0) = 0$, а r_1 – такое частичное рациональное отображение, что $r_1(x_0, y_0) \neq 0$, то отображение t называется *локальным параметром* в точке (x_0, y_0).

Замечание 1.58. Пусть $\mathcal{K}$ – алгебраически замкнутое поле. Тогда:

1) в качестве локального параметра может быть выбрана переменная x, если $\mathsf{D}_y g|_{(x_0,y_0)} \neq 0$, и переменная y, если $\mathsf{D}_x g|_{(x_0,y_0)} \neq 0$;

2) любые два локальных параметра t_1 и t_2 связаны соотношением $t_1 = t_2 h$, где h – такое регулярное в точке (x_0, y_0) частичное рациональное отображение, что $h(x_0, y_0) \neq 0$.

В равенстве (1.25) для частичного рационального отображения r число k называется *кратностью нуля* в точке (x_0, y_0), если $k \in \mathbf{N}$, и *кратностью полюса* в точке (x_0, y_0), если $-k \in \mathbf{N}$.

Частичные рациональные отображения $r_1(x, y) = \frac{p_1(x,y)}{q_1(x,y)} \in R_{K^2 \mapsto \overline{K}}$ и $r_2(x, y) = \frac{p_2(x,y)}{q_2(x,y)} \in R_{K^2 \mapsto \overline{K}}$ равны на кривой Γ тогда и только тогда, когда

$$\operatorname{Dom} r_1 \cap \Gamma = \operatorname{Dom} r_2 \cap \Gamma$$

и многочлен $p_1 q_2 - q_1 p_2$ делится на многочлен g.

Обозначим через $R(\Gamma)$ множество всех частичных рациональных отображений кривой Γ в множество $\overline{K}$.

Кольцо

$$\mathcal{R}(\Gamma) = (R(\Gamma), +, \cdot)$$

представляет собой кольцо всех частичных рациональных отображений кривой Γ в множество $\overline{K}$.

А так как $g(x, y) = 0$ (т.е. элементы x и y алгебраически зависимы) для любой точки $(x, y) \in \Gamma$, то степень трансцендентности кольца $\mathcal{R}(\Gamma)$ относительно кольца $\mathcal{K}$ равна единице.

Пусть $\Gamma = V(x - a)$ (соответственно, $\Gamma = V(y - a)$), где $a \in K$ – фиксированный элемент кольца $\mathcal{K}$.

Тогда каждое частичное рациональное отображение $r(x, y)$ на Γ представляет собой частичное рациональное отображение $r(a, y)$ (соответственно, $r(x, a)$) от одного переменного, т.е. $\mathcal{R}(\Gamma) = \mathcal{R}_{K \mapsto \overline{K}}$.

Отсюда, в частности, вытекает, что построение рациональной параметризации для неприводимой рациональной кривой Γ эквивалентно поиску двух таких частичных рациональных отображений $x = \psi(t)$, $y = \chi(t)$ $(\psi, \chi \in R_{K \mapsto \overline{K}})$, что каждому частичному рациональному отображению $r \in R(\Gamma)$ соответствует такое частичное рациональное отображение $h_r(t) \in R_{K \mapsto \overline{K}}$, что $h_r(t) = r(\psi(t), \chi(t))$.

Замечание 1.59. Пусть $\mathcal{K}$ – алгебраически замкнутое поле. Тогда:

1) если $r_1 \neq r_2$ $(r_1, r_2 \in R(\Gamma))$, то $h_{r_1} \neq h_{r_2}$;

2) кривая Γ является рациональной кривой тогда и только тогда, когда она бирационально эквивалентна прямой.

1.3.2. Проективная плоскость.

Пусть $\mathcal{K} = (K, +, \cdot)$ – поле. Определим на множестве

$$\mathbf{S} = \{(\xi, \eta, \zeta) \in K^3 | (\xi, \eta, \zeta) \neq (0, 0, 0)\}$$

отношение эквивалентности «$\sim$» следующим образом:

$$(\forall (\xi_1, \eta_1, \zeta_1), (\xi_2, \eta_2, \zeta_2) \in \mathbf{S})((\xi_1, \eta_1, \zeta_1) \sim (\xi_2, \eta_2, \zeta_2) \Leftrightarrow$$

$$\Leftrightarrow (\exists \lambda \in K \backslash \{0\})(\xi_1 = \lambda \xi_2 \,\&\, \eta_1 = \lambda \eta_2 \,\&\, \zeta_2 = \lambda \zeta_1)).$$

Фактор-множество $\mathbf{P} = \mathbf{S}/_{\sim}$ называется *проективной плоскостью* над полем $\mathcal{K}$, а элементы множества $\mathbf{P}$ – *точками* проективной плоскости.

Для представления точки

$$M = \{(\lambda \xi, \lambda \eta, \lambda \zeta) | \lambda \in K \backslash \{0\}\} \in \mathbf{P}, \tag{1.26}$$

в *проективных координатах* (их называют также *однородными координатами*) используется запись

$$M = (\xi : \eta : \zeta). \tag{1.27}$$

Относительно координаты ζ точки проективной плоскости $\mathbf{P}$ делятся на следующие два класса.

К 1-му классу относятся все точки $M \in \mathbf{P}$, для которых $\zeta \neq 0$.

Для любой такой точки запись (1.27) эквивалентна записи

$$M = (x : y : 1),$$

где $x = \frac{\xi}{\zeta}$ и $y = \frac{\eta}{\zeta}$.

Точка $M = (x : y : 1) \in \mathbf{P}$ может быть отождествлена с точкой (x, y) аффинной плоскости.

Таким образом, проективная плоскость $\mathbf{P}$ содержит аффинную плоскость

$$\mathbf{A}_3 = \{(x, y) | x, y \in K\}.$$

Ко 2-му классу относятся все точки $M \in \mathbf{P}$, для которых $\zeta = 0$. Такие точки называются *бесконечно удаленными* точками.

Замечание 1.60. Указанная выше классификация точек проективной плоскости $\mathbf{P}$ имеет следующую геометрическую интерпретацию в случае поля $\mathcal{R}$ всех действительных чисел.

Зафиксируем в 3-х мерном пространстве прямоугольную декартову систему координат $(O; x, y, z)$ и проведем плоскость $z = 1$.

Каждой точке $M = (x, y, 1)$ аффинной плоскости $z = 1$ соответствует прямая, проходящая через точки O и M, причем это соответствие – взаимно-однозначное.

Каждой бесконечно удаленной точке $M = (\xi : \eta : 0)$ проективной плоскости $\mathbf{P}$ соответствует прямая, лежащая в плоскости $z = 1$ и пересекающая ось Oz, причем это соответствие – взаимно-однозначное. Такие прямые называются *асимптотическими направлениями* (или *пучками параллельных прямых*).

Таким образом, проективная плоскость $\mathbf{P}$ состоит из аффинной плоскости $\mathbf{A}_3$, к которой добавлено по одной бесконечно удаленной точке для каждого асимптотического направления.

Аналогичным образом, относительно координаты ξ точки проективной плоскости $\mathbf{P}$ делятся на точки аффинной плоскости

$$\mathbf{A}_1 = \{(y, z) | y, z \in K\},$$

где $y = \frac{\eta}{\xi}$ и $z = \frac{\zeta}{\xi}$, и бесконечно удаленные точки, для которых $\xi = 0$, а относительно координаты η точки проективной плоскости $\mathbf{P}$ делятся на точки аффинной плоскости

$$\mathbf{A}_2 = \{(x, z) | x, z \in K\},$$

где $x = \frac{\xi}{\eta}$ и $z = \frac{\zeta}{\eta}$, и бесконечно удаленные точки, для которых $\eta = 0$.

Аффинные плоскости $\mathbf{A}_1$, $\mathbf{A}_2$ и $\mathbf{A}_3$ попарно пересекаются.

Действительно, пусть $M = (\xi : \eta : \zeta) \in \mathbf{P}$ – такая точка , что $\xi \neq 0$, $\eta \neq 0$ и $\zeta \neq 0$. Тогда точка M имеет:

1) в аффинной плоскости $\mathbf{A}_1$ координаты $(y, z) = (\frac{\eta}{\xi}, \frac{\zeta}{\xi})$;

2) в аффинной плоскости $\mathbf{A}_2$ координаты $(x', z') = (\frac{\xi}{\eta}, \frac{\zeta}{\eta})$, т.е. $x' = \frac{1}{y}$ и $z' = \frac{z}{y}$;

3) в аффинной плоскости $\mathbf{A}_3$ координаты $(x'', y'') = (\frac{\xi}{\zeta}, \frac{\eta}{\zeta})$, т.е. $x'' = \frac{1}{z}$ и $y'' = \frac{y}{z}$, а также $x'' = \frac{x'}{z'}$ и $y'' = \frac{1}{z'}$.

Аффинное преобразование аффинной плоскости $\mathbf{A}_3$ имеет вид

$$\mathbf{u}' = A\mathbf{u} + \mathbf{b}, \tag{1.28}$$

где $\mathbf{u} = (x, y)^T$, A – обратимая 2×2-матрица (если A – ортогональная матрица, то преобразование (1.28) называется *евклидовым*), а $\mathbf{b} = (b_1, b_2)^T$ – вектором сдвига.

Замечание 1.61. Известно, что любая коника с помощью евклидового преобразования приводится к *канонической форме*. Классификация канонических форм коник над полем $\mathcal{R}$ действительных чисел приведена в замечании 1.55.

Проективное преобразование проективной плоскости $\mathbf{P}$ имеет вид

$$\mathbf{U}' = D\mathbf{U}, \tag{1.29}$$

где D – обратимая 3×3-матрица, а $\mathbf{U} = (\xi, \eta, \zeta)^T$.

Замечание 1.62. Пусть для проективного преобразования (1.29) матрица D представлена в виде

$$D = \left(\begin{array}{cc|c} & & \\ & A & \\ & & \\ \hline c & d & e \end{array}\right) \begin{array}{c} \\ \\ \\ \\ \mathbf{b} \end{array}.$$

Тогда на аффинной плоскости $\mathbf{A}_3$ проективное преобразование (1.29) совпадает с дробно-линейным преобразованием

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \frac{1}{cx + dy + e} \left(A \begin{pmatrix} x \\ y \end{pmatrix} + \mathbf{b} \right),$$

которое определено тогда и только тогда, когда $cx + dy + e \neq 0$.

Проективная кривая (в проективной плоскости $\mathbf{P}$) задается уравнением

$$G(\xi, \eta, \zeta) = 0,$$

где G – однородный многочлен.

Замечание 1.63. Для любого $\lambda \neq 0$ равенство $G(\xi, \eta, \zeta) = 0$ сохраняется при замене $\xi' = \lambda\xi$, $\eta' = \lambda\eta$ и $\zeta' = \lambda\zeta$. Это означает, что задание алгебраической кривой в проективной плоскости не зависит от выбора однородных координат точки.

Аффинной кривой Γ_g, определяемой уравнением

$$g(x, y) = 0,$$

где $g(x, y)$ – многочлен степени n, соответствует проективная кривая Γ_G, определяемая уравнением

$$G(\xi, \eta, \zeta) = 0,$$

где

$$G(\xi, \eta, \zeta) = \zeta^n g\left(\frac{\xi}{\zeta}, \frac{\eta}{\zeta}\right)$$

представляет собой однородный многочлен степени n.

Обратно, каждая проективная кривая Γ, определяемая уравнением

$$G(\xi, \eta, \zeta) = 0,$$

где $G(\xi, \eta, \zeta)$ – однородный многочлен степени n состоит из аффинной кривой $\Gamma \cap \mathbf{A}_3$, определяемой уравнением

$$g(x, y) = 0,$$

где

$$g(x, y) = G(x, y, 1)$$

является многочленом степени n, и бесконечно удаленных точек $(\xi, \eta, 0)$, удовлетворяющих уравнению

$$G(\xi, \eta, 0) = 0.$$

Пример 1.14. 1. Аффинной прямой

$$ax + by + c = 0,$$

где $a, b, c \in K$, причем a и b одновременно не равны нулю, соответствует проективная прямая Γ, определяемая уравнением

$$a\xi + b\eta + c\zeta = 0.$$

Прямая Γ проходит через такую бесконечно удаленную точку $M = (\xi : \eta : 0)$, что

$$a\xi + b\eta = 0.$$

Отсюда вытекает, что проективные прямые, соответствующие параллельным аффинным прямым, пересекаются в одной и той же бесконечно удаленной точке проективной плоскости $\mathbf{P}$.

2. *Кониками* в проективной плоскости $\mathbf{P}$ называются кривые, определяемые уравнением $G(\xi,\eta,\zeta)=0$, где $G(\xi,\eta,\zeta)$ – однородный многочлен 2-й степени.

В случае поля $\mathcal{R}$ действительных чисел с помощью проективного преобразования любая коника в проективной плоскости $\mathbf{P}$ может быть приведена к одному из следующих видов:

1) *невырожденная коника*, определяемая уравнением $\xi^2+\eta^2-\zeta^2=0$;

2) *пустое множество*, определяемое уравнением $\xi^2+\eta^2+\zeta^2=0$;

3) *пара прямых*, определяемая уравнением $\xi^2-\eta^2=0$;

4) *точка* $(0,0,1)$, определяемая уравнением $\xi^2+\eta^2=0$;

5) *двойная прямая*, определяемая уравнением $\xi^2=0$.

Осуществив в частичном рациональном отображении

$$r(x,y)=\frac{p(x,y)}{q(x,y)}$$

подстановку $x=\frac{\xi}{\zeta}$ и $y=\frac{\eta}{\zeta}$, получим частичное рациональное отображение

$$R(\xi,\eta,\zeta)=\frac{P(\xi,\eta,\zeta)}{Q(\xi,\eta,\zeta)},$$

определенное на проективной плоскости $\mathbf{P}$, где P и Q – однородные многочлены.

Отсюда вытекает, что каждому частичному рациональному отображению

$$(x,y)\mapsto(r_1(x,y),r_2(x,y))$$

аффинной плоскости $\mathbf{A}_3$ в себя соответствует такое частичное отображение

$$(\xi:\eta:\zeta)\mapsto(P(\xi,\eta,\zeta):Q(\xi,\eta,\zeta):H(\xi,\eta,\zeta)), \tag{1.30}$$

проективной плоскости $\mathbf{P}$ в себя, что P, Q и H – однородные многочлены одной и той же степени $n\in\mathbf{N}$.

Отображение (1.30) регулярно в точке $M=(\xi:\eta:\zeta)\in\mathbf{P}$ тогда и только тогда, когда в этой точке хотя бы один из многочленов P, Q или H не обращается в нуль.

Пусть Γ – кривая в проективной плоскости $\mathbf{P}$, определяемая уравнением $G(\xi,\eta,\zeta)=0$.

Точка $M=(\xi_0:\eta_0:\zeta_0)\in\Gamma$ называется:

1) *особой* точкой, если $\mathsf{D}_\xi G(\xi,\eta,\zeta)|_{(\xi_0,\eta_0,\zeta_0)}=0$, $\mathsf{D}_\eta G(\xi,\eta,\zeta)|_{(\xi_0,\eta_0,\zeta_0)}=0$ и $\mathsf{D}_\zeta G(\xi,\eta,\zeta)|_{(\xi_0,\eta_0,\zeta_0)}=0$;

2) *простой* точкой, если она не является особой точкой.

Кривая Γ в проективной плоскости $\mathbf{P}$, все точки которой – простые, называется *гладкой* кривой.

Для того, чтобы исследовать свойства отображения (1.30) для точек аффинной плоскости $\mathbf{A}_3$, достаточно представить его (разделив многочлены P, Q и H на ζ^n) в виде

$$(x, y) \mapsto (u(x, y), v(x, y), w(x, y)). \tag{1.31}$$

где u, v и w – многочлены.

Отображение (1.31) регулярно в каждой такой точке $(x_0, y_0) \in \mathbf{A}_3$, что все три многочлена u, v и w не обращаются в нуль.

Пусть Γ – кривая в проективной плоскости $\mathbf{P}$ и для многочленов u, v и w существует представление (1.25) в простой точке $(x_0, y_0) \in \mathbf{A}_3$ кривой $\Gamma \cap \mathbf{A}_3$. Тогда отображение (1.31) регулярно в точке (x_0, y_0).

Используя построенные выше конструкции, можно показать, что бирациональный изоморфизм гладких проективных кривых регулярен во всех точках и является взаимно-однозначным соответствием.

Отсюда, в частности, вытекает, что никакая эллиптическая кривая бирационально не изоморфна прямой, т.е. не является рациональной кривой.

Если Γ неприводимая гладкая кубика в проективной плоскости $\mathbf{P}$, то точки кривой Γ обладают структурой абелевой группы.

Это обстоятельство, а также высокая сложность решения уравнений в этой абелевой группе в случае конечного поля $\mathcal{K}$ явились основным фактором применения эллиптических кривых над конечными полями при решении задач современной криптографии.

Предположим теперь, что кольцо $\mathcal{K} = (K, +, \cdot)$ не является полем.

Пусть $\mathcal{K} = (K, +, \cdot)$ – область целостности. Тогда исследование кривой

$$\Gamma = V(g) \ (g \in K[x, y])$$

может быть осуществлено следующим образом.

Перейдем к полю частных $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ и рассмотрим над этим полем, кривую $\overline{\Gamma}$, определенную уравнением $g(x, y) = 0$ $(x, y \in \overline{K})$. Для исследования кривой $\overline{\Gamma}$ могут быть использованы все рассмотренные выше конструкции. Следовательно, для нее истинны все установленные выше результаты.

Теперь остается переформулировать эти результаты для кривой Γ, т.е. сформулировать их при дополнительном условии, что $x, y \in K$.

Пусть кольцо $\mathcal{K} = (K, +, \cdot)$ содержит делители нуля. Тогда при исследовании кривой Γ возникают следующие обстоятельства.

Во-первых, при построении кольца частных $\overline{\mathcal{K}}$ обратимыми становятся только элементы, принадлежащие множеству $S_{\mathcal{K}}$.

Из-за этого возникают сложности, связанные с построением рациональной параметризации кривой Γ. В частности, возникает вопрос о существовании локальной параметризации (1.25) для кривой Γ.

Во-вторых, при построении проективной плоскости $\mathbf{P}$ описанным выше способом естественно определить отношение эквивалентности «$\sim$» на множестве $\mathbf{S}$ следующим образом: $(\xi_1, \eta_1, \zeta_1) \sim (\xi_2, \eta_2, \zeta_2)$ тогда и только тогда, когда (ξ_1, ξ_2), (η_1, η_2) и (ζ_1, ζ_2) – пары ассоциированных элементов мультипликативной полугруппы $(\overline{K}, \cdot)$.

Однако, при этом в множестве $\mathbf{P}$ возникают точки вида

$$M = \{(\lambda\xi, \lambda\eta, \lambda\zeta) | \lambda \in \overline{K}^{inv}\},$$

где ξ, η и ζ – делители нуля.

Эти точки не являются ни точками аффинной плоскости, ни бесконечно удаленными точками.

Из-за наличия таких точек возникают сложности при интерпретации для кривой $\Gamma = V(g)$ $(g \in K[x, y])$ свойств соответствующей ей кривой, определенной в множестве $\mathbf{P}$.

Замечание 1.64. Аналог проективной плоскости для кольца вычетов рассмотрен в п.2.3.5.

2. НЕКОТОРЫЕ ТИПЫ КРИВЫХ НАД КОНЕЧНЫМИ КОЛЬЦАМИ

В настоящем разделе рассмотрены некоторые типы кривых над ассоциативно-коммутативным кольцом $\mathcal{K} = (K, +, \cdot)$.

В п.2.1 исследуются коники над кольцом $\mathcal{K}$. Найдены множества точек разложимых коник, а также коник специального вида. Охарактеризовано множество особых точек коники. Исследуются методы приведения коники к каноническому виду. В п.2.2 исследуется кубика над кольцом $\mathcal{K}$, представленная уравнением

$$ay^2 = b_3x^3 + b_2x^2 + b_1x + b_0 \ (a, b_3 \in K\backslash\{0\}; b_2, b_1, b_0 \in K).$$

Найдены множества точек разложимых кубик. Охарактеризовано множество особых точек кубики. Установлены условия существования кратных корней многочлена, являющегося правой частью уравнения кубики. В п.2.3 рассмотрены основные свойства эллиптических кривых над полями, а также некоторые приложения эллиптических кривых.

Результаты авторов, представленные в разделе, опубликованы в [52,58].

Известные результаты изложены в соответствии с [7,32,36,42].

2.1. Коники над кольцами.

Общее уравнение коники Γ над кольцом $\mathcal{K} = (K, +, \cdot)$ имеет вид

$$a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0, \tag{2.1}$$

где $a_{11}, a_{12}, a_{22}, a_1, a_2, a_0 \in K$, причем $(a_{11}, a_{12}, a_{22}) \neq (0, 0, 0)$.

2.1.1. Типы коник над кольцом.

Для многочлена

$$f(x, y) = a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0$$

возможны следующие три ситуации.

Ситуация 2.1. Многочлен $f(x, y)$ неразложим над кольцом $\mathcal{K}$.

Ситуация 2.2. Для любых многочленов $f_i \in \mathcal{K}[x, y]$ $(i = 1, 2)$ степени $m_i \geq 1$ $(i = 1, 2)$, удовлетворяющих равенству

$$f(x, y) = f_1(x, y)f_2(x, y),$$

истинно неравенство

$$m_1 + m_2 > 2.$$

Ситуация 2.3. Существуют многочлены $f_i \in \mathcal{K}[x, y]$ $(i = 1, 2)$ степени $m_i = 1$ $(i = 1, 2)$, удовлетворяющие равенству

$$f(x, y) = f_1(x, y)f_2(x, y).$$

Если имеет место ситуация 2.2, то $f(x, y)$ – многочлен наименьшей степени, определяющий конику Γ. Поэтому, в этой ситуации анализ коники Γ осуществляется непосредственно на основе уравнения (2.1).

Если имеет место ситуация 2.3, то при известном разложении многочлена $f(x, y)$ уравнение (2.1) естественно представить в виде

$$(b_1x + b_2y + b_0)(c_1x + c_2y + c_0) = 0. \tag{2.2}$$

Множество точек коники Γ, определенной уравнением (2.2), может быть представлено в виде

$$\Gamma = S_1 \cup S_2 \cup S_3,$$

где S_1 – объединение множеств решений однопараметрического семейства F_α $(\alpha \in K)$ систем линейных уравнений

$$F_\alpha : \begin{cases} b_1x + b_2y + b_0 = 0 \\ c_1x + c_2y + c_0 = \alpha \end{cases},$$

S_2 – объединение множеств решений однопараметрического семейства G_β $(\beta \in K\backslash\{0\})$ систем линейных уравнений

$$G_\beta : \begin{cases} b_1x + b_2y + b_0 = \beta \\ c_1x + c_2y + c_0 = 0 \end{cases},$$

а S_3 – объединение множеств решений двухпараметрического семейства $H_{\alpha,\beta}$ $(\alpha, \beta \in K\backslash\{0\}, \alpha\beta = 0)$ систем линейных уравнений

$$H_{\alpha,\beta} : \begin{cases} b_1x + b_2y + b_0 = \alpha \\ c_1x + c_2y + c_0 = \beta \end{cases}.$$

Замечание 2.1. Таким образом, в случае конечного кольца построение в явном виде множества точек коники Γ в ситуациях 2.1 и 2.2 эквивалентно поиску множества решений нелинейного уравнения (2.1) от двух переменных, а в ситуации 2.3 – поиску множеств решений трех семейств F_α $(\alpha \in K)$, G_β $(\beta \in K\backslash\{0\})$ и $H_{\alpha,\beta}$ $(\alpha, \beta \in K\backslash\{0\}, \alpha\beta = 0)$ систем линейных уравнений.

Отметим, что если кольцо $\mathcal{K}$ не содержит делителей нуля, то

$$H_{\alpha,\beta} = \emptyset.$$

2.1.2. Особые точки коник над кольцом.

Охарактеризуем особые точки коники (2.1).

Из определения особой точки кривой вытекает, что множеством особых точек коники (2.1) является множество решений системы уравнений

$$\begin{cases} \mathsf{D}_x(a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0) = 0 \\ \mathsf{D}_y(a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0) = 0 \\ a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 2a_{11}x + a_{12}y + a_1 = 0 \\ a_{12}x + 2a_{22}y + a_2 = 0 \\ a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0 \end{cases} .$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 2.1. Коника Γ, определяемая уравнением (2.1) имеет особые точки тогда и только тогда, когда существует такое решение (x_0, y_0) системы линейных уравнений

$$\begin{cases} 2a_{11}x + a_{12}y = -a_1 \\ a_{12}x + 2a_{22}y = -a_2 \end{cases} , \tag{2.3}$$

что истинно равенство

$$a_{11}x_0^2 + a_{12}x_0y_0 + a_{22}y_0^2 + a_1x_0 + a_2y_0 + a_0 = 0.$$

Пусть характеристика кольца $\mathcal{K}$ равна 2. Тогда система уравнений (2.3) принимает вид

$$\begin{cases} a_{12}y = -a_1 \\ a_{12}x = -a_2 \end{cases} . \tag{2.4}$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 2.2. Пусть характеристика кольца $\mathcal{K}$ равна 2. Тогда коника Γ, определяемая уравнением (2.1):

1) имеет единственную особую точку, если $a_{12} \in K^{inv}$ и

$$a_{11}a_2^2 - a_{12}a_1a_2 + a_{22}a_1^2 + a_0a_{12}^2 = 0;$$

2) является гладкой кривой, если либо $a_{12} \in K^{inv}$ и

$$a_{11}a_2^2 - a_{12}a_1a_2 + a_{22}a_1^2 + a_0a_{12}^2 \neq 0,$$

либо $a_{12} \notin K^{inv}$ и, кроме того, $a_1 \in K^{inv}$ или $a_2 \in K^{inv}$.

2.1.3. Характеристика множеств точек коник над кольцом.

Рассмотрим следующие специальные случаи уравнения (2.1).

1. Пусть

$$\begin{cases} a_{22} \neq 0 \\ a_{11} = a_{12} = a_1 = 0 \end{cases}.$$

Тогда уравнение (2.1) принимает вид

$$a_{22}y^2 + a_2y + a_0 = 0. \tag{2.5}$$

Следовательно, коника Γ состоит из всех таких точек $(x_0, y_0) \in K^2$, что y_0 – корень уравнения (2.5) над кольцом $\mathcal{K}$.

В частности, если уравнение (2.5) не имеет решений над кольцом $\mathcal{K}$, то $\Gamma = \emptyset$.

2. Пусть

$$\begin{cases} a_{22} \neq 0 \\ a_{11} = a_{12} = 0 \\ a_1 \neq 0 \end{cases}.$$

Истинна следующая теорема.

Теорема 2.1. Пусть характеристика кольца $\mathcal{K}$ отлична от 2. Если $a_{11} = a_{12} = 0$, $a_{22} \neq 0$, $a_1 \neq 0$ и существуют такие элементы $b, c \in K\backslash\{0\}$, что

$$\begin{cases} a_{22} = cb^2 \\ a_2 = 2cb \end{cases}, \tag{2.6}$$

то коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что

$$(w_0, u_0) = (by_0 + 1, x_0)$$

является корнем уравнения

$$cw^2 + a_1 u + (a_0 - c) = 0 \tag{2.7}$$

над кольцом $\mathcal{K}$.

Доказательство. Пусть характеристика кольца $\mathcal{K}$ отлична от 2.

Если $a_{11} = a_{12} = 0$, $a_{22} \neq 0$, $a_1 \neq 0$, то уравнение (2.1) принимает вид

$$a_{22}y^2 + a_1 x + a_2 y + a_0 = 0. \tag{2.8}$$

Подставив (2.6) в (2.8), получим

$$c(by + 1)^2 + a_1 x + (a_0 - c) = 0. \tag{2.9}$$

Положив в (2.9)

$$\begin{cases} w = by + 1 \\ u = x \end{cases},$$

получим уравнение (2.7).

Отсюда вытекает, что $(x_0, y_0) \in \Gamma$ тогда и только тогда, когда

$$(w_0, u_0) = (by_0 + 1, x_0)$$

является корнем уравнения (2.7) над кольцом $\mathcal{K}$.

□

3. Пусть

$$\begin{cases} a_{11} \neq 0 \\ a_{22} = a_{12} = a_2 = 0 \end{cases}.$$

Тогда уравнение (2.1) принимает вид

$$a_{11}x^2 + a_1 x + a_0 = 0. \tag{2.10}$$

Следовательно, коника Γ состоит из всех таких точек $(x_0, y_0) \in K^2$, что x_0 – корень уравнения (2.10) над кольцом $\mathcal{K}$.

В частности, если уравнение (2.10) не имеет решений над кольцом $\mathcal{K}$, то $\Gamma = \emptyset$.

4. Пусть

$$\begin{cases} a_{11} \neq 0 \\ a_{22} = a_{12} = 0 \\ a_2 \neq 0 \end{cases}.$$

Истинна следующая теорема.

Теорема 2.2. Пусть характеристика кольца $\mathcal{K}$ отлична от 2. Если $a_{11} \neq 0$, $a_{22} = a_{12} = 0$, $a_2 \neq 0$ и существуют такие элементы $b, c \in K \backslash \{0\}$, что

$$\begin{cases} a_{11} = cb^2 \\ a_1 = 2cb \end{cases}, \tag{2.11}$$

то коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что

$$(w_0, u_0) = (bx_0 + 1, y_0)$$

является корнем уравнения

$$cw^2 + a_2 u + (a_0 - c) = 0 \tag{2.12}$$

над кольцом $\mathcal{K}$.

Доказательство теоремы 2.2 аналогично доказательству теоремы 1.1.

5. Пусть

$$\begin{cases} a_{11} = a_{22} = 0 \\ a_{12} \neq 0 \end{cases}.$$

Истинна следующая теорема.

Теорема 2.3. Пусть $a_{11} = a_{22} = 0$ и $a_{12} \neq 0$. Тогда:

1) если $a_1 = a_2 = 0$, то коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что (x_0, y_0) – корень уравнения

$$a_{12}xy + a_0 = 0 \tag{2.13}$$

над кольцом $\mathcal{K}$;

2) если $a_2 \neq 0$ и существует такой элемент $c \in K \backslash \{0\}$, что $a_2 = ca_{12}$, то коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что

$$(u_0, v_0) = (a_{12}y_0 + a_1, x_0 + c)$$

является корнем уравнения

$$uv + (a_0 - ca_1) = 0 \tag{2.14}$$

над кольцом $\mathcal{K}$;

3) если $a_1 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_1 = ca_{12}$, то коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что

$$(u_0, v_0) = (a_{12}x_0 + a_2, y_0 + c)$$

является корнем уравнения

$$uv + (a_0 - ca_2) = 0 \tag{2.15}$$

над кольцом $\mathcal{K}$.

Доказательство. Пусть $a_{11} = a_{22} = 0$ и $a_{12} \neq 0$. Тогда уравнение (2.1) принимает вид

$$a_{12}xy + a_1x + a_2y + a_0 = 0. \tag{2.16}$$

Следовательно, коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что (x_0, y_0) – корень уравнения (2.16) над кольцом $\mathcal{K}$.

Если $a_1 = a_2 = 0$, то уравнение (2.16) совпадает с уравнением (2.13).

Отсюда вытекает, что коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что (x_0, y_0) – корень уравнения (2.13) над кольцом $\mathcal{K}$, что и требовалось показать.

Пусть $a_2 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_2 = ca_{12}$. Тогда

$$a_{12}xy + a_1x + a_2y + a_0 = x(a_{12}y + a_1) + ca_{12}y + a_0 =$$

$$= x(a_{12}y + a_1) + c(a_{12}y + a_1) + (a_0 - ca_1) =$$

$$= (a_{12}y + a_1)(x + c) + (a_0 - ca_1).$$

Следовательно, уравнение (2.16) принимает вид

$$(a_{12}y + a_1)(x + c) + (a_0 - ca_1) = 0. \tag{2.17}$$

Положив в (2.17)

$$\begin{cases} u = a_{12}y + a_1 \\ v = x + c \end{cases},$$

получим уравнение (2.14).

Отсюда вытекает, что коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что

$$(u_0, v_0) = (a_{12}y_0 + a_1, x_0 + c)$$

является корнем уравнения (2.14) над кольцом $\mathcal{K}$, что и требовалось показать.

Пусть $a_1 \neq 0$ и существует такой элемент $c \in K\backslash\{0\}$, что $a_1 = ca_{12}$. Тогда

$$a_{12}xy + a_1x + a_2y + a_0 = y(a_{12}x + a_2) + ca_{12}x + a_0 =$$

$$= y(a_{12}x + a_2) + c(a_{12}x + a_2) + (a_0 - ca_2) =$$

$$= (a_{12}x + a_2)(y + c) + (a_0 - ca_2).$$

Следовательно, уравнение (2.16) принимает вид

$$(a_{12}x + a_2)(y + c) + (a_0 - ca_2) = 0. \tag{2.18}$$

Положив в (2.18)

$$\begin{cases} u = a_{12}x + a_2 \\ v = y + c \end{cases},$$

получим уравнение (2.15).

Отсюда вытекает, что коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что

$$(u_0, v_0) = (a_{12}x_0 + a_2, y_0 + c)$$

является корнем уравнения (2.15) над кольцом $\mathcal{K}$, что и требовалось показать.

□

6. Пусть

$$\begin{cases} a_{ii} \neq 0 \ (i = 1, 2) \\ a_j \neq 0 \ (j = 1, 2) \end{cases}.$$

Истинна следующая теорема.

Теорема 2.4. Пусть характеристика кольца $\mathcal{K}$ отлична от 2. Если $a_{ii} \neq 0 \ (i = 1, 2)$, $a_j \neq 0 \ (j = 1, 2)$ и существуют такие элементы $b_1, b_2, c, d \in K \backslash \{0\}$, что

$$\begin{cases} a_{11} = cb_1^2 \\ a_{12} = 2cb_1b_2 \\ a_{22} = cb_2^2 \\ a_1 = db_1 \\ a_2 = db_2 \end{cases}, \tag{2.19}$$

то коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что

$$w_0 = b_1x_0 + b_2y_0$$

является корнем уравнения

$$cw^2 + dw + a_0 = 0 \tag{2.20}$$

над кольцом $\mathcal{K}$.

Доказательство. Пусть характеристика кольца $\mathcal{K}$ отлична от 2, $a_{ii} \neq 0 \ (i = 1, 2)$ и $a_j \neq 0 \ (j = 1, 2)$.

Подставив (2.19) в (2.1), получим

$$a_{11}x^2 + a_{12}xy + a_{22}y^2 + a_1x + a_2y + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow cb_1^2x^2 + 2cb_1b_2xy + cb_2^2y^2 + db_1x + db_2y + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow c(b_1^2x^2 + 2b_1b_2xy + b_2^2y^2) + d(b_1x + b_2y) + a_0 = 0 \Leftrightarrow$$

$$\Leftrightarrow c(b_1x + b_2y)^2 + d(b_1x + b_2y) + a_0 = 0. \tag{2.21}$$

Положив в (2.21)

$$w = b_1 x + b_2 y,$$

получим уравнение (2.20).

Отсюда вытекает, что коника Γ, определяемая уравнением (2.1), состоит из всех таких точек $(x_0, y_0) \in K^2$, что

$$w_0 = b_1 x_0 + b_2 y_0$$

является корнем уравнения (2.20) над кольцом $\mathcal{K}$.

□

2.1.4. Канонический вид коник над кольцом.

Построим канонические формы коник над кольцом $\mathcal{K}$.

Рассмотрим линейное преобразование

$$\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} u \\ v \end{pmatrix}, \tag{2.22}$$

где

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}. \tag{2.23}$$

Подставив (2.23) в (2.22) и выполнив действия, получим

$$\begin{cases} x = \alpha_{11} u + \alpha_{12} v \\ y = \alpha_{21} u + \alpha_{22} v \end{cases}. \tag{2.24}$$

Будем говорить,что линейная форма

$$h(x, y) = a_1 x + a_2 y$$

аннулируется в результате применения линейного преобразования (2.24) тогда и только тогда, когда

$$h(\alpha_{11} u + \alpha_{12} v, \alpha_{21} u + \alpha_{22} v) = 0u + 0v.$$

Лемма 2.1. Над кольцом $\mathcal{K}$ линейная форма

$$h(x, y) = a_1 x + a_2 y \tag{2.25}$$

аннулируется в результате применения линейного преобразования (2.24) тогда и только тогда, когда истинны равенства

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \end{cases} . \tag{2.26}$$

Доказательство. Подставив (2.24) в (2.25), получим

$$h(\alpha_{11}u + \alpha_{12}v, \alpha_{21}u + \alpha_{22}v) =$$

$$= a_1(\alpha_{11}u + \alpha_{12}v) + a_2(\alpha_{21}u + \alpha_{22}v) =$$

$$= (a_1\alpha_{11} + a_2\alpha_{21})u + (a_1\alpha_{12} + a_2\alpha_{22})v. \tag{2.27}$$

Из (2.27) вытекает, что равенство

$$h(\alpha_{11}u + \alpha_{12}v, \alpha_{21}u + \alpha_{22}v) = 0u + 0v$$

истинно тогда и только тогда, когда истинны равенства (2.26).

□

Следствие 2.1. Если $a_1 \in K^{inv}$ или $a_2 \in K^{inv}$, то любое линейное преобразование (2.24), аннулирующее линейную форму (2.25), является необратимым линейным преобразованием над кольцом $\mathcal{K}$.

Доказательство. Предположим, что линейное преобразование (2.24) аннулирует линейную форму (2.25).

Пусть $a_1 \in K^{inv}$. Тогда

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \end{cases} \Leftrightarrow \begin{cases} \alpha_{11} = -a_1^{-1}a_2\alpha_{21} \\ \alpha_{12} = -a_1^{-1}a_2\alpha_{22} \end{cases} .$$

Следовательно,

$$\det(A) = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} =$$

$$= -a_1^{-1}a_2\alpha_{21}\alpha_{22} + a_1^{-1}a_2\alpha_{22}\alpha_{21} = 0,$$

откуда вытекает, что линейное преобразование (2.24), аннулирующее линейную форму (2.25), является необратимым линейным преобразованием над кольцом $\mathcal{K}$.

В случае, когда $a_2 \in K^{inv}$, доказательство осуществляется аналогичным образом.

□

Выясним, к какому виду в результате применения линейного преобразования (2.24) над кольцом $\mathcal{K}$ может быть приведена квадратичная форма

$$f(x, y) = a_{11}x^2 + a_{12}xy + a_{22}y^2, \tag{2.28}$$

где $a_{11}, a_{12}, a_{22} \in K$ $((a_{11}, a_{12}, a_{22}) \neq (0, 0, 0))$.

Теорема 2.5. Над кольцом $\mathcal{K}$ квадратичная форма (2.28) в результате применения линейного преобразования (2.24) может быть приведена к виду

$$g(u, v) = b_{11}u^2 + b_{22}v^2 \tag{2.29}$$

тогда и только тогда, когда

$$2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0. \tag{2.30}$$

При этом, коэффициенты b_{11} и b_{22} определяются равенствами

$$b_{11} = a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2, \tag{2.31}$$

$$b_{22} = a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2. \tag{2.32}$$

Доказательство. Применив линейное преобразование (2.24) к квадратичной форме (2.28), получим

$$g(u, v) = f(\alpha_{11}u + \alpha_{12}v, \alpha_{21}u + \alpha_{22}v) =$$

$$= a_{11}(\alpha_{11}^2u^2 + 2\alpha_{11}\alpha_{12}uv + \alpha_{12}^2v^2) +$$

$$+a_{12}(\alpha_{11}\alpha_{21}u^2 + (\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21})uv + \alpha_{12}\alpha_{22}v^2) +$$

$$+a_{22}(\alpha_{21}^2u^2+2\alpha_{21}\alpha_{22}uv+\alpha_{22}^2v^2)=$$

$$=(a_{11}\alpha_{11}^2+a_{12}\alpha_{11}\alpha_{21}+a_{22}\alpha_{21}^2)u^2+$$

$$+(2(a_{11}\alpha_{11}\alpha_{12}+a_{22}\alpha_{21}\alpha_{22})+a_{12}(\alpha_{11}\alpha_{22}+\alpha_{12}\alpha_{21}))uv+$$

$$+(a_{11}\alpha_{12}^2+a_{12}\alpha_{12}\alpha_{22}+a_{22}\alpha_{22}^2)v^2. \tag{2.33}$$

Из (2.33) вытекает, что истинность равенства (2.30) является необходимым и достаточным условием приведения квадратичной формы (2.28) к виду (2.29).

При этом, коэффициенты b_{11} и b_{22} определяются, соответственно, равенством (2.31) и (2.32).

□

Из теоремы 2.5 непосредственно вытекает, что истинны следующие три следствия.

Следствие 2.2. Над кольцом $\mathcal{K}$ квадратичная форма (2.28) в результате применения линейного преобразования (2.24) может быть приведена к виду

$$g(u,v)=b_{11}u^2 \tag{2.34}$$

тогда и только тогда, когда

$$\begin{cases}2(a_{11}\alpha_{11}\alpha_{12}+a_{22}\alpha_{21}\alpha_{22})+a_{12}(\alpha_{11}\alpha_{22}+\alpha_{12}\alpha_{21})=0\\ a_{11}\alpha_{12}^2+a_{12}\alpha_{12}\alpha_{22}+a_{22}\alpha_{22}^2=0\end{cases}. \tag{2.35}$$

При этом, коэффициент b_{11} определяется равенством (2.31).

Следствие 2.3. Над кольцом $\mathcal{K}$ квадратичная форма (2.28) в результате применения линейного преобразования (2.24) может быть приведена к виду

$$g(u,v)=b_{22}v^2 \tag{2.36}$$

тогда и только тогда, когда

$$\begin{cases} 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0 \end{cases} . \tag{2.37}$$

При этом, коэффициент b_{22} определяется равенством (2.32).

Следствие 2.4. Над кольцом $\mathcal{K}$ квадратичная форма (2.28) в результате применения линейного преобразования (2.24) может быть приведена к виду

$$g(u, v) = b_{12}uv \tag{2.38}$$

тогда и только тогда, когда

$$\begin{cases} a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0 \end{cases} . \tag{2.39}$$

При этом, коэффициент b_{22} определяется равенством

$$b_{12} = 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}). \tag{2.40}$$

Замечание 2.2. Некоторые из установленных выше равенств упрощаются в случае, когда характеристика кольца $\mathcal{K}$ равна 2. Действительно, равенство (2.30) принимает вид

$$a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0, \tag{2.41}$$

а равенство (2.40) – вид

$$b_{12} = a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}). \tag{2.42}$$

Из леммы 2.1, теоремы 2.5 и следствий 2.2-2.4 вытекают следующие достаточные условия приведения к каноническому виду коники Γ, определяемой над кольцом $\mathcal{K}$ уравнением (2.1), в результате применения линейного преобразования (2.24).

Коника Γ, определяемая уравнением (2.1) над кольцом $\mathcal{K}$, применением линейного преобразования (2.24):

1) может быть приведена к виду

$$b_{11}u^2 + b_{22}v^2 + a_0 = 0, \tag{2.43}$$

если

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \end{cases}; \tag{2.44}$$

2) может быть приведена к виду

$$b_{11}u^2 + a_0 = 0, \tag{2.45}$$

если

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0 \end{cases}; \tag{2.46}$$

3) может быть приведена к виду

$$b_{22}v^2 + a_0 = 0, \tag{2.47}$$

если

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ 2(a_{11}\alpha_{11}\alpha_{12} + a_{22}\alpha_{21}\alpha_{22}) + a_{12}(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) = 0 \\ a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0 \end{cases}; \tag{2.48}$$

4) может быть приведена к виду

$$b_{12}uv + a_0 = 0, \tag{2.49}$$

если

$$\begin{cases} a_1\alpha_{11} + a_2\alpha_{21} = 0 \\ a_1\alpha_{12} + a_2\alpha_{22} = 0 \\ a_{11}\alpha_{11}^2 + a_{12}\alpha_{11}\alpha_{21} + a_{22}\alpha_{21}^2 = 0 \\ a_{11}\alpha_{12}^2 + a_{12}\alpha_{12}\alpha_{22} + a_{22}\alpha_{22}^2 = 0 \end{cases}. \tag{2.50}$$

Таким образом, системы нелинейных уравнений (2.44), (2.46), (2.48) и (2.50) могут быть использованы для поиска линейного преобразования,

осуществляющего приведение коники Γ, определяемой уравнением (2.1) над кольцом $\mathcal{K}$, соответственно, к виду (2.43), (2.45), (2.47) или (2.49).

Линейное преобразование (2.22) является биекцией множества K^2 на себя тогда и только тогда, когда 2×2-матрица (2.23) обратима над кольцом $\mathcal{K}$.

Последнее имеет место тогда и только тогда, когда

$$\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \in K^{inv}. \tag{2.51}$$

Теорема 2.6. Если характеристика кольца $\mathcal{K}$ равна 2, а $a_{12} \in K^{inv}$, то никаким обратимым линейным преобразованием (2.22) квадратичная форма (2.28) не может быть приведена ни к виду (2.34), ни к виду (2.36).

Доказательство. Предположим, что характеристика кольца $\mathcal{K}$ равна 2, $a_{12} \in K^{inv}$ и существует обратимое линейное преобразование (2.22), приводящее квадратичную форму (2.28) к виду (2.34) или (2.36).

Тогда истинно равенство (2.41).

Так как $a_{12} \in K^{inv}$, то равенство (2.41) эквивалентно равенству

$$\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21} = 0. \tag{2.52}$$

А так как 2×2-матрица (2.23) обратима над кольцом $\mathcal{K}$, то истинно условие (2.51).

Из (2.51) и (2.52) вытекает, что

$$2\alpha_{11}\alpha_{22} \in K^{inv} \Leftrightarrow 0 \in K^{inv}.$$

Полученное противоречие показывает, что предположение – ложное.

Отсюда и вытекает, что если характеристика кольца $\mathcal{K}$ равна 2, а $a_{12} \in K^{inv}$, то никаким обратимым линейным преобразованием (2.22) квадратичная форма (2.28) не может быть приведена ни к виду (2.34), ни к виду (2.36).

□

2.2. Кубики над кольцами.

Рассмотрим над кольцом $\mathcal{K} = (K, +, \cdot)$ кубику Γ, определяемую уравнением

$$ay^2 = b_3x^3 + b_2x^2 + b_1x + b_0, \tag{2.53}$$

где $a, b_3 \in K\backslash\{0\}$ и $b_2, b_1, b_0 \in K$.

2.2.1. Типы кубик над кольцом.

Для многочлена

$$f(x) = b_3x^3 + b_2x^2 + b_1x + b_0,$$

являющегося правой частью равенства (2.53) возможны следующие три ситуации.

Ситуация 2.4. Многочлен $f(x)$ неразложим над кольцом $\mathcal{K}$.

Ситуация 2.5. Для любых многочленов $f_i \in \mathcal{K}[x]$ $(i = 1, 2)$ степени $m_i \geq 1$ $(i = 1, 2)$, удовлетворяющих равенству

$$f(x) = f_1(x)f_2(x),$$

истинно неравенство $m_1 + m_2 > 3$.

Ситуация 2.6. Существуют многочлены $f_i \in \mathcal{K}[x]$ $(i = 1, 2)$ степени $m_i \geq 1$ $(i = 1, 2)$, удовлетворяющие равенству

$$f(x) = f_1(x)f_2(x),$$

для которых $m_1 + m_2 = 3$.

Если имеет место ситуация 2.5, то $f(x)$ – многочлен наименьшей степени, определяющий кубику Γ.

Поэтому, в ситуациях 2.4 и 2.5 анализ кубики Γ осуществляется на анализе уравнения (2.53).

Пусть имеет место ситуация 2.6. Тогда либо

$$f(x) = (\alpha_2x^2 + \alpha_1x + \alpha_0)(\beta_1x + \beta_0),$$

где $\alpha_2, \alpha_1, \alpha_0, \beta_1, \beta_0 \in K$, причем

$$\alpha_2\beta_1 \neq 0$$

либо

$$f(x) = (\gamma_1x + \delta_1)(\gamma_2x + \delta_2)(\gamma_3x + \delta_3),$$

где $\gamma_i, \delta_i \in K$ $(i = 1, 2, 3)$, причем

$$\gamma_1\gamma_2\gamma_3 \neq 0.$$

Следовательно, уравнение (2.53) принимает либо вид

$$ay^2 = (\alpha_2x^2 + \alpha_1x + \alpha_0)(\beta_1x + \beta_0), \tag{2.54}$$

либо вид

$$ay^2 = (\gamma_1 x + \delta_1)(\gamma_2 x + \delta_2)(\gamma_3 x + \delta_3). \qquad (2.55)$$

Положим

$$S_a = \{ay^2 | y \in K\},$$

$$S_a^{(2)} = \{(\mu_1, \mu_2) \in K^2 | \mu_1\mu_2 \in S_a\},$$

$$S_a^{(3)} = \{(\nu_1, \nu_2, \nu_3) \in K^3 | \nu_1\nu_2\nu_3 \in S_a\}.$$

Если кубика Γ определена уравнением (2.54), то множество ее точек представляет собой объединение множеств решений двухпараметрического семейства F_{μ_1,μ_2} ($(\mu_1, \mu_2) \in S_a^{(2)}$) систем нелинейных уравнений

$$F_{\mu_1,\mu_2} : \begin{cases} ay^2 = \mu_1\mu_2 \\ \alpha_2 x^2 + \alpha_1 x + \alpha_0 = \mu_1 \\ \beta_1 x + \beta_0 = \mu_2 \end{cases} .$$

Пусть кубика Γ определена уравнением (2.55). Тогда множество ее точек представляет собой объединение множеств решений трехпараметрического семейства G_{ν_1,ν_2,ν_3} ($(\nu_1, \nu_2, \nu_3) \in S_a^{(3)}$) систем нелинейных уравнений

$$G_{\nu_1,\nu_2,\nu_3} : \begin{cases} ay^2 = \nu_1\nu_2\nu_3 \\ \gamma_1 x + \delta_1 = \nu_1 \\ \gamma_2 x + \delta_2 = \nu_2 \\ \gamma_3 x + \delta_3 = \nu_3 \end{cases} .$$

Замечание 2.3. Таким образом, в случае конечного кольца построение в явном виде множества точек кубики Γ в ситуациях 2.4 и 2.5 эквивалентно поиску множества решений нелинейного уравнения (2.53) от двух переменных, а в ситуации 2.6 – поиску множества решений двухпараметрического семейства F_{μ_1,μ_2} ($(\mu_1, \mu_2) \in S_a^{(2)}$) или трехпараметрического семейства G_{ν_1,ν_2,ν_3} ($(\nu_1, \nu_2, \nu_3) \in S_a^{(3)}$) систем нелинейных уравнений.

В ситуации 2.6 построение в явном виде множества точек кубики Γ включает в себя необходимость построения в явном виде всех факторизаций всех элементов множества S_a на два, либо на три сомножителя.

Отметим, что наилучший из алгоритмов факторизации для конечных колец имеет субэкспоненциальную сложность.

2.2.2. Особые точки кубик над кольцом.

Охарактеризуем особые точки кубики (2.53).

Из определения особой точки кривой вытекает, что множеством особых точек кубики (2.53) является множество решений системы уравнений

$$\begin{cases} \mathsf{D}_x(b_3x^3+b_2x^2+b_1x+b_0-ay^2)=0 \\ \mathsf{D}_x(ay^2-b_3x^3-b_2x^2-b_1x-b_0)=0 \\ ay^2=b_3x^3+b_2x^2+b_1x+b_0 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 3b_3x^2+2b_2x+b_1=0 \\ 2ay=0 \\ ay^2=b_3x^3+b_2x^2+b_1x+b_0 \end{cases}.$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 2.3. Кубика Г, определяемая уравнением (2.53) имеет особые точки тогда и только тогда, когда существует такое решение (x_0, y_0) системы уравнений

$$\begin{cases} 3b_3x^2+2b_2x+b_1=0 \\ 2ay=0 \end{cases}, \tag{2.56}$$

что истинно равенство

$$ay_0^2=b_3x_0^3+b_2x_0^2+b_1x_0+b_0.$$

Пусть характеристика кольца $\mathcal{K}$ равна 2. Тогда система уравнений (2.56) принимает вид

$$\begin{cases} b_3x^2+b_1=0 \\ y\in K \end{cases}. \tag{2.57}$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 2.4. Пусть характеристика кольца $\mathcal{K}$ равна 2. Тогда:

1) кубика Г, определяемая уравнением (2.53), является гладкой кривой, если над кольцом $\mathcal{K}$ уравнение

$$b_3x^2+b_1=0$$

не имеет решений;

2) если $b_3 \in K^{inv}$, то множеством особых точек кубики Γ, определяемой уравнением (2.53), является множество решений системы нелинейных уравнений

$$\begin{cases} x^2 = b_3^{-1} b_1 \\ ay^2 = b_0 + b_1 b_2 b_3^{-1} \end{cases}$$

над кольцом $\mathcal{K}$;

3) если $b_3 \in K \backslash K^{inv}$, то множеством особых точек кубики Γ, определяемой уравнением (2.53), является множество решений системы нелинейных уравнений

$$\begin{cases} b_3 x^2 = b_1 \\ ay^2 = b_2 x^2 + b_0 \end{cases}$$

над кольцом $\mathcal{K}$.

Пусть характеристика кольца $\mathcal{K}$ равна 3. Тогда система уравнений (2.56) принимает вид

$$\begin{cases} b_2 x = b_1 \\ ay = 0 \end{cases} . \tag{2.58}$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 2.5. Пусть характеристика кольца $\mathcal{K}$ равна 3. Тогда:

1) кубика Γ, определяемая уравнением (2.53), является гладкой кривой, если над кольцом $\mathcal{K}$ уравнение

$$b_3 x^3 + 2 b_1 x + b_0 = 0$$

не имеет решений;

2) если $b_2 \in K^{inv}$ и

$$b_1^3 b_2^{-3} b_3 - b_1^2 b_2^{-1} + b_0 = 0,$$

то множеством особых точек кубики Γ, определяемой уравнением (2.53), является множество

$$\{(b_1 b_2^{-1}, y) | ay = 0\};$$

3) если $b_2 \in K \backslash K^{inv}$, то множеством особых точек кубики Γ, определяемой уравнением (2.53), является множество решений системы нелинейных уравнений

$$\begin{cases} b_2 x = b_1 \\ b_3 x^3 - b_1 x + b_0 = 0 \\ ay = 0 \end{cases}$$

над кольцом $\mathcal{K}$.

2.2.3. Кратные корни кубического многочлена над кольцом.

Найдем условия, при которых многочлен, являющийся правой частью уравнения (2.53), имеет кратный корень, т.е. когда имеет место разложение

$$b_3 x^3 + b_2 x^2 + b_1 x + b_0 = (x - \alpha)^2 (b_3 x + \beta) \tag{2.59}$$

или разложение

$$b_3 x^3 + b_2 x^2 + b_1 x + b_0 = b_3 (x - \alpha)^3. \tag{2.60}$$

Пусть характеристика кольца $\mathcal{K}$ равна 2. Тогда:

1) равенство (2.59) истинно тогда и только тогда, когда

$$\begin{cases} \beta = b_2 \\ \alpha^2 b_3 = b_1 \\ \alpha^2 \beta = b_0 \end{cases};$$

2) равенство (2.60) истинно тогда и только тогда, когда

$$\begin{cases} \alpha b_3 = b_2 \\ \alpha^2 b_3 = b_1 \\ \alpha^3 b_3 = b_0 \end{cases}.$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 2.6. Если характеристика кольца $\mathcal{K}$ равна 2, то:

1) существование разложения (2.59) эквивалентно существованию решения α системы нелинейных уравнений

$$\begin{cases} b_3 \alpha^2 = b_1 \\ b_2 \alpha^2 = b_0 \end{cases};$$

2) существование разложения (2.60) эквивалентно существованию решения α системы линейных уравнений

$$\begin{cases} b_3\alpha = b_2 \\ b_2\alpha = b_1 \\ b_1\alpha = b_0 \end{cases}.$$

Пусть характеристика кольца $\mathcal{K}$ равна 3. Тогда:

1) равенство (2.59) истинно тогда и только тогда, когда

$$\begin{cases} \alpha b_3 + \beta = b_2 \\ \alpha^2 b_3 + \alpha\beta = b_1 \\ \alpha^2\beta = b_0 \end{cases};$$

2) равенство (2.60) истинно тогда и только тогда, когда

$$\begin{cases} b_2 = 0 \\ b_1 = 0 \\ \alpha^3 b_3 = -b_0 \end{cases}.$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 2.7. Если характеристика кольца $\mathcal{K}$ равна 3, то:

1) существование разложения (2.59) эквивалентно существованию решения (α, β) системы нелинейных уравнений

$$\begin{cases} \alpha b_3 + \beta = b_2 \\ \alpha b_2 = b_1 \\ \alpha^2\beta = b_0 \end{cases};$$

2) существование разложения (2.60) эквивалентно условию

$$b_2 = b_1 = 0$$

и существованию решения α нелинейного уравнения

$$b_3\alpha^3 = -b_0.$$

Для кольца (в отличие от поля) равенство нулю результанта двух многочленов является только необходимым условием существования их

общего корня. Поэтому в случае, когда характеристика кольца $\mathcal{K}$ отлична от 2 и 3 с использованием понятия «результант двух многочленов» может быть установлено следующее необходиме условие существования разложений (2.59) и (2.60).

Теорема 2.7. Пусть характеристика кольца $\mathcal{K}$ отлична от 2 и 3. Тогда, если существует

1) разложение (2.59), то истинно равенство

$$b_3(4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2) = 0; \tag{2.61}$$

2) разложение (2.60), то истинны равенства

$$\begin{cases} b_3(4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2) = 0 \\ 12b_3(3b_1b_3 - b_2) = 0 \end{cases} . \tag{2.62}$$

Доказательство. Необходимым условием наличия кратного корня у многочлена над кольцом $\mathcal{K}$ является равенство нулю результанта этого многочлена и его производной.

Найдем производную многочлена $f(x)$:

$$\mathsf{D}f(x) = 3b_3x^2 + 2b_2x + b_1.$$

Вычислим результант многочленов $f(x)$ и $\mathsf{D}f(x)$.

$$\mathrm{Res}(f, \mathsf{D}f, x) = \det(\mathrm{Syl}(f, \mathsf{D}f, x)) =$$

$$= \begin{vmatrix} b_3 & 0 & 3b_3 & 0 & 0 \\ b_2 & b_3 & 2b_2 & 3b_3 & 0 \\ b_1 & b_2 & b_1 & 2b_2 & 3b_3 \\ b_0 & b_1 & 0 & b_1 & 2b_2 \\ 0 & b_0 & 0 & 0 & b_1 \end{vmatrix} =$$

$$= b_3 \begin{vmatrix} b_3 & 2b_2 & 3b_3 & 0 \\ b_2 & b_1 & 2b_2 & 3b_3 \\ b_1 & 0 & b_1 & 2b_2 \\ b_0 & 0 & 0 & b_1 \end{vmatrix} + 3b_3 \begin{vmatrix} b_2 & b_3 & 3b_3 & 0 \\ b_1 & b_2 & 2b_2 & 3b_3 \\ b_0 & b_1 & b_1 & 2b_2 \\ 0 & b_0 & 0 & b_1 \end{vmatrix} =$$

$$= b_3 \begin{vmatrix} -2b_3 & 2b_2 & 3b_3 & 0 \\ -b_2 & b_1 & 2b_2 & 3b_3 \\ 0 & 0 & b_1 & 2b_2 \\ b_0 & 0 & 0 & b_1 \end{vmatrix} + 3b_3 \begin{vmatrix} b_2 & -2b_3 & 3b_3 & 0 \\ b_1 & -b_2 & 2b_2 & 3b_3 \\ b_0 & 0 & b_1 & 2b_2 \\ 0 & b_0 & 0 & b_1 \end{vmatrix}. \qquad (2.63)$$

Вычислим по отдельности определители 4-го порядка.

$$\begin{vmatrix} -2b_3 & 2b_2 & 3b_3 & 0 \\ -b_2 & b_1 & 2b_2 & 3b_3 \\ 0 & 0 & b_1 & 2b_2 \\ b_0 & 0 & 0 & b_1 \end{vmatrix} = -b_0 \begin{vmatrix} 2b_2 & 3b_3 & 0 \\ b_1 & 2b_2 & 3b_3 \\ 0 & b_1 & 2b_2 \end{vmatrix} + b_1 \begin{vmatrix} -2b_3 & 2b_2 & 3b_3 \\ -b_2 & b_1 & 2b_2 \\ 0 & 0 & b_1 \end{vmatrix} =$$

$$= -b_0(8b_2^3 - 12b_1b_2b_3) + b_1^2(-2b_1b_3 + 2b_2^2) =$$

$$= -8b_0b_2^3 + 12b_0b_1b_2b_3 - 2b_1^3b_3 + 2b_1^2b_2^2, \qquad (2.64)$$

$$\begin{vmatrix} b_2 & -2b_3 & 3b_3 & 0 \\ b_1 & -b_2 & 2b_2 & 3b_3 \\ b_0 & 0 & b_1 & 2b_2 \\ 0 & b_0 & 0 & b_1 \end{vmatrix} = b_0 \begin{vmatrix} b_2 & 3b_3 & 0 \\ b_1 & 2b_2 & 3b_3 \\ b_0 & b_1 & 2b_2 \end{vmatrix} + b_1 \begin{vmatrix} b_2 & -2b_3 & 3b_3 \\ b_1 & -b_2 & 2b_2 \\ b_0 & 0 & b_1 \end{vmatrix} =$$

$$= b_0(4b_2^3 + 9b_0b_3^2 - 9b_1b_2b_3) + b_1(-b_1b_2^2 - b_0b_2b_3 + 2b_1^2b_3) =$$

$$= 4b_0b_2^3 + 9b_0^2b_3^2 - 10b_0b_1b_2b_3 - b_1^2b_2^2 + 2b_1^3b_3. \qquad (2.65)$$

Подставив (2.64) и (2.65) в (2.63), получим

$$\mathrm{Res}(f, \mathsf{D}f, x) = b_3(-8b_0b_2^3 + 12b_0b_1b_2b_3 - 2b_1^3b_3 + 2b_1^2b_2^2) +$$

$$+3b_3(4b_0b_2^3 + 9b_0^2b_3^2 - 10b_0b_1b_2b_3 - b_1^2b_2^2 + 2b_1^3b_3) =$$

$$= b_3(-8b_0b_2^3 + 12b_0b_1b_2b_3 - 2b_1^3b_3 + 2b_1^2b_2^2 +$$

$$+12b_0b_2^3 + 27b_0^2b_3^2 - 30b_0b_1b_2b_3 - 3b_1^2b_2^2 + 6b_1^3b_3) =$$

$$= b_3(4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2). \qquad (2.66)$$

Из (2.66) вытекает, что если существует разложение (2.59), то истинно равенство (2.60), что и требовалось показать.

Найдем производную многочлена $\mathsf{D}f(x)$:

$$\mathsf{D}^2 f(x) = 6b_3x + 2b_2.$$

Вычислим результант многочленов $\mathsf{D}f(x)$ и $\mathsf{D}^2 f(x)$.

$$\mathrm{Res}(\mathsf{D}f, \mathsf{D}^2 f, x) = \det(\mathrm{Syl}(\mathsf{D}f, \mathsf{D}^2 f, x)) =$$

$$= \begin{vmatrix} 3b_3 & 6b_3 & 0 \\ 2b_2 & 2b_2 & 6b_3 \\ b_1 & 0 & 2b_2 \end{vmatrix} = \begin{vmatrix} -3b_3 & 6b_3 & 0 \\ 0 & 2b_2 & 6b_3 \\ b_1 & 0 & 2b_2 \end{vmatrix} = 12b_3(3b_1b_3 - b_2). \qquad (2.67)$$

Из (2.66) и (2.67) вытекает, что если существует разложение (2.60), то истинны равенства (2.61), что и требовалось показать.

□

Замечание 2.4. Пусть характеристика кольца $\mathcal{K}$ равна 4. Из (2.67) вытекает, что

$$\mathrm{Res}(\mathsf{D}f, \mathsf{D}^2 f, x) \equiv 0,$$

т.е. необходимое условие существования разложения (2.60), устанавливаемое равенствами (2.62), становится тривиальным для кольца характеристики 4.

Из (1.4) и (2.66) вытекает, что

$$b_3\mathrm{disc}(f) = -b_3(4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2). \qquad (2.68)$$

Следовательно, если либо $b_3 \in K^{inv}$, либо $\mathcal{K}$ – гауссово кольцо, то

$$\mathrm{disc}(f) = -(4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2). \qquad (2.69)$$

Из (2.68) непосредственно вытекает, что истинно утверждение.

Утверждение 2.8. Пусть либо $b_3 \in K^{inv}$, либо $\mathcal{K}$ – гауссово кольцо. Тогда достаточное условие отсутствия для многочлена

$$f(x) = b_3x^3 + b_2x^2 + b_1x + b_0,$$

разложения (2.59) имеет вид

$$4b_0b_2^3 + 27b_0^2b_3^2 - 18b_0b_1b_2b_3 + 4b_1^3b_3 - b_1^2b_2^2 \neq 0. \tag{2.70}$$

2.3. Эллиптические кривые над полями.

В настоящем пункте предполагается, что кольцо $\mathcal{K} = (K, +, \cdot)$ является полем.

2.3.1. Основные понятия.

Уравнением Вейерштрасса для кубики Γ над полем $\mathcal{K}$ называется уравнение вида

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.71}$$

где $a_1, a_2, a_3, a_4, a_6 \in K$.

Замечание 2.5. Если в уравнении (2.71) положить

$$a_1 = a_3 = 0,$$

то получим специальный случай уравнения (2.53), исследованного в п.2.2 в предположении, что $\mathcal{K}$ – кольцо.

Множеством особых точек кубики Γ, определенной уравнением (2.71), является множество решений системы уравнений

$$\begin{cases} \mathsf{D}_x(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6) = 0 \\ \mathsf{D}_y(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6) = 0 \\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} a_1y - 3x^2 - 2a_2x - a_4 = 0 \\ 2y + a_1x + a_3 = 0 \\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \end{cases}.$$

Таким образом, кубика Γ, определенная уравнением (2.71), является гладкой кривой, если

$$a_1 y - 3x^2 - 2a_2 x - a_4 \neq 0 \tag{2.72}$$

или

$$2y + a_1 x + a_3 \neq 0 \tag{2.73}$$

для всех $(x, y) \in \Gamma$.

Уравнение (2.71) может рассматриваться над любым расширением $\widetilde{\mathcal{K}} = (\widetilde{K}, +, \cdot)$ поля $\mathcal{K}$.

Чтобы подчеркнуть, что кубика Γ рассматривается над полем $\widetilde{\mathcal{K}}$, используют запись $\Gamma/\widetilde{\mathcal{K}}$ (вместо $\Gamma/\mathcal{K}$, как правило, пишут Γ).

Упорядоченные пары $(x, y) \in \widetilde{K}^2$, являющиеся решениями уравнения (2.71) в поле $\widetilde{\mathcal{K}}$, называются *$\widetilde{\mathcal{K}}$-рациональными точками* кубики Γ.

Множество всех точек кубики Γ над расширением $\widetilde{\mathcal{K}}$ обозначается через $\Gamma(\widetilde{\mathcal{K}})$ (вместо $\Gamma(\mathcal{K})$, как правило, пишут Γ).

Кубика Γ, определенная уравнением (2.71), является *эллиптической кривой*, если ни для одного расширения $\widetilde{\mathcal{K}}$ поля $\mathcal{K}$ кубика $\Gamma/\widetilde{\mathcal{K}}$ не содержит особых точек, т.е. для любой точки $(x, y) \in \Gamma(\widetilde{\mathcal{K}})$ истинно (2.72) или (2.73).

Критерий того, что кубика Γ, определенная уравнением (2.71), является эллиптической кривой состоит в том, что отличен от нуля ее дискриминант Δ_Γ. Последний определяется формулой

$$\Delta_\Gamma = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6, \tag{2.74}$$

где

$$\begin{cases} d_2 = a_1^2 + 4a_2 \\ d_4 = 2a_4 + a_1 a_3 \\ d_6 = a_3^2 + 4a_6 \\ d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \end{cases} . \tag{2.75}$$

Замечание 2.6. Обоснование формул (2.74), (2.75) и конструкций, рассмотренных в настоящем пункте, дано в п.2.4.3.

Эллиптические кривые, определенные над полем $\mathcal{K}$ уравнениями

$$\Gamma_1 : \ y^2 + a_1^{(1)} xy + a_3^{(1)} y = x^3 + a_2^{(1)} x^2 + a_4^{(1)} x + a_6^{(1)},$$

$$\Gamma_2 : \ u^2 + a_1^{(2)} vu + a_3^{(2)} u = v^3 + a_2^{(2)} v^2 + a_4^{(2)} v + a_6^{(2)},$$

называются *изоморфными*, если существуют такие $\alpha, \beta, \gamma, \delta \in K$ $(\alpha \neq 0)$, что в результате преобразования

$$\begin{cases} x = \alpha^2 v + \beta \\ y = \alpha^3 u + \alpha^2 \gamma v + \delta \end{cases} \tag{2.76}$$

эллиптическая кривая Γ_1 отображается на эллиптическую кривую Γ_2.

Замечание 2.7. Отображение (2.76) является биекцией множества K^2 на себя. Обратное отображение имеет вид

$$\begin{cases} v = \alpha^{-2}(x - \beta) \\ u = \alpha^{-3}(y - \gamma x + \gamma\beta - \delta) \end{cases}.$$

Нетрудно убедиться в том, что отображение (2.76) определяет отношение эквивалентности на множестве всех эллиптических кривых как над полем $\mathcal{K}$, так и над любым расширением $\widetilde{\mathcal{K}}$ поля $\mathcal{K}$.

j-инвариантом эллиптической кривой Γ, определенной уравнением (2.71), называется элемент

$$j(\Gamma) = (d_2^2 - 24d_4)^3 \Delta_\Gamma^{-1} \tag{2.77}$$

поля $\mathcal{K}$, где дискриминант Δ_Γ определен формулой (2.74), а элементы d_2 и d_4 поля $\mathcal{K}$ – формулами (2.75).

Критерий изоморфизма двух эллиптических кривых состоит в равенстве их j-инвариантов, т.е. эллиптические кривые Γ_1 и Γ_2 изоморфны тогда и только тогда, когда $j(\Gamma_1) = j(\Gamma_2)$.

Замечание 2.8. Пусть $\mathcal{K} = (K, +, \cdot)$ – произвольное ассоциативно-коммутативное кольцо с единицей. Тогда формула (2.77) имеет смысл над кольцом $\mathcal{K}$ тогда и только тогда, когда $\Delta_\Gamma \in K^{inv}$.

Если $\Delta_\Gamma \notin K^{inv}$, но $\Delta_\Gamma \in S_\mathcal{K}$, то формула (2.77) имеет смысл над расширением $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ кольца $\mathcal{K}$.

Следовательно, для кривой Γ, определенной уравнением (2.71) над кольцом $\mathcal{K}$, в случае, когда $\Delta_\Gamma \in S_\mathcal{K}$ понятие «j-инвариант» имеет смысл при рассмотрении этой кривой в расширении $\overline{\mathcal{K}}$ кольца $\mathcal{K}$.

2.3.2. Стандартные формы эллиптических кривых.

Известно, что стандартные формы, к которым (в зависимости от характеристики поля $\mathcal{K}$) может быть приведено (в результате замены переменных) уравнение (2.71) эллиптической кривой Γ имеют следующий вид:

1. Если характеристика поля $\mathcal{K}$ равна 2, то уравнение (2.71) приводится либо к виду

$$y^2 + b_3 y = x^3 + b_4 x + b_6. \tag{2.78}$$

либо к виду

$$y^2 + xy = x^3 + b_2 x^2 + b_6, \tag{2.79}$$

2. Если характеристика поля $\mathcal{K}$ не равна 2, то уравнение (2.71) приводится к виду

$$y^2 = x^3 + b_2 x^2 + b_4 x + b_6, \tag{2.80}$$

причем если характеристика поля $\mathcal{K}$ больше, чем 3, то уравнение (2.71) приводится к виду

$$y^2 = x^3 + b_4 x + b_6. \tag{2.81}$$

Замечание 2.9. Эллиптические кривые над полем характеристики 2, заданные уравнением (2.78) называются *суперсингулярными*, а уравнением (2.79) – *несуперсингулярными*. Уравнение (2.81) для эллиптических кривых над полем характеристики большей, чем 3, называется *канонической формой Вейерштрасса*.

Приведение уравнения (2.71) к стандартной форме осуществляется следующим образом.

Пусть характеристика поля $\mathcal{K}$ равна 2. Возможны следующие два случая:

1. Пусть $a_1 = 0$. Тогда в результате обратимого преобразования

$$\begin{cases} x = v + a_2 \\ y = u \end{cases} \tag{2.82}$$

уравнение

$$y^2 + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{2.83}$$

преобразуется в эквивалентное уравнение

$$u^2 + b_3 u = v^3 + b_4 v + b_6, \tag{2.84}$$

где

$$\begin{cases} b_3 = a_3 \\ b_4 = a_2^2 + a_4 \\ b_6 = a_2 a_4 + a_6 \end{cases}.$$

Заменив в уравнении (2.84) v на x, а u на y, получим уравнение (2.78).

2. Пусть $a_1 \neq 0$. Тогда в результате обратимого преобразования

$$\begin{cases} x = a_1^2 v + a_1^{-1} a_3 \\ y = a_1^3 u \end{cases} \tag{2.85}$$

уравнение (2.71) преобразуется в эквивалентное уравнение

$$u^2 + vu = v^3 + c_2v^2 + c_4v + c_6, \tag{2.86}$$

где

$$\begin{cases} c_2 = a_1^{-3}(a_3 + a_1a_2) \\ c_4 = a_1^{-6}(a_3^2 + a_1^2a_4) \\ c_6 = a_1^{-6}(a_1^{-3}a_3^3 + a_1^{-2}a_2a_3^2 + a_1^{-1}a_3a_4 + a_6) \end{cases}.$$

В результате обратимого преобразования

$$\begin{cases} v = x \\ u = y + c_4 \end{cases} \tag{2.87}$$

уравнение (2.86) преобразуется в эквивалентное уравнение (2.79), где

$$\begin{cases} b_2 = c_2 \\ b_6 = c_6 + c_4^2 \end{cases}.$$

Пусть характеристика поля $\mathcal{K}$ не равна 2. Тогда в результате обратимого преобразования

$$\begin{cases} x = v \\ y = u - 2^{-1}a_1v - 2^{-1}a_3 \end{cases} \tag{2.88}$$

уравнение (2.71) преобразуется в эквивалентное уравнение

$$u^2 = v^3 + b_2v^2 + b_4v + b_6, \tag{2.89}$$

где

$$\begin{cases} b_2 = a_2 \\ b_4 = a_4 + 2^{-1}a_1a_3 \\ b_6 = a_6 - 2^{-2}a_3^2 \end{cases}.$$

Заменив в уравнении (2.89) v на x, а u на y, получим уравнение (2.80).

Если характеристика поля $\mathcal{K}$ больше, чем 3, то в результате применения к уравнению

$$u^2 = v^3 + c_2v^2 + c_4v + c_6, \tag{2.90}$$

обратимого преобразования

$$\begin{cases} v = x - 3^{-1}c_2 \\ u = y \end{cases} \tag{2.91}$$

уравнение (2.90) преобразуется в эквивалентное уравнение (2.81), где

$$\begin{cases} b_4 = 3^{-1}c_2 - 2 \cdot 3^{-1}c_2^2 + c_4 \\ b_6 = 3^{-3}c_2 + 3^{-2}c_2^3 - 3^{-1}c_2c_4 + c_6 \end{cases}.$$

Рассмотрим теперь возможность применения изложенной выше техники приведения уравнения эллиптической кривой к стандартной форме в случае, когда $\mathcal{K} = (K, +, \cdot)$ – произвольное ассоциативно-коммутативное кольцо с единицей.

Пусть $\mathcal{K}$ – ассоциативно-коммутативное кольцо с единицей, характеристика которого равна 2.

Преобразование (2.82) является обратимым преобразованием над кольцом $\mathcal{K}$.

Следовательно, над произвольным ассоциативно-коммутативным кольцом $\mathcal{K}$ с единицей, характеристика которого равна 2, уравнение (2.82) может быть приведено к стандартной форме (2.78).

Преобразование (2.87) является обратимым преобразованием над кольцом $\mathcal{K}$, а формула (2.85) имеет смысл над кольцом $\mathcal{K}$ тогда и только тогда, когда $a_1 \in K^{inv}$. При этом, при $a_1 \in K^{inv}$ преобразование (2.85) является обратимым преобразованием над кольцом $\mathcal{K}$.

Следовательно, над ассоциативно-коммутативным кольцом $\mathcal{K}$ с единицей, характеристика которого равна 2, уравнение (2.71) может быть приведено к стандартной форме (2.79), если $a_1 \in K^{inv}$.

Если $a_1 \notin K^{inv}$, но $a_1 \in S_{\mathcal{K}}$, то формула (2.85) имеет смысл (а определяемое ею преобразование становится обратимым) над расширением $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ кольца $\mathcal{K}$.

Следовательно, для ассоциативно-коммутативного кольца $\mathcal{K}$ с единицей, характеристика которого равна 2, уравнение (2.71) может быть приведено к стандартной форме (2.79) над расширением $\overline{\mathcal{K}}$ кольца $\mathcal{K}$, если $a_1 \in S_{\mathcal{K}}$.

Пусть $\mathcal{K}$ – ассоциативно-коммутативное кольцо с единицей, характеристика которого не равна 2.

Формула (2.88) имеет смысл над кольцом $\mathcal{K}$ тогда и только тогда, когда $2 \in K^{inv}$. При этом, при $2 \in K^{inv}$ преобразование (2.88) является обратимым преобразованием над кольцом $\mathcal{K}$.

Следовательно, над ассоциативно-коммутативным кольцом $\mathcal{K}$ с единицей, характеристика которого не равна 2, уравнение (2.71) может быть приведено к стандартной форме (2.80), если $2 \in K^{inv}$.

Если $2 \notin K^{inv}$, но $2 \in S_{\mathcal{K}}$, то формула (2.88) имеет смысл (а определяемое ею преобразование становится обратимым) над расширением $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ кольца $\mathcal{K}$.

Следовательно, для ассоциативно-коммутативного кольца $\mathcal{K}$ с единицей, характеристика которого не равна 2, уравнение (2.71) может быть приведено к стандартной форме (2.80) над расширением $\overline{\mathcal{K}}$ кольца $\mathcal{K}$, если $2 \in S_{\mathcal{K}}$.

Пусть $\mathcal{K}$ – произвольное ассоциативно-коммутативное кольцо с единицей, характеристика которого больше, чем 3.

Формула (2.91) имеет смысл над кольцом $\mathcal{K}$ тогда и только тогда, когда $3 \in K^{inv}$. При этом, при $3 \in K^{inv}$ преобразование (2.91) является обратимым преобразованием над кольцом $\mathcal{K}$.

Следовательно, над ассоциативно-коммутативным кольцом $\mathcal{K}$ с единицей, характеристика которого больше, чем 3, уравнение (2.71) может быть приведено к стандартной форме (2.81), если $2, 3 \in K^{inv}$.

Если $3 \notin K^{inv}$, но $3 \in S_{\mathcal{K}}$, то формула (2.91) имеет смысл (а определяемое ею преобразование становится обратимым) над расширением $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ кольца $\mathcal{K}$.

Следовательно, для ассоциативно-коммутативного кольца $\mathcal{K}$ с единицей, характеристика которого больше, чем 3, уравнение (2.71) может быть приведено к стандартной форме (2.81) над расширением $\overline{\mathcal{K}}$ кольца $\mathcal{K}$, если $2, 3 \in S_{\mathcal{K}}$.

Найдем дискриминанты и j-инварианты кривых, заданных уравнениями (2.78)-(2.81).

Пусть $\mathcal{K}$ – поле характеристики 2.

Для кривой Γ, заданной уравнением (2.78),

$$\Delta_\Gamma = -b_3^2, \tag{2.92}$$

$$j(\Gamma) = 0. \tag{2.93}$$

Отсюда вытекает, что уравнение (2.78) задает над полем $\mathcal{K}$ характеристики 2 эллиптическую кривую тогда и только тогда, когда $b_3 \neq 0$, причем все эллиптические кривые, заданные уравнением вида (2.78), изоморфны друг другу.

Для кривой Γ, заданной уравнением (2.79),

$$\Delta_\Gamma = b_6, \tag{2.94}$$

$$j(\Gamma) = b_6^{-1}. \tag{2.95}$$

Отсюда вытекает, что уравнение (2.79) задает над полем $\mathcal{K}$ характеристики 2 эллиптическую кривую тогда и только тогда, когда $b_6 \neq 0$, причем количество классов изоморфных эллиптических кривых над полем $\mathcal{K}$ характеристики 2, заданных уравнением вида (2.79), совпадает с мощностью мультипликативной группы поля $\mathcal{K}$.

Пусть характеристика поля $\mathcal{K}$ не равна 2.

Для кривой Γ, заданной уравнением (2.80),

$$\Delta_\Gamma = 16(b_2^2 b_4^2 - 4b_2^3 b_6 - 4b_4^3 - 27b_6^2 + 18b_2 b_4 b_6), \tag{2.96}$$

$$j(\Gamma) = 16^3 (b_2^2 - 3b_4)^3 \Delta_\Gamma^{-1}. \tag{2.97}$$

В частности, если характеристика поля $\mathcal{K}$ равна 3, то

$$\Delta_\Gamma = b_2^2 b_4^2 - b_2^3 b_6 - b_4^3, \tag{2.98}$$

$$j(\Gamma) = b_2^6 \Delta_\Gamma^{-1}. \tag{2.99}$$

Замечание 2.10. Пусть эллиптическая кривая Γ задана над полем $\mathcal{K}$ характеристики 3 уравнением (2.80).

Возможны следующие два случая.

Пусть $b_2 = 0$. Тогда уравнение (2.80) принимает вид

$$y^2 = x^3 + b_4 x + b_6, \tag{2.100}$$

причем из (2.98) вытекает, что $b_4 \neq 0$.

Пусть $b_2 \neq 0$ в уравнении (2.80) .

Если $c_2 \neq 0$, то в результате применения к уравнению

$$u^2 = v^3 + c_2 v^2 + c_4 v + c_6 \tag{2.101}$$

обратимого преобразования

$$\begin{cases} v = x - 2^{-1} c_2^{-1} c_4 \\ u = y \end{cases} \tag{2.102}$$

получим уравнение

$$y^2 = x^3 + b_2 x^2 + b_6, \tag{2.103}$$

где

$$\begin{cases} b_2 = c_2 \\ b_6 = c_6 - 2^{-3} c_2^{-3} c_4^3 - 2^{-2} c^{-1} c_4^2 \end{cases} .$$

Уравнения (2.100) и (2.103) называются стандартными формами эллиптических кривых над полем $\mathcal{K}$ характеристики 3.

Пусть $\mathcal{K} = (K, +, \cdot)$ – ассоциативно-коммутативное кольцо характеристики 3 с единицей.

Формула (2.102) имеет смысл над кольцом $\mathcal{K}$ тогда и только тогда, когда $2, c_2 \in K^{inv}$. При этом, при $2, c_2 \in K^{inv}$ преобразование (2.102) является обратимым преобразованием над кольцом $\mathcal{K}$.

Следовательно, над ассоциативно-коммутативным кольцом $\mathcal{K}$ с единицей, характеристика которого равна 3, уравнение (2.101) может быть приведено к стандартной форме (2.103), если $2, c_2 \in K^{inv}$.

Если $2, c_2 \notin K^{inv}$, но $2, c_2 \in S_{\mathcal{K}}$, то формула (2.102) имеет смысл (а определяемое ею преобразование становится обратимым) над расширением $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ кольца $\mathcal{K}$.

Следовательно, для ассоциативно-коммутативного кольца $\mathcal{K}$ с единицей, характеристика которого равна 3, уравнение (2.101) может быть приведено к стандартной форме (2.103) над расширением $\overline{\mathcal{K}}$ кольца $\mathcal{K}$, если $2, c_2 \in S_{\mathcal{K}}$.

Пусть характеристика поля $\mathcal{K}$ больше, чем 3.

Для кривой Γ, заданной уравнением (2.81),

$$\Delta_\Gamma = -16(4b_4^3 + 27b_6^2), \tag{2.104}$$

$$j(\Gamma) = (1728 \cdot 64) b_4^3 \Delta_\Gamma^{-1}. \tag{2.105}$$

2.3.3. Абелева группа на эллиптической кривой.

Многочисленные приложения эллиптических кривых над полями основаны на том обстоятельстве, что множество точек эллиптической кривой можно наделить структурой абелевой группы $\mathfrak{G}_\Gamma$.

Замечание 2.11. Содержательно построение структуры абелевой группы $\mathfrak{G}_\Gamma$ на множестве точек эллиптической кривой Γ, определенной уравнением (2.71), можно охарактеризовать следующим правилом: *сумма трех лежащих на одной прямой точек эллиптической кривой равна нулю $\mathcal{O}$ абелевой группы $\mathfrak{G}_\Gamma$.*

Для обоснования этого правила достаточно рассмотреть в проективной плоскости $\mathbf{P}$ проективную кривую $G(\xi, \eta, \zeta) = 0$ (G – однородный многочлен), соответствующую эллиптической кривой Γ.

Точки эллиптической кривой Γ лежат в аффинной плоскости $\mathbf{A}_3$, а нулем $\mathcal{O}$ абелевой группы $\mathfrak{G}_\Gamma$ является бесконечно удаленная точка $(0:1:0)$.

Таким образом,

$$\mathfrak{G}_\Gamma = (\Gamma \cup \{\mathcal{O}\}, +_{\mathfrak{G}_\Gamma}),$$

где:

1) для всех $P \in \Gamma \cup \{\mathcal{O}\}$

$$P +_{\mathfrak{G}_\Gamma} \mathcal{O} = \mathcal{O} +_{\mathfrak{G}_\Gamma} P = P;$$

2) если $P = (x, y) \in \Gamma$, то для противоположного элемента $-_{\mathfrak{G}_\Gamma} P$ истинно равенство

$$-_{\mathfrak{G}_\Gamma} P = (x, -y - a_1 x - a_3),$$

откуда, в частности вытекает, что для любой точки $P = (x, -2^{-1}(a_1 x + a_3)) \in \Gamma$ истинно равенство $P +_{\mathfrak{G}_\Gamma} P = \mathcal{O}$;

3) для любых трех точек $P_1, P_2, P_3 \in \Gamma$, лежащих на одной прямой

$$P_1 +_{\mathfrak{G}_\Gamma} P_2 +_{\mathfrak{G}_\Gamma} P_3 = \mathcal{O}.$$

Для того, чтобы вывести формулы, по которым вычисляются координаты суммы двух точек эллиптической кривой, достаточно учесть то обстоятельство, что в аффинной плоскости $\mathbf{A}_3$ бесконечно удаленной точке $(0:1:0)$ соответствует вертикальная прямая.

Пусть эллиптическая кривая Γ задана уравнением (2.71). Тогда в абелевой группе $\mathfrak{G}_\Gamma$ для любых двух таких точек $P_i = (x_i, y_i) \in \Gamma$ $(i = 1, 2)$, что $P_1 \neq -P_2$ точка

$$P_3 = P_1 +_{\mathfrak{G}_\Gamma} P_2 = (x_3, y_3)$$

вычисляется по формулам

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 + \alpha a_1 - a_2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) + a_1 x_3 - a_3 \end{cases}, \tag{2.106}$$

где

$$\alpha = \begin{cases} (3x_1^2 + 2a_2 x_1 + \\ \qquad +a_4 - a_1 y_1)(2y_1 + a_1 x_1 + a_3)^{-1}, & \text{если } x_1 = x_2\,. \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases} \tag{2.107}$$

Замечание 2.12. Из условия $P_1 \neq -P_2$ вытекает, что $P_1 = P_2$, если $x_1 = x_2$.

Это означает, что значение α, определяемое 1-й строкой формулы (2.107), используется для вычисления точки

$$2P_1 = P_1 +_{\mathfrak{G}_\Gamma} P_1 \ (P_1 \in \Gamma, P_1 \neq -P_1)$$

эллиптической кривой.

Отюда, в свою очередь, вытекает, что в абелевой группе $\mathfrak{G}_\Gamma$ для любой точки $P \in \Gamma$ вычисление точки

$$nP = \underbrace{P +_{\mathfrak{G}_\Gamma} \cdots +_{\mathfrak{G}_\Gamma} P}_{n} \ (n \in \mathbf{N})$$

может быть организовано с помощью стандартного алгоритма «удвоения элемента».

Если эллиптическая кривая приведена к стандартной форме, то формулы (2.106) и (2.107) принимают следующий вид.

Пусть характеристика поля $\mathcal{K}$ равна 2.

Если эллиптическая кривая Γ задана уравнением (2.78), то

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) - b_3 \end{cases}, \tag{2.108}$$

где

$$\alpha = \begin{cases} b_3^{-1}(x_1^2 + b_4), & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}. \tag{2.109}$$

Если эллиптическая кривая Γ задана уравнением (2.79), то

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 + \alpha - b_2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) + x_3 \end{cases}, \tag{2.110}$$

где

$$\alpha = \begin{cases} x_1 - y_1 x_1^{-1}, & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}. \tag{2.111}$$

Пусть характеристика поля $\mathcal{K}$ не равна 2, а эллиптическая кривая Γ задана уравнением (2.80). Тогда

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 - b_2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) \end{cases}, \tag{2.112}$$

где

$$\alpha = \begin{cases} (2y_1)^{-1}(3x_1^2 + 2b_2 x_1 + b_4), & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}. \tag{2.113}$$

В частности, если характеристика поля $\mathcal{K}$ равна 3, то

$$\alpha = \begin{cases} y_1^{-1}(b_2 x_1 - b_4), & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}. \tag{2.114}$$

Пусть характеристика поля $\mathcal{K}$ больше, чем 3, а эллиптическая кривая Γ задана уравнением (2.81). Тогда

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) \end{cases}, \tag{2.115}$$

где

$$\alpha = \begin{cases} (2y_1)^{-1}(3x_1^2 + b_4), & \text{если } x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & \text{если } x_1 \neq x_2 \end{cases}. \tag{2.116}$$

2.3.4. Эллиптические кривые над конечными полями.

Пусть в качестве поля $\mathcal{K}$ выбрано поле $\mathcal{Z}_p = (\mathbf{Z}_p, \oplus, \circ)$, где p ($p > 3$) – простое число, и для всех $a, b \in \mathbf{Z}_p$

$$a \oplus b = a + b \,(mod\, p),$$

$$a \circ b = ab \,(mod\, p).$$

Из (2.81) и (2.100) вытекает, что эллиптическая кривая Γ над полем $\mathcal{Z}_p$ может быть задана уравнением

$$y^2 = x^3 \oplus a \circ x \oplus b, \tag{2.117}$$

где $a, b \in \mathbf{Z}_p$, причем

$$4 \circ a^3 \oplus 27 \circ b^2 \neq 0. \tag{2.118}$$

Множество точек этой эллиптической кривой Γ совпадает с множеством решений сравнения

$$y^2 = x^3 + ax + b \,(mod\, p). \tag{2.119}$$

Для фиксированного числа $x \in \mathbf{Z}$ число решений этого сравнения равно:

1) 1, если $x^3 + ax + b = 0$;

2) 0, если $x^3 + ax + b$ – квадратичный невычет по модулю p;

3) 2, если $x^3 + ax + b$ – квадратичный вычет по модулю p.

Используя символ Лежандра, определяемый для числа $c \in \mathbf{Z}$, взаимно простого с числом p (т.е. $(c, p) = 1$) формулой

$$\left(\frac{c}{p}\right) = \begin{cases} 1, & \text{если сравнение } x^2 = c \text{ имеет решения} \\ -1, & \text{если сравнение } x^2 = c \text{ не имеет решений} \end{cases}, \tag{2.120}$$

и, положив по определению

$$\left(\frac{0}{p}\right) = 0,$$

получим, что для каждого фиксированного числа $x \in \mathbf{Z}$ число решений сравнения (2.119) равно

$$1 + \left(\frac{x^3 + ax + b}{p}\right).$$

Следовательно, для числа точек эллиптической кривой Γ, заданной над полем $\mathcal{Z}_p$ уравнением (2.117), истинно равенство

$$|\Gamma| = \sum_{x=0}^{p-1} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) =$$

$$= p + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p}\right). \qquad (2.121)$$

Отсюда вытекает, что истинно следующее равенство для порядка абелевой группы $\mathfrak{G}_\Gamma$, определенной для эллиптической кривой Γ, заданной над полем $\mathcal{Z}_p$ уравнением (2.117)

$$|\Gamma \cup \{\mathcal{O}\}| = 1 + p + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p}\right). \qquad (2.122)$$

Замечание 2.13. Для любого простого числа $p \in \mathbf{N}$ для каждого конечного расширения $\widetilde{\mathcal{Z}_p}$ поля $\mathcal{Z}_p$ существует такое число $k \in \mathbf{N}$, что поле $\widetilde{\mathcal{Z}_p}$ изоморфно полю многочленов от одной переменной с коэффициентами из поля $\mathcal{Z}_p$, степень которых не превосходит числа $k - 1$.

Такое поле называется *полем Галуа* и обозначается $\mathcal{GF}(p^k)$.

Таким образом, $\mathcal{Z}_p = \mathcal{GF}(p)$.

Известно, что множество всех конечных полей – это множество полей вида $\mathcal{GF}(p^k)$, где p – простое число, а $k \in \mathbf{N}$.

Рассмотрим эллиптическую кривую $\Gamma/\mathcal{GF}(p^k)$, где эллиптическая кривая Γ задана над полем $\mathcal{Z}_p$ $(p > 3)$ уравнением (2.117).

Известно (см., напр., [7]), что порядок абелевой группы $\mathfrak{G}_{\Gamma/\mathcal{GF}(p^k)}$ может быть вычислен по формуле

$$|\Gamma/\mathcal{GF}(p^k) \cup \{\mathcal{O}\}| = p^k + 1 - t_k, \qquad (2.123)$$

где число t_k определяется рекуррентным соотношением

$$\begin{cases} t_{j+1} = t_1 t_j - p t_{j-1} \ (j \in \mathbf{N}) \\ t_0 = 2 \\ t_1 = \sum\limits_{x=0}^{p-1} \left(\frac{x^3+ax+b}{p}\right) \end{cases} . \qquad (2.124)$$

Хотя формулы (2.122) и (2.124) дают возможность точно вычислить порядки абелевых групп $\mathfrak{G}_{\Gamma/\mathcal{GF}(p^k)}$, их использование затруднительно с вычислительной точки зрения.

Кроме того, они не дают возможность оценить порядки указанных абелевых групп.

Последний недостаток устраняется следующим образом.

Пусть $\mathcal{F}_q$ – конечное поле, характеристика которого больше, чем 3 (т.е. $\mathcal{F}_q = \mathcal{GF}(p^k)$, где p – простое число ($p \geq 3$), а $k \in \mathbf{N}$), а Γ – эллиптическая кривая, заданная над полем $\mathcal{F}_q$ уравнением

$$y^2 = x^3 + ax + b, \tag{2.125}$$

где

$$4a^3 + 27b^2 \neq 0.$$

Хассе показал, что для порядка абелевой группы $\mathfrak{G}_\Gamma$ истинна следующая оценка

$$\big|\,|\Gamma \cup \{\mathcal{O}\}| - (q+1)\big| \leq 2\sqrt{q}. \tag{2.126}$$

Замечание 2.14. Вывод оценки (2.126) осуществляется следующим образом.

Дзета-функцией эллиптической кривой Γ, определенной уравнением над полем $\mathcal{F}_q$, называется производящая функция

$$Z(\Gamma; T) = e^{\sum\limits_{l=1}^{\infty} \frac{N_l T^l}{l}}, \tag{2.127}$$

где N_l – порядок абелевой группы $\mathfrak{G}_{\Gamma/\mathcal{F}_{q^l}}$, а $\mathcal{F}_{q^l} = \mathcal{GF}(q^l)(= \mathcal{GF}(p^{kl}))$.

Для эллиптической кривой Γ, определенной уравнением (2.117) над полем $\mathcal{F}_q$, ряд (2.127) равномерно сходится (и,следовательно, он определяет аналитическую функцию) на интервале $-q^{-1} < T < q^{-1}$, причем на этом интервале истинно равенство

$$Z(\Gamma; T) = \frac{1 - tT + qT^2}{(1-T)(1-qT)}, \tag{2.128}$$

где число t определяется равенством

$$N_1 = q + 1 - t,$$

а дискриминант числителя неположителен (т.е. уравнение $1 - tT + qT^2 = 0$ имеет комплесно сопряженные корни).

Из (2.127) и (2.128) вытекает, что истинно равенство

$$N_l = q^l + 1 - \omega^l - \overline{\omega}^l \ \ (l \in \mathbf{N}), \tag{2.129}$$

где ω и $\overline{\omega}$ – комплексно-сопряженные корни уравнения

$$T^2 - tT + q = 0.$$

Из (2.129), в свою очередь вытекает, что

$$|N_1 - (q+1)| = |\omega + \overline{\omega}| \le |\omega| + |\overline{\omega}|. \tag{2.130}$$

По теореме Виетта

$$\omega\overline{\omega} = q.$$

Следовательно,

$$|\omega| = |\overline{\omega}| = \sqrt{q}. \tag{2.131}$$

Из (2.130) и (2.131) вытекает (2.126).

Из (2.126) вытекает, что для порядка абелевой группы $\mathfrak{G}_\Gamma$, определенной для эллиптической кривой Γ, заданной над полем $\mathcal{Z}_p$ (p – простое число, $p > 3$) уравнением (2.117), истинны неравенства

$$p + 1 - 2\sqrt{p} \le |\Gamma \cup \{\mathcal{O}\}| \le p + 1 + 2\sqrt{p}.$$

В [112] показано, что порядки абелевых групп $\mathfrak{G}_\Gamma$ эллиптических кривых Γ, заданных над полем $\mathcal{Z}_p$ (p – простое число, $p > 3$) уравнением (2.117), имеют на этом отрезке распределение, близкое к равномерному распределению.

Замечание 2.15. Более точно, в [112] доказано, что существуют такие эффективно вычисляемые константы $c_1, c_2 > 0$, что для каждого простого числа $p > 3$ для любого такого подмножества S целых чисел, что

$$S \subseteq [p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}]$$

вероятность $\mathtt{p}_S$ того, что случайно выбранная пара

$$(a, b) \in \mathbf{Z}_p^2$$

определяет такую эллиптическую кривую, заданную уравнением (2.117), что

$$|\Gamma \cup \{\mathcal{O}\}| \in S,$$

удовлетворяет неравенствам

$$\frac{|S| - 2}{2\lfloor\sqrt{p}\rfloor + 1} c_1 \log^{-1} p \le \mathtt{p}_S \le \frac{|S|}{2\lfloor\sqrt{p}\rfloor + 1} c_2 \log p (\log\log p)^2.$$

Пусть эллиптическая кривая Γ задана над полем $\mathcal{F}_q$ характеристики большей, чем 3 уравнением

$$y^2 = x^3 + ax + b,$$

а ν – квадратичный невычет над полем $\mathcal{F}_q$, т.е. уравнение

$$x^2 = \nu$$

не имеет решений в поле $\mathcal{F}_q$. Эллиптическая кривая Γ_1, заданная уравнением

$$y^2 = x^3 + a_1 x + b_1,$$

где

$$a_1 = \nu^2 a,$$
$$b_1 = \nu^3 b$$

называется *скручиванием* эллиптической кривой Γ над полем $\mathcal{F}_q$. Известно, что:

1) $|\Gamma| + |\Gamma_1| = 2q$, и следовательно, порядки абелевых групп $\mathfrak{G}_\Gamma$ и $\mathfrak{G}_{\Gamma_1}$ эллиптических кривых Γ и Γ_1 связаны соотношением

$$|\Gamma \cup \{\mathcal{O}\}| + |\Gamma_1 \cup \{\mathcal{O}\}| = 2q + 2;$$

2) эллиптические кривые Γ и Γ_1 не изоморфны над полем $\mathcal{F}_q$, но изоморфны над полем $\mathcal{F}_{q^2}$.

В заключение отметим, что для любого конечного поля $\mathcal{F}_q$ структура абелевой группы $\mathfrak{G}_\Gamma$, определенной для эллиптической кривой Γ, заданной уравнением над полем $\mathcal{F}_q$, имеет следующий вид: либо группа $\mathfrak{G}_\Gamma$ является циклической группой, либо группа $\mathfrak{G}_\Gamma$ изоморфна прямой сумме абелевых групп $\mathcal{Z}_{d_i} = (\mathbf{Z}_{d_i}, \oplus)$ $(i = 1, 2)$, где d_1 – делитель числа $q-1$, а d_2 – делитель числа d_1.

Замечание 2.16. Прямой суммой абелевых групп $\mathcal{G}_1 = (G_1, +_{\mathcal{G}_1})$ и $\mathcal{G}_2 = (G_2, +_{\mathcal{G}_2})$ называется абелева группа

$$\mathcal{G}_1 \dot{+} \mathcal{G}_2 = (G_1 \times G_2, +_{\mathcal{G}}),$$

где

$$(a_1, b_1) +_{\mathcal{G}} (a_2, b_2) = (a_1 +_{\mathcal{G}_1} a_2, b_1 +_{\mathcal{G}_2} b_2)$$

для всех $(a_1, b_1), (a_2, b_2) \in G_1 \times G_2$.

2.3.5. Некоторые приложения эллиптических кривых.

По-видимому, наиболее известным приложением эллиптических кривых над конечными полями при решении задач криптографии является электронно-цифровая подпись (ЭЦП) на основе эллиптических кривых – одно из наиболее интенсивно развиваемых в настоящее время направлений современной асимметрической криптографии.

Рассмотрим алгоритм ECDSA формирования ЭЦП над полем Галуа $\mathcal{Z}_p = (\mathbf{Z}_p, \oplus, \circ)$ (p – простое число).

Для организации ЭЦП вначале осуществляется генерация ключей на основе следующего алгоритма.

Алгоритм 2.1.

Шаг 1. Фиксируем достаточно большое число $n \in \mathbf{N}$ и выбираем над полем $\mathcal{Z}_p$ такую эллиптическую кривую Γ, что порядок абелевой группы $\mathfrak{G}_\Gamma$ делится на число n.

Шаг 2. Выбираем точку $P \in \Gamma$ порядка n (в абелевой группе $\mathfrak{G}_\Gamma$).

Шаг 3. Выбираем случайное число $d \in \mathbf{N}_{n-1}$.

Шаг 4. Вычисляем элемент $Q = dP$ абелевой группы $\mathfrak{G}_\Gamma$.

Шаг 5. Число d – секретный ключ, а (Γ, P, n, Q) – открытый ключ.

Зафиксируем хэш-функцию $H : \mathbf{E}^+ \to \mathbf{Z}_p$ ($\mathbf{E} = \{0, 1\}$).

Замечание 2.17. В стандартах ANSI X9F1 и IEEE P1363 в качестве H используется стандартная хэш-функция SHA-1.

Алгоритм ECDSA формирования ЭЦП под сообщением $u \in \mathbf{E}^+$ имеет следующий вид.

Алгоритм 2.2.

Шаг 1. Выбираем случайное число $k \in \mathbf{N}_{n-1}$.

Шаг 2. Вычисляем элемент $kP = (x_1, y_1)$ абелевой группы $\mathfrak{G}_\Gamma$.

Шаг 3. $r := x_1 \,(mod\, n)$.

Шаг 4. Если $r = 0$, то переход к шагу 1, иначе – к шагу 5.

Шаг 5. В поле $\mathcal{Z}_p$ вычисляется элемент k^{-1}.

Шаг 6. В поле $\mathcal{Z}_p$ вычисляется элемент $H(u)$.

Шаг 7. $s := k^{-1} \circ (H(u) \oplus d \circ r)$.

Шаг 8. Если $s = 0$, то переход к шагу 1, иначе – к шагу 9.

Шаг 9. Упорядоченная пара чисел (r, s) объявляется ЭЦП под сообщением u и конец.

Алгоритм проверки ЭЦП, сформированной на основе алгоритма 2.2, имеет следующий вид.

Алгоритм 2.3.

Шаг 1. Если $r, s \in \mathbf{N}_{n-1}$, то переход к шагу 2, иначе – к шагу 10.
Шаг 2. В поле $\mathcal{Z}_p$ вычисляется элемент s^{-1}.
Шаг 3. В поле $\mathcal{Z}_p$ вычисляется элемент $H(u)$.
Шаг 4. $\alpha := H(u) \circ s^{-1}$.
Шаг 5. $\beta := r \circ s^{-1}$.
Шаг 6. Вычисляем элемент $\alpha P +_{\mathfrak{G}_\Gamma} \beta Q = (x_0, y_0)$ абелевой группы $\mathfrak{G}_\Gamma$.
Шаг 7. $v := x_0 \,(mod\, n)$.
Шаг 8. Если $v = r$, то переход к шагу 9, иначе – к шагу 10.
Шаг 9. ЭЦП принимается и конец.
Шаг 10. ЭЦП отвергается и конец.

Предположение о вычислительной стойкости алгоритма ECDSA основано на предположении, что трудной является задача дискретного логарифмирования в абелевой группе $\mathfrak{G}_\Gamma$, а именно: поиск решения d уравнения

$$dP = Q.$$

Замечание 2.18. В [52] показано, что алгоритм ECDSA с небольшими изменениями остается корректным в поле $\mathcal{Q} = (\mathbf{Q}, +\cdot)$ рациональных чисел.

Предложенный в [52] подход состоит в следующем.

Пусть эллиптическая кривая Γ задана над полем $\mathcal{Q}$ уравнением

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6,$$

т.е. сложение в абелевой группе $\mathfrak{G}_\Gamma$ осуществляется в соответствии с формулами (2.106) и (2.107).

По аналогии с тем, как это сделано для алгоритма ECDSA, секретный ключ – случайно выбранное число $l \in \mathbf{N}$, а открытый ключ – набор (E, P, Q), где $P, Q \in \Gamma$, причем $Q = lP$.

Пусть $gnrtr()$ – псевдослучайный генератор натуральных чисел, а $H : \mathbf{E}^+ \to \mathbf{E}^{256}$ – хэш-функция.

Для двоичной последовательности

$$v = \alpha_{255} \ldots \alpha_0$$

положим

$$a(v) = \sum_{i=0}^{255} \alpha_i 2^i.$$

Алгоритм формирования ЭЦП под сообщением $u \in \mathbf{E}^+$ имеет следующий вид.

Алгоритм 2.4.

Шаг 1. $v := H(u)$, $w := a(v)$.
Шаг 2. Если $w = 0$, то $w := 1$.
Шаг 3. $k := gnrtr()$.
Шаг 4. Вычисляем элемент $kP = (x_1, y_1)$ абелевой группы $\mathfrak{G}_\Gamma$.
Шаг 5. $r := \lfloor x_1 \rfloor$.
Шаг 6. Если $r = 0$, то переход к шагу 3, иначе – к шагу 7.
Шаг 7. $s := rl + kw^{-1}$.
Шаг 8. Если $s = 0$, то переход к шагу 3, иначе – к шагу 9.
Шаг 9. Упорядоченная пара чисел (r, s) объявляется ЭЦП под сообщением u и конец.

Алгоритм 2.4 отличается от алгоритма ГОСТ Р 34.10-2001 только следующим.
На шаге 5 алгоритма 2.4 число r определяется формулой

$$r = \lfloor x_1 \rfloor,$$

а в алгоритме ГОСТ Р 34.10-2001 – формулой

$$r := x_1.$$

На шаге 7 алгоритма 2.4 число s определяется формулой

$$s = rl + kw^{-1},$$

а в алгоритме ГОСТ Р 34.10-2001 – формулой

$$s = r \circ l \oplus k \circ w.$$

Отсюда и из корректности алгоритма ГОСТ Р 34.10-2001 непосредственно вытекает корректность алгоритма 2.4.

Алгоритм проверки ЭЦП, сформированной на основе алгоритма 2.4, состоит в следующем.

Алгоритм 2.5.

Шаг 1. $v := H(u)$, $w := a(v)$.
Шаг 2. Если $w = 0$, то $w := 1$.
Шаг 3. $z_1 := sw$.
Шаг 4. $z_2 := -rw$.
Шаг 5. Вычисляем элемент $z_1 P +_{\mathfrak{G}_\Gamma} z_2 Q = (x_0, y_0)$ абелевой группы $\mathfrak{G}_\Gamma$.
Шаг 6. $b := \lfloor x_0 \rfloor$.
Шаг 7. Если $b = r$, то переход к шагу 8, иначе – к шагу 9.
Шаг 8. ЭЦП принимается и конец.
Шаг 9. ЭЦП отвергается и конец.

Алгоритм 2.5 отличается от алгоритма ГОСТ Р 34.10-2001 только следующим.
На шаге 3 алгоритма 2.5 число z_1 определяется формулой

$$z_1 := sw,$$

а в алгоритме ГОСТ Р 34.10-2001 – формулой

$$z_1 := s \circ w^{-1}.$$

На шаге 4 алгоритма 2.5 число z_2 определяется формулой

$$z_2 = -rw,$$

а в алгоритме ГОСТ Р 34.10-2001 – формулой

$$z_2 = \ominus r \circ w^{-1}.$$

Отсюда и из корректности алгоритма ГОСТ Р 34.10-2001 непосредственно вытекает корректность алгоритма 2.5.

Теоретически возможно, что в процессе использования компьютерной реализации алгоритмов 2.4 и 2.5 могут возникнуть ошибки, связанные с процессом округления.

Для нивелирования таких ошибок достаточно применить подход, основанный на повышении точности вычислений, по аналогии с тем, как это сделано в [2] при решении обратных задач хаотической динамики.

Эллиптические кривые над конечным кольцом могут быть использованы при решении задачи факторизации чисел – модельной теоретико-числовой задачи, имеющей многочисленные приложения.

В [112] предложен вероятностный алгоритм субэкспоненциальной сложности, предназначенный для разложения числа $n \in \mathbf{N}$ на простые множители (этот алгоритм получил имя *алгоритм Ленстры*), основанный на следующих построениях.

Зафиксируем кольцо $\mathcal{Z}_n = (\mathbf{Z}_n, \oplus, \circ)$, где $n \in \mathbf{N}$ – составное нечетное не делящееся на 3 число.

Будем рассматривать только такие тройки элементов

$$(x, y, z) \in \mathbf{Z}_n^3,$$

что идеал

$$I = (x, y, z)$$

совпадает с кольцом $\mathcal{Z}_n$ (достаточным условием для этого является взаимная простота чисел x и n).

Множество

$$(x : y : z) = \{(ux, uy, uz) | u \in \mathbf{Z}_n^{inv}\}$$

называется *орбитой* элемента (x, y, z), а множество всех орбит $\mathbf{P}$ представляет собой аналог проективной плоскости над полем.

Положим

$$\mathbf{V} = \{(x : y : 1) | x, y \in \mathbf{Z}_n\} \cup \{\mathcal{O}\}.$$

Обозначим через $\Gamma_{a,b}$ эллиптическую кривую заданную над кольцом $\mathcal{Z}_n$ уравнением

$$y^2 = x^3 \oplus a \circ x \oplus b,$$

где $a, b \in \mathbf{Z}_n$, причем

$$4 \circ a^3 \oplus 27 \circ b^2 \in \mathbf{Z}_n^{inv}. \tag{2.132}$$

Факторизация числа n основана на следующем свойстве сложения в абелевой группе $\mathfrak{G}_{\Gamma_{a,b}} = (\mathbf{V}, +_{\mathfrak{G}_{\Gamma_{a,b}}})$.

Пусть $P_1 = (x_1 : y_1 : 1) \in \mathbf{V}$ и $P_2 = (x_2 : y_2 : 1) \in \mathbf{V}$.

При вычислении элемента

$$P_3 = P_1 +_{\mathfrak{G}_{\Gamma_{a,b}}} P_2$$

прежде всего вычисляется число

$$d = \text{НОД}(x_1 - x_2, n).$$

Возможны следующие три ситуации.

1. Пусть $d = 1$. Тогда d – делитель числа n и алгоритм Ленстры заканчивает работу.

2. Пусть $1 < d < n$. Тогда $P_3 = (x_3 : y_3 : 1)$, где

$$\begin{cases} x_3 = (\lambda^2 - x_1 - x_2) \, (mod \, n) \\ y_3 = (-\lambda x_3 - \nu) \, (mod \, n) \end{cases},$$

а

$$\begin{cases} \lambda = (y_1 - y_2)(x_1 - x_2)^{-1} \, (mod \, n) \\ \nu = y_1 - \lambda x_1 \, (mod \, n) \end{cases}.$$

3. Пусть $d = n$. Тогда

$$x_1 \equiv x_2 \, (mod \, n).$$

В этом случае вычисляется число

$$d_1 = \text{НОД}(y_1 + y_2, n).$$

Здесь, в свою очередь, возможны следующие три ситуации.

3.1. Пусть $1 < d_1 < n$. Тогда d_1 – делитель числа n и алгоритм Ленстры заканчивает работу.

3.2. Пусть $d_1 = n$. Тогда

$$y_1 \equiv -y_2 \,(mod\, n)$$

и, следовательно, $P_3 = \mathcal{O}$.

3.3. Пусть $d_1 = 1$. Тогда $P_3 = (x_3 : y_3 : 1)$, где

$$\begin{cases} x_3 = (\lambda^2 - 2x_1) \,(mod\, n) \\ y_3 = (-\lambda x_3 - \nu) \,(mod\, n) \end{cases},$$

а

$$\begin{cases} \lambda = (3x_1^2 + a)(y_1 + y_2)^{-1} \,(mod\, n) \\ \nu = (y_1 - \lambda x_1) \,(mod\, n) \end{cases}.$$

Отметим, что представив число $k \in \mathbf{N}$ в виде

$$k = k_1 \ldots k_l \ (k_1 > \ldots k_l > 1),$$

можно осуществить вычисление элемента kP $(P \in \mathbf{V})$ абелевой группы $\mathfrak{G}_{\Gamma_{a,b}}$ в соответствии с формулой

$$kP = k_1(\ldots(k_l P)\ldots). \tag{2.133}$$

Алгоритм Ленстры состоит в следующем.

Задано факторизуемое число $n \in \mathbf{N}$, параметры $v, w \in \mathbf{N}$, а также такие элементы $a, x, y \in \mathbf{Z}_n$ кольца $\mathcal{Z}_n$, что для элемента

$$b = y^2 \ominus x^3 \ominus a \circ x$$

выполнено условие (2.128).

Для каждого числа $r \in \{2, \ldots, w\}$ вычисляется число

$$e(r) = \max\{m \in \mathbf{Z}_+ | r^m \leq v + 2\sqrt{v} + 1\}.$$

Для числа

$$k = \prod_{\substack{2 \leq r \leq w \\ r \ - \text{ простое}}} r^{e(r)}$$

и элемента $P = (x : y : 1)$ абелевой группы $\mathfrak{G}_{\Gamma_{a,b}}$ в соответствии с формулой (2.133) вычисляется элемент kP.

Если при этих вычислениях найден делитель числа n, то число n разложено на два множителя и алгоритм останавливается.

Если же делитель не найден, то алгоритм выдает сообщение о неудачной факторизации.

3. ИССЛЕДОВАНИЕ КРИВЫХ НАД КОЛЬЦАМИ МЕТОДАМИ АЛГЕБРАИЧЕСКОЙ ГЕОМЕТРИИ

В разделе 2 в процессе анализа алгебраических кривых фрагментарно использовались модели и методы алгебраической геометрии.

Целью настоящего раздела является систематическое изложение моделей и методов алгебраической геометрии, применяемых в процессе анализа алгебраических кривых, определенных над конечными кольцами. Существенная характеристика изложенного ниже подхода состоит в том, что наряду с непосредственным рассмотрением алгебраических кривых с коэффициентами в конечных кольцах, анализ таких кривых осуществляется также в результате их локализации по модулям идеалов над более общими кольцами их определения. Необходимость именно такого подхода к анализу алгебраических кривых, определенных над конечными кольцами, возникает при исследовании как теоретических, так и прикладных задач. А безусловным достоинством такого подхода является то, что он дает возможность применять в процессе анализа алгебраических кривых как локальные, так и глобальные методы.

В п.3.1 введены необходимые понятия и определения. В п.3.2 охарактеризована минимальная модель эллиптической кривой над полем p-адических чисел и над полем рациональных чисел. В п.3.3 рассмотрены подходы к представлению гомоморфизмов эллиптических кривых в терминах решеток и в терминах линейных преобразований переменных. В п.3.4 показано, каким образом понятие «степень отображения» используется в процессе анализа морфизмов алгебраических кривых. Охарактеризовано кольцо эндоморфизмов эллиптической кривой. В п.3.5 рассмотрено значение понятия «изогения» при исследовании морфизмов алгебраических кривых. В п.3.6 рассмотрены модулярные функции и модулярные формы и установлена их связь с эллиптическими кривыми. В п. 3.7 изложены основы кодирования специального класса отображений, реализующих псевдослучайные генераторы, d-ичными ($d \in \mathbf{N}, d \geq 2$) последовательностями.

Результаты авторов, представленные в разделе, опубликованы в [11-23,97-104].

Известные результаты, представленные в настоящем разделе, изложены в соответствии с подходом, принятым в [1,5,6,8-10,27-30,32,42,43,45,45,48,49,80,82-84,86-94].

3.1. Основные понятия.

С каждой плоской неприводимой алгебраической кривой Γ можно сопоставить некоторое множество функций, определенных на этой кривой, которое содержит существенную информацию об этой кривой и ее свойствах. Рассмотрим такие множества функций.

3.1.1. Рациональные функции на кривых.

Пусть $\mathcal{K} = (K, +, \cdot)$ – поле, а $\mathcal{K}[x, y] = (K[x, y], +, \cdot)$ – кольцо многочленов от переменных x и y над полем $\mathcal{K}$.

Плоской аффинной кривой над полем $\mathcal{K}$ называется множество Γ точек в $K^2 = K \times K$, удовлетворяющих уравнению

$$f(x, y) = 0,$$

где $f(x, y) \in K[x, y]$.

Замечание 3.1. Далее предполагается, что поле $\mathcal{K}$ алгебраически замкнуто, а случаи, когда это условие не выполняется, будут оговариваться специально.

Кривая, уравнение которой является неприводимым многочленом в $\mathcal{K}[x, y]$ называется неприводимой.

Пусть $p(x, y), q(x, y) \in K[x, y]$, а $f(x, y) = 0$ – уравнение плоской неприводимой алгебраической кривой Γ.

Рациональные функции

$$r(x, y) = \frac{p(x, y)}{q(x, y)} \quad \left(= \frac{p}{q}\right),$$

удовлетворяющие условию:

$$f \text{ не делит } q,$$

называются рациональными функциями на кривой Γ.

Рациональные функции $r_1 = \frac{p_1}{q_1}$ и $r_2 = \frac{p_2}{q_2}$ считаются равными (на кривой Γ) тогда и только тогда, когда

$$p_1 q_2 - p_2 q_1 \equiv 0 \, (mod \, f).$$

Множество всех таких рациональных функций обозначим $K(\Gamma)$.

Утверждение 3.1. Алгебраическая система $\mathcal{K}(\Gamma) = (K(\Gamma), +, \cdot)$ является полем.

Доказательство. Пусть $r_1 = \frac{p_1}{q_1}$ и $r_2 = \frac{p_2}{q_2}$ – рациональные функции на кривой Γ. Тогда их сумма

$$r_1 + r_2 = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2}$$

также является рациональной функцией на кривой Γ.

Рациональная функция $\frac{p}{q}$, где $p \equiv 0 \, (mod \, f)$ и $q \not\equiv 0 \, (mod \, f)$, равна на кривой Γ нулевой функции $\frac{0}{q}$.

Обратно, любая нулевая функция на кривой Γ имеет вид $\frac{p_1 f^n}{q}$, где $n \in \mathbf{N}$ и $p_1, q \not\equiv 0\,(mod\, f)$.

Пусть $\frac{p}{q}$ – ненулевая рациональная функция на кривой Γ. Тогда функция $\frac{q}{p}$ также является рациональной функцией на кривой Γ.

А из равенства

$$\frac{p}{q} \cdot \frac{q}{p} = 1$$

вытекает, что $\mathcal{K}(\Gamma)$ – поле.

□

Поле $\mathcal{K}(\Gamma)$ – это поле рациональных функций на кривой Γ.

Рациональная функция $\frac{p}{q} \in K(\Gamma)$ регулярна в точке $P \in \Gamma$, если $q(P) \neq 0$.

Элементы поля $\mathcal{K}(\Gamma)$ можно рассматривать как функции на кривой Γ, определенные всюду на Γ, кроме, возможно, конечного числа точек.

Пусть Γ_1, Γ_2 – две плоские алгебраические кривые и $u, v \in K(\Gamma_1)$.

Замечание 3.2. Далее алгебраические кривые всегда предполагаются плоскими и неприводимыми, кроме специально оговариваемых случаев.

Отображение

$$\varphi(P) = (u(P), v(P))$$

называется рациональным отображением кривой Γ_1 в кривую Γ_2, если $\varphi(P) \in \Gamma_2$ при $P \in \Gamma_1$. Если кривая Γ_2 определяется уравнением $g(x, y) = 0$, то $g(u(P), v(P))$ обращается в нуль во всех точках кривой Γ_1, кроме, может быть, конечного числа точек.

Алгебраические кривые над полем $\mathcal{K}$ и рациональные отображения, определенные между этими кривыми, образуют *категорию*.

Действительно, рассмотрим для кривых Γ_1, Γ_2 и Γ_3 рациональные отображения $\varphi_1 : \Gamma_1 \to \Gamma_2$ и $\varphi_2 : \Gamma_2 \to \Gamma_3$, где

$$\varphi_1(P_1) = (u_1(P_1), v_1(P_1)) \ (P_1 \in \Gamma_1),$$

$$\varphi_2(P_2) = (u_2(P_2), v_2(P_2)) \ (P_2 \in \Gamma_2).$$

Определим композицию $\varphi_2 \circ \varphi_1 : \Gamma_1 \to \Gamma_3$ равенством

$$(\varphi_2 \circ \varphi_1)(P) = (u_2(u_1(P), v_1(P)), v_2(u_1(P), v_1(P))).$$

Эта композиция ассоциативна и для всякой кривой Γ имеется тождественное рациональное отображение 1_Γ, оставляющее точки кривой Γ на месте.

Обозначим через $\mathtt{Alc}(\mathcal{K})$ категорию, объекты которой – алгебраические кривые над полем $\mathcal{K}$, а морфизмы – множества рациональных отображений одной алгебраической кривой в другую.

Рациональное отображение $\varphi : \Gamma_1 \to \Gamma_2$ называется бирациональным изоморфизмом кривых Γ_1 и Γ_2, если существует такое рациональное отображение $\psi : \Gamma_2 \to \Gamma_1$, что $\psi \circ \varphi = 1_{\Gamma_1}$ и $\varphi \circ \psi = 1_{\Gamma_2}$, т.е. $\psi \circ \varphi$ и $\varphi \circ \psi$ являются тождественными отображениями (в точках, где они определены). Кривые Γ_1 и Γ_2 называются в этом случае бирационально изоморфными.

Пусть $\Gamma : y^2 = f(x)$ есть алгебраическая кривая, а Δ_Γ – дискриминант $\mathrm{disc}(f)$ многочлена $f(x)$.

Алгебраические кривые классифицируются по их роду $g \in \mathbf{N}$.

Замечание 3.3. Пусть $\mathbf{V}$ – векторное пространство размерности $n+1$ над полем $\mathcal{F} = (F, +, \cdot)$. Совокупность *прямых* (т.е. одномерных подпространств) пространства $\mathbf{V}$ называется *n-мерным проективным пространством* и обозначается $\mathbf{P}^n(\mathcal{F})$.

Любая точка $\mathbf{x} \in \mathbf{P}^n(\mathcal{F})$ задается *обобщенными координатами*, т.е. таким набором $(\xi_0 : \xi_1 : \cdots : \xi_n)$ элементов поля $\mathcal{F}$, что не все ξ_i $(i = 0, 1, \ldots, n)$ равны нулю

Точки $(\xi_0 : \xi_1 : \cdots : \xi_n)$ и $(\eta_0 : \eta_1 : \cdots : \eta_n)$ равны тогда и только тогда, когда существует такой элемент $\lambda \in F \backslash \{0\}$, что

$$\eta_i = \lambda \xi_i \ \ (i = 0, 1, \ldots, n).$$

Многочлен $f \in F[s_0, s_1, \ldots, s_n]$ обращается в нуль в точке $\mathbf{x} \in \mathbf{P}^n(\mathcal{F})$ тогда и только тогда, когда когда для любых координат $(\xi_0 : \xi_1 : \cdots : \xi_n)$ этой точки равенство

$$f(\lambda\xi_0, \lambda\xi_1, \ldots, \lambda\xi_n) = 0$$

истинно для всех $\lambda \in F \backslash \{0\}$.

Подмножество $\mathbf{X} \subset \mathbf{P}^n(\mathcal{F})$ называется *замкнутым*, если оно состоит из всех точек, в которых одновременно обращается в нуль конечное число многочленов с коэффициентами из поля $\mathcal{F}$.

Множество всех многочленов $f \in F[s_0, s_1, \ldots, s_n]$, обращающихся в нуль во всех точках $\mathbf{x} \in \mathbf{X}$ является идеалом кольца $\mathcal{F}[s_0, s_1, \ldots, s_n]$. Если этому идеалу принадлежит многочлен f, то ему принадлежат и все однородные составляющие многочлена f. Идеалы, обладающие таким свойством, называются *однородными*.

Таким образом, идеал замкнутого подмножества проективного пространства – однородный идеал.

Если $\mathbf{X}, \mathbf{Y} \subset \mathbf{P}^n(\mathcal{F})$ ($\mathbf{Y} \subset \mathbf{X}$) – проективные замкнутые множества, то множество $\mathbf{X}\backslash\mathbf{Y}$ называется *открытым* в $\mathbf{X}$.

Квазипроективным многообразием называется открытое подмножество замкнутого проективного множества.

Дифференциалом многочлена $f(t_1, \ldots, t_n)$ в точке $\mathbf{x} = (x_1, \ldots, x_n)$ называется линейная форма

$$\mathsf{d}_{\mathbf{x}} f = \sum_{i=1}^{n} (\mathsf{D}_{t_i} f(t_1, \ldots, t_n))|_{\mathbf{x}} (t_i - x_i).$$

Пусть $V = V(f_1, \ldots, f_m)$ – многообразие в множестве F^n и $\mathbf{x} \in V$. *Касательным пространством* $\Theta_{\mathbf{x},V}$ многообразия V в точке $\mathbf{x}$ называется множество решений системы уравнений

$$\mathsf{d}_{\mathbf{x}} f_1 = \cdots = \mathsf{d}_{\mathbf{x}} f_m = 0.$$

Содержательно, касательное пространство $\Theta_{\mathbf{x},V}$ представляет собой множество всех прямых, касающихся многообразия V в точке $\mathbf{x}$.

Истинно следующее утверждение: *при изоморфизме многообразий касательные пространства соответствующих точек отображаются изоморфно.*

Обозначим через $\Theta^*_{\mathbf{x},V}$ пространство линейных форм на $\Theta_{\mathbf{x},V}$, а через $\Phi[V]$ – множество отображений φ, сопоставляющих каждой точке $\mathbf{x} \in V$ вектор $\varphi(\mathbf{x}) \in \Theta^*_{\mathbf{x},V}$. Множество $\Phi[V]$ является абелевой группой, если операцию сложения отображений $\varphi, \psi \in \Phi[V]$ определить равенством

$$(\varphi + \psi)(\mathbf{x}) = \varphi(\mathbf{x}) + \psi(\mathbf{x}).$$

Множество $\Phi[V]$ становится модулем над кольцом всех отображений, определенных на многообразии V и принимающих значения в поле $\mathcal{F}$, если положить

$$(f \circ \varphi)(\mathbf{x}) = f(\mathbf{x}) \cdot \varphi(\mathbf{x})$$

где f – отображение, определенное на многообразии V и принимающее значения в поле $\mathcal{F}$, а $\varphi \in \Phi[V]$.

Элемент $\varphi \in \Phi[V]$ называется *регулярной на V дифференциальной формой*, если любая точка $\mathbf{x} \in V$ имеет такую окрестность U, что сужение φ на U принадлежит подмодулю модуля $\Phi[U]$, порожденному над кольцом $\mathcal{F}[U]$ элементами $\mathsf{d}_{\mathbf{x}} f$ ($f \in \mathcal{F}[U]$).

Все регулярные на многообразии V дифференциальные формы образуют модуль $\Omega[V]$ над кольцом $\mathcal{F}[U]$.

Если V – гладкая проективная алгебраическая кривая, то размерность векторного пространства $\Omega[V]$ называется родом кривой V и обозначается через g.

Рассмотрим эллиптические кривые ($g = 1$) и гиперэллиптические кривые рода $g \geq 2$ над полем $\mathcal{F}_p$ $(= \mathcal{Z}_p)$ (где p – простое число)

$$\Gamma_g : \; y^2 = f(x) \; (\mathrm{disc}(f) \neq 0).$$

Для проективного замыкания Γ_g квазипроективное многообразие

$$\mathbf{H}_{g,p} = (\mathbf{P}^{2g+1}(\mathcal{F}_p) \backslash \Delta_{\Gamma_g} = 0)$$

параметризует все гиперэллиптические кривые рода g над полем $\mathcal{F}_p$.

Для многих приложений эллиптических кривых над конечными кольцами привлекаются результаты не только о кривых над полями характеристики p, но также и над кольцами целых элементов полей. Поэтому ниже рассматриваются результаты об эллиптических кривых и накрытиях Артина-Шрайера в любой характеристике.

3.1.2. Нормальные формы эллиптических кривых.

В математических и прикладных исследованиях используются, в зависимости от исследуемых задач и вкусов исследователей, различные формы алгебраических уравнений, задающих эллиптические кривые.

Такие уравнения называют *нормальными* (или *стандартными*) *формами*.

Отметим, что большинство из таких форм было выведено еще в прошлом и позапрошлом веках при исследовании эллиптических кривых над полем комплексных чисел.

Замечание 3.4. Для того, чтобы приводимые ниже уравнения определяли эллиптические кривые, требуется, чтобы дискриминанты многочленов, стоящих в правой части уравнения, были отличны от нуля. Всюду в дальнейшем предполагается, что это условие выполнено.

В случае поля комплесных чисел наиболее известными являются следующие модификации Вейерштрассовой нормальной формы:

$$(\wp')^2 = 4(\wp)^3 - 60c_2\wp - 140c_3, \tag{3.1}$$

$$y^2 = 4x^3 - g_2x - g_3 \; (g_2^3 - 27g_3^2 \neq 0), \tag{3.2}$$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.3}$$

Замечание 3.5. Пусть $\omega_1, \omega_2 \in \mathbf{C}$ – такие числа, не лежащие на одной прямой, проходящей через начало координат, что поворот от вектора ω_1 к вектору ω_2 осуществляется по часовой стрелке, т.е.

$$Im\frac{\omega_1}{\omega_2} > 0.$$

Решеткой, построенной по числам ω_1 и ω_2 называется множество

$$\Lambda = \{m\omega_1 + n\omega_2 | m, n \in \mathbf{Z}\}.$$

$\wp$-функция Вейерштрасса $\wp = \wp(z)$ $(z \in \mathbf{C})$ определяется равенством

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{l\in\Lambda \\ l\neq 0}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right).$$

Нормальные формы, определяемые уравнениями (3.1), (3.2) и (3.3) обозначим, соответственно, через (NW), (W) и (EC).

Нормальные формы (NW) и (W) пригодны и для полей характеристики, отличной от 2 и 3, а форма (EC) – для полей любой характеристики.

Лежандрова нормальная форма эллиптической кривой имеет вид

$$y^2 = x(x-1)(x-\lambda) \ (\lambda \in \mathbf{C}\backslash\{0,1\}). \tag{3.4}$$

Эту нормальную форму обозначим через (L).

Если нормальная форма (L) рассматривается над полем $\mathcal{F}$ характеристики $p > 0$, то (L) определяет эллиптическую кривую при условии, что $\lambda \neq 0$.

Пусть эллиптическая кривая Γ над кольцом целых чисел $\mathcal{Z} = (\mathbf{Z}, +, \cdot)$ определена уравнением

$$y^2 = x^3 + ax + b \ (a, b \in \mathbf{Z}, \ \Delta_\Gamma \neq 0). \tag{3.5}$$

Эту нормальную форму обозначим через (E).

Пусть $\mathcal{K} = (K, +, \cdot)$ – поле, характеристика которого не равна 2.

Эллиптические кривые Эдвардса над полем $\mathcal{K}$ задаются уравнением

$$x^2 + y^2 = 1 + dx^2y^2 \ (d \in K\backslash\{0,1\}). \tag{3.6}$$

Эту нормальную форму обозначим через (Ed1).

Эллиптической кривой Эдвардса также называют и кривую над полем $\mathcal{K}$, которая задана уравнением

$$x^2 + y^2 = c^2(1 + dx^2y^2) \ (c, d \in K, \ cd(1 - c^4d) \neq 0). \tag{3.7}$$

Эту нормальную форму обозначим через (Ed2).

Скрученные кривые Эдвардса над полем $\mathcal{K}$ задаются уравнением

$$ax^2 + y^2 = 1 + dx^2y^2. \tag{3.8}$$

Эту нормальную форму обозначим через (CEd).

Эллиптические кривые Монтгомери над полем $\mathcal{K}$ задаются уравнением

$$by^2 = x^3 + ax^2 + x \ (a, b \in K, \ b(a^2 - 4) \neq 0). \tag{3.9}$$

Эту нормальную форму обозначим через (Mo).

Замечание 3.6. Отметим, что уравнение (CEd) бирационально эквивалентно уравнению (Mo).

3.2. Минимальные модели эллиптических кривых.

Помимо обширных арифметико-алгебраических приложений, построение минимальной модели является также промежуточным этапом при переходе от рассмотрения алгебраических кривых над полями алгебраических чисел к рассмотрению алгебраических кривых над конечными полями и кольцами.

3.2.1. Предварительные замечания.

Рассмотрим только один аспект глубокой и обширной теории минимальных моделей на примере эллиптической кривой, заданной в общей нормальной форме Вейерштрасса (EC) и определенных над полем p-адических чисел или над полем рациональных чисел.

Результатом редукции таких кривых к их минимальным моделям является, соответственно, нормальная форма Вейерштрасса (EC) с коэффициентами из кольца целых поля p-адических чисел (минимальная модель), имеющая минимальное значение p-адического показателя дискриминанта кривой, и нормальная форма Вейерштрасса (EC) с коэффициентами из кольца целых рациональных чисел, имеющая минимальный дискриминант.

При работе с минимальными моделями существенно облегчаются вычисления как некоторых характеристик исходных кривых, так и (что очень важно с прикладной точки зрения) вычисления с редукциями этих моделей над конечными полями и кольцами (в рассматриваемов случае над простыми конечными полями и кольцами вычетов).

Построение будем вести следующим образом.

В предположении, что эллиптическая кривая Γ задана над полем $\mathcal{Q}_p$ p-адических чисел (соответственно, над полем $\mathcal{Q}$ рациональных чисел) вначале исходная модель кривой Γ сводится к модели кривой Γ над кольцом $\mathcal{Z}_p$ (соответственно, над кольцом $\mathcal{Z}$), а затем осуществляется построение минимальной модели кривой Γ над кольцом $\mathcal{Z}_p$ (соответственно, над кольцом $\mathcal{Z}$).

В том случае, когда построения для полей $\mathcal{Q}_p$ и $\mathcal{Q}$ одни и те же, будем обозначать поле через $\mathcal{K} = (K, +, \cdot)$.

Замечание 3.7. Пусть p – простое число.

Целым p-адическим числом называется бесконечный ряд

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \ldots,$$

где $0 \le a_n < p$ ($n \in \mathbf{Z}_+$).

Сложение и умножение p-адических чисел

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \ldots,$$

и

$$\beta = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \ldots,$$

определяется следующим образом:

$$\alpha + \beta = c_0 + c_1 p + c_2 p^2 + \cdots + c_n p^n + \ldots,$$

где все коэффициенты c_n ($n \in \mathbf{Z}_+$) являются такими вычетами по модулю p, что

$$\begin{cases} c_0 = a_0 + b_0 - pq_0 \\ c_n = a_n + b_n + q_{n-1} - pq_n \ \ (n \in \mathbf{N}) \end{cases},$$

а

$$\alpha\beta = d_0 + d_1 p + d_2 p^2 + \cdots + d_n p^n + \ldots,$$

где все коэффициенты d_n $(n \in \mathbf{Z}_+)$ являются такими вычетами по модулю p, что

$$\begin{cases} d_0 = a_0 b_0 - ps_0 \\ d_n = \sum\limits_{k+l=n} a_k b_l + s_{n-1} - ps_n \ \ (n \in \mathbf{N}) \end{cases}.$$

В результате построено ассоциативно-коммутативное кольцо целых p-адических чисел.

Это кольцо не содержит делителей нуля (так как p – простое число). Следовательно, для него существует поле дробей $\mathcal{Q}_p$.

Это поле можно рассматривать как множество всех рядов вида

$$a_k + a_{k+1} p + a_{k+2} p^2 + \cdots + a_n p^n + \ldots,$$

где $k \in \mathbf{Z}$, а все коэффициенты a_n являются вычетами по модулю p.

При этом, если не все коэффициенты ряда равны нулю, то $a_k > 0$ (все ряды с нулевыми коэффициентами считаются тождественными и они определяют нулевой элемент поля $\mathcal{Q}_p$).

Операции сложения и умножения переносятся на эти ряды естественным образом, а единицей поля $\mathcal{Q}_p$ является такой ряд, что $a_0 = 1$, а все остальные коэффициенты равны нулю.

Обратным к элементу

$$a_k + a_{k+1} p + a_{k+2} p^2 + \cdots + a_n p^n + \ldots \ \ (a_k \neq 0)$$

является элемент

$$b_{-k} + b_{-k+1} p + a_{-k+2} p^2 + \cdots + a_n p^n + \ldots \ \ (a_k \neq 0),$$

где все коэффициенты b_n являются такими вычетами по модулю p, что

$$\begin{cases} a_k b_{-k} - ps_{-k} = 1 \\ a_k b_{-k+1} + a_{k+1} b_{-k} + s_{-k} - ps_{-k+1} = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \\ a_k b_n + a_{k+1} b_{n-1} + \cdots + a_{2k+n} b_{-k} + s_{n-1} - ps_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \end{cases}.$$

Отметим, что в поле $\mathcal{Q}_p$ те ряды

$$a_k + a_{k+1}p + a_{k+2}p^2 + \cdots + a_n p^n + \ldots,$$

для которых $k \geq 0$, образуют подкольцо, изоморфное подкольцу целых p-адических чисел.

3.2.2. Характеристики эллиптических кривых над полем.

Пусть эллиптическая кривая Γ задана над полем $\mathcal{K}$ в нормальной форме (EC):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.10}$$

где $a_1, a_2, a_3, a_4, a_6 \in K$.

С эллиптической кривой Γ, заданной уравнением (3.10), ассоциируются следующие величины $b_2, b_4, b_6, b_8, c_4, c_6$ (введенные, по-видимому, Тейтом) и выражение через них Δ_Γ и $j(\Gamma)$

$$\begin{cases} b_2 = a_1^2 + 4a_2 \\ b_4 = a_1a_3 + 2a_4 \\ b_6 = a_3^2 + 4a_6 \\ b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \\ c_4 = b_2^2 - 24b_4 \\ c_6 = -b_2^3 - 36b_2b_4 - 216b_6 \\ \Delta_\Gamma = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j(\Gamma) = c_4^3\Delta_\Gamma^{-1} \text{ (если } \Delta_\Gamma \text{ обратим)} \end{cases}. \tag{3.11}$$

Эти величины связаны, в частности, тождествами

$$\begin{cases} 4b_8 = b_2b_6 - b_4^2 \\ 1728\Delta_\Gamma = c_4^3 - c_6^2 \end{cases}. \tag{3.12}$$

В случае, когда характеристика поля $\mathcal{K}$ отлична от 2 и 3, то с помощью преобразования

$$\begin{cases} x = (12)^{-1}b_2 - z \\ y = w - 2^{-1}(a_1 z + a_3) \end{cases} \tag{3.13}$$

уравнение (EC) может быть приведено к виду

$$w^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

либо к виду

$$w^2 = z^3 - \frac{c_4}{48}z - \frac{c_6}{864},$$

где

$$\begin{cases} c_4 = 12g_2 \\ c_6 = 216g_3 \\ \Delta_\Gamma = g_2^3 - 27g_3^2 \end{cases}, \tag{3.14}$$

а величины g_2 и g_3 определяются равенствами

$$\begin{cases} g_2 = 60 \sum\limits_{\substack{l \in \Lambda \\ l \neq 0}} l^{-4} \\ g_3 = 140 \sum\limits_{\substack{l \in \Lambda \\ l \neq 0}} l^{-6} \end{cases}.$$

Пусть эллиптические кривые Γ_1 и Γ_2 заданы над полем $\mathcal{K}$ в нормальной форме (EC), а именно:

$$\Gamma_1 : \ y_1^2 + a_1^{(1)}x_1y_1 + a_3^{(1)}y_1 = x_1^3 + a_2^{(1)}x_1^2 + a_4^{(1)}x_1 + a_6^{(1)},$$

$$\Gamma_2 : \ y_2^2 + a_1^{(2)}x_2y_2 + a_3^{(2)}y_2 = x_2^3 + a_2^{(2)}x_2^2 + a_4^{(2)}x_2 + a_6^{(2)}.$$

Если $f : \Gamma_1 \to \Gamma_2$ – бирегулярное отображение (изоморфизм) между кривыми Γ_1 и Γ_2, то этот изоморфизм имеет вид

$$\begin{cases} f(x_1) = u^2 x_2 + r \\ f(y_1) = u^3 y_2 + s u^2 x_2 + t \end{cases} \quad (r, s, t \in K;\ u \in K \backslash \{0\}). \tag{3.15}$$

Формулы, связывающие коэффициенты уравнений кривых Γ_1 и Γ_2, имеют следующий вид:

1) значения коэффициентов $a_i^{(1)}$ и $a_i^{(2)}$ связаны равенствами

$$\begin{cases} a_1^{(2)} = u^{-1}(a_1^{(1)} + 2s) \\ a_2^{(2)} = u^{-2}(a_2^{(1)} - s a_1^{(1)} + 3r - s^2) \\ a_3^{(2)} = u^{-3}(a_3^{(1)} + r a_1^{(1)} + 2t) \\ a_4^{(2)} = u^{-4}(a_4^{(1)} + s a_3^{(1)} + 2r a_2^{(1)} - (t + rs) a_1^{(1)} + 3r^2 - 2st) \\ a_6^{(2)} = u^{-6}(a_6^{(1)} + r a_4^{(1)} + r^2 a_2^{(1)} + r^3 - t a_3^{(1)} - t^2 - rt a_1^{(1)}) \end{cases} ; \tag{3.16}$$

2) значения $b_i^{(1)}$ и $b_i^{(2)}$ связаны равенствами

$$\begin{cases} b_2^{(2)} = u^{-2}(b_2^{(1)} + 12rs) \\ b_4^{(2)} = u^{-4}(b_4^{(1)} + r b_2^{(1)} + 6r^2) \\ b_6^{(2)} = u^{-6}(b_6^{(1)} + 2r b_4^{(1)} + r^2 b_2^{(1)} + 4r^3) \\ b_8^{(2)} = u^{8}(b_8^{(1)} + 3r b_6^{(1)} + 3r^2 b_4^{(1)} + r^3 b_2^{(1)} + 3r^4) \end{cases} ; \tag{3.17}$$

2) значения $c_i^{(1)}$ и $c_i^{(2)}$, а также Δ_{Γ_1} и Δ_{Γ_2}, связаны равенствами

$$\begin{cases} c_4^{(2)} = u^{-4} c_4^{(1)} \\ c_6^{(2)} = u^{-6} c_6^{(1)} \\ \Delta_{\Gamma_2} = u^{-12} \Delta_{\Gamma_1} \end{cases} . \tag{3.18}$$

3.2.3. Минимальная модель.

Пусть $\mathcal{K} = \mathcal{Q}_p$.

Применив к (EC) изоморфное преобразование

$$(x, y) \mapsto (u^{-2} x, u^{-3} y)$$

с u делящимся на достаточно большую степень p, мы сводим уравнение (EC), учитывая формулы (3.16) и (3.17), к уравнению над $\mathcal{Z}_p$.

Пусть $\nu_p(\ )$ – показатель поля $\mathcal{Q}_p$.

Так как ν_p принимает дискретные значения, а после указанного выше приведения

$$\nu_p(\Delta_\Gamma) > 0.$$

то мы можем рассмотреть наименьшее положительное значение $\nu_p(\Delta_\Gamma)$.

Определение 3.1. Пусть Γ – эллиптическая кривая над полем $\mathcal{Q}_p$. Уравнение (EC) называется *минимальной моделью* для Γ относительно показателя ν_p, если $\nu_p(\Delta_\Gamma)$ принимает наименьшее возможное значение на классе изоморфных кривых с $a_1, a_2, a_3, a_4, a_6 \in \mathbf{Z}_p$.

p-адическая норма Δ_Γ называется *знаменателем* минимального дискриминанта кривой Γ в точке, соответствующей показателю ν_p.

Существует простой способ проверки минимальности модели кривой вида (EC). Во-первых, должно быть что все $a_i \in \mathbf{Z}_p$. Тогда модель минимальна, если

$$\nu_p(\Delta_\Gamma) < 12.$$

Рассмотрим теперь эллиптическую кривую Γ вида (EC) над полем $\mathcal{Q}$.

Для каждого простого числа p мы можем рассмотреть кривую $\Gamma/\mathcal{Z}_p$ и вычислить ее минимальный дискриминант $\Delta_{\Gamma/\mathcal{Z}_p}$ относительно показателя ν_p.

Определение 3.2. Минимальным дискриминантом эллиптической кривой $\Gamma/\mathcal{Q}$ называется выражение

$$\delta(\Gamma/\mathcal{Q}) = \prod_{p\ -\ \text{простое}} p^{\nu_p(\Delta_{\Gamma/\mathcal{Z}_p})}.$$

Замечание 3.8. Может показаться, что для вычисления $\delta(\Gamma/\mathcal{Q})$ необходимо перебрать все простые числа p и проводить необходимые преобразования.

Однако, ввиду конечности множества простых чисел, делящих дискриминант $\Delta_{\Gamma/\mathcal{Z}}$, величина $\delta(\Gamma/\mathcal{Q})$ всегда эффективно вычислима.

Определение 3.3. *Глобальной минимальной моделью* эллиптической кривой $\Gamma/\mathcal{Q}$ вида (EC) называется такое уравнение (EC) с коэффициентами из множества $\mathbf{Z}$, что

$$\Delta_{\Gamma/\mathcal{Z}} = \delta(\Gamma/\mathcal{Q}).$$

Истинно следующее утверждение.

Утверждение 3.2. Над полем рациональных чисел $\mathcal{Q}$ глобальная минимальная модель эллиптической кривой $\Gamma/\mathcal{Q}$ существует всегда.

3.3. Гомоморфизмы эллиптических кривых над полем комплексных чисел $\mathcal{C}$.

Исследуем связь между решетками, посредством которых задаются эллиптические кривые в нормальной форме (W) над полем комплексных чисел $\mathcal{C}$, отображениями комплексной плоскости в эллиптическую кривую, задаваемыми посредством функции Вейерштрасса решеток, групповой структурой на эллиптической кривой, гомоморфизмами и эндоморфизмади эллиптических кривых.

3.3.1. Решетки и эллиптические кривые.

Пусть эллиптическая кривая Γ представлена в нормальной форме Вейерштрасса (W):

$$y^2 = 4x^3 - g_2x - g_3 \ (g_2^3 - 27g_3^2 \neq 0).$$

Рассмотрим рациональные функции на кривой Γ и выразим через них групповую структуру на кривой Γ.

Отметим, что существует отображение $\varphi : \mathbf{C} \mapsto \Gamma$, задаваемое эллиптическими функциями:

$$z \mapsto (\wp(z), \wp'(z)) \ (= \varphi(z)).$$

Так как отображение φ задано эллиптическими функциями, то оно является периодическим, а именно:

$$\varphi(z + l) = \varphi(z) \ (l \in \Lambda)$$

где

$$\Lambda = \{m\omega_1 + n\omega_2 | m, n \in \mathbf{Z}\}$$

представляет собой решетку, по которой строится поле эллиптических функций.

Следовательно, определено отображение $\mathbf{C}/\Lambda \to \Gamma$, т.е. φ отображает тор в эллиптическую кривую.

Выразим в терминах отображения φ и эллиптических функций аддитивные алгебраические структуры на множествах $\mathbf{C}$ и $\mathbf{C}/\Lambda$.

В комплексных точках z_1, z_2 и $z_1 + z_2$ отображение φ характеризуется тем, что

$$\begin{cases} z_1 \mapsto (\wp(z_1), \wp'(z_1)) \\ z_2 \mapsto (\wp(z_2), \wp'(z_2)) \\ z_1 \mapsto (\wp(z_1 + z_2), \wp'(z_1 + z_2)) \end{cases} .$$

Найдем представление

$$\begin{cases} \wp(z_1 + z_2) = A_1(\wp(z_1), \wp'(z_1), \wp(z_2), \wp'(z_2)) \\ \wp'(z_1 + z_2) = A_2(\wp(z_1), \wp'(z_1), \wp(z_2), \wp'(z_2)) \end{cases} .$$

Полагая $x_i = \wp(z_i)$ и $y_i = \wp'(z_i)$, где $i = 1, 2$, мы приходим к задаче вычисления рациональных функций $A_1(\wp(z_1), \wp'(z_1), \wp(z_2), \wp'(z_2))$ и $A_2(\wp(z_1), \wp'(z_1), \wp(z_2), \wp'(z_2))$.

Для вывода формулы сложения эллиптических функций рассмотрим эллиптическую функцию $\mathfrak{f}$ в *параллелограмме периодов*

$$\Pi = \{a\omega_1 + b\omega_2 | 0 \le a < 1, 0 \le b < 1\},$$

определяемом решеткой Λ.

Теорема 3.1. В параллелограмме периодов число нулей эллиптической функции $\mathfrak{f}$ равно числу ее полюсов (с учетом их кратности).

Доказательство. Пусть $\mathfrak{f}$ – произвольная эллиптическая функция, определенная и непрерывная на сторонах параллелограмма Π.

Выберем точку O таким образом, чтобы на границе $\partial\Pi$ отсутствовали полюса функции $\mathfrak{f}$.

Положительный обход стороны $[0;\omega_1]$ обозначим через 1, а положительный обход стороны $[\omega_1;\omega_1+\omega_2]$ – через 2.

В силу периодичности функции $\mathfrak{f}(z)$ при положительном обходе границы $\partial\Pi$ истинно равенство

$$\int\limits_{\partial\Pi}\mathfrak{f}(z)dz=\int\limits_{1}(\mathfrak{f}(z)-\mathfrak{f}(z+\omega_2))dz+\int\limits_{2}(\mathfrak{f}(z+\omega_1)-\mathfrak{f}(z))dz=0.$$

Отсюда по формуле вычетов получаем

$$\int\limits_{\partial\Pi}\mathfrak{f}(z)dz=2\pi i\sum_j res\,\mathfrak{f}(z_j)=0,$$

т.е.

$$\sum_j res\,\mathfrak{f}(z_j)=0.$$

Обозначим через $\mathtt{n}$ число нулей, а $\mathtt{p}$ – число полюсов эллиптической функции $\mathfrak{f}(z)$.

По формуле приращения аргумента при $\mathfrak{g}(z)=\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)}$ получаем

$$\mathtt{n}-\mathtt{p}=\frac{1}{2\pi i}\int\limits_{\partial\Pi}\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)}dz=\sum_j res\,\mathfrak{g}(z_j)=0,$$

т.е.

$$\mathtt{n}=\mathtt{p}.$$

□

Теорема 3.2. Пусть $\alpha_1,\dots\alpha_{\mathtt{n}}$ – нули, а $\beta_1,\dots,\beta_{\mathtt{n}}$ – полюса эллиптической функции в параллелограмме периодов Π. Тогда

$$\sum_{j=1}^{\mathtt{n}}\alpha_j=\sum_{j=1}^{\mathtt{n}}\beta_j\,(mod\,\Lambda).$$

Доказательство. Предположим, что на границе параллелограмма периодов Π нет ни нулей, ни полюсов эллиптической функции $\mathfrak{f}(z)$ (что всегда можно получить за счет выбора точки O).

Тогда истинно равенство

$$\frac{1}{2\pi i}\int\limits_{\partial\Pi} z\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)}dz = \alpha_1 + \cdots + \alpha_{\mathtt{n}} - (\beta_1 + \cdots + \beta_{\mathtt{n}}),$$

где $\alpha_1, \ldots \alpha_{\mathtt{n}}$ – нули, а $\beta_1, \ldots, \beta_{\mathtt{n}}$ – полюса эллиптической функции $\mathfrak{f}(z)$.

Так как

$$(z+\omega_1)\frac{\mathfrak{f}'(z+\omega_1)}{\mathfrak{f}(z+\omega_1)} - z\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)} = \omega_1\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)},$$

то

$$\frac{1}{2\pi i}\left(\int\limits_0^{\omega_2}(z+\omega_1)\frac{\mathfrak{f}'(z+\omega_1)}{\mathfrak{f}(z+\omega_1)}dz - \int\limits_{\omega_1}^{\omega_1+\omega_2} z\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)}dz\right) =$$

$$= \frac{1}{2\pi i}\int\limits_0^{\omega_2}\omega_1\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)}dz = \omega_1\frac{1}{2\pi i}\int\limits_0^{\omega_2}\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)}dz = \omega_1\frac{1}{2\pi i}\int\limits_0^{\omega_2} d\ln\mathfrak{f}(z) =$$

$$= \omega_1\frac{1}{2\pi i}2\pi i\int\limits_{C_1} dn = \omega_1 n,$$

где n – число оборотов вокруг начала координат замкнутого контура C_1, который пробегает $\mathfrak{f}(z)$ при прохождении переменной z в положительном направлении стороны $[0, \omega_2]$ параллелограмма Π. Здесь следует учесть, что

$$\mathfrak{f}(0) = \mathfrak{f}(\omega_2).$$

А так как

$$(z+\omega_2)\frac{\mathfrak{f}'(z+\omega_2)}{\mathfrak{f}(z+\omega_2)} - z\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)} = \omega_2\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)},$$

то

$$\frac{1}{2\pi i}\left(\int\limits_0^{\omega_1}(z+\omega_2)\frac{\mathfrak{f}'(z+\omega_2)}{\mathfrak{f}(z+\omega_2)}dz - \int\limits_{\omega_2}^{\omega_1+\omega_2} z\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)}dz\right) =$$

$$= \frac{1}{2\pi i}\int\limits_0^{\omega_1} \omega_2 \frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)}dz = \omega_2 \frac{1}{2\pi i}\int\limits_0^{\omega_1} \frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)}dz = \omega_2 \frac{1}{2\pi i}\int\limits_0^{\omega_1} d\ln \mathfrak{f}(z) =$$

$$= \omega_2 \frac{1}{2\pi i} 2\pi i \int\limits_{C_2} dm = \omega_2 m,$$

где m – число оборотов вокруг начала координат замкнутого контура C_2, который пробегает $\mathfrak{f}(z)$ при прохождении переменной z в положительном направлении стороны $[0, \omega_1]$ параллелограмма Π. Здесь следует учесть, что

$$\mathfrak{f}(0) = \mathfrak{f}(\omega_1).$$

Таким образом,

$$\frac{1}{2\pi i}\int\limits_{\partial\Pi} z\frac{\mathfrak{f}'(z)}{\mathfrak{f}(z)}dz = \omega_1 n + \omega_2 m,$$

и, следовательно,

$$\alpha_1 + \cdots + \alpha_{\mathtt{n}} = (\beta_1 + \cdots + \beta_{\mathtt{n}}) + \omega_1 n + \omega_2 m.$$

А так как $\omega_1 n + \omega_2 m \in \Lambda$, то

$$\sum_{j=1}^{\mathtt{n}} \alpha_j = \sum_{j=1}^{\mathtt{n}} \beta_j \; (mod\, \Lambda).$$

□

Рассмотрим теперь функцию

$$f(z) = a\wp(z) + b\wp'(z) + c,$$

линейно зависящую от эллиптических функций $\wp$ и $\wp'$, которая в точках z_1 и z_2 обращается в нуль, т.е.

$$f(z_1) = f(z_2) = 0.$$

По определению эллиптической фушкции Вейерштрасса $\wp(z)$, она имеет полюс порядка 2 в точке $z = 0$. Следовательно, ее производная имеет в точке $z = 0$ полюс порядка 3.

Нули z_1 и z_2 являются нулями 1-го порядка. Следовательно, по теореме 3.1, функция $f(z)$ имеет еще один нуль z_3. А из теоремы 3.2 вытекает, что

$$z_1 + z_2 + z_3 \equiv 0 \, (mod\, \Lambda).$$

Применим эти результаты к эллиптической кривой, представленной в нормальной форме Вейерштрасса (W):

$$y^2 = 4x^3 - g_2x - g_3.$$

Перейдя к обозначениям $x = \wp(z)$ и $y = \wp'(z)$, условие прохождения прямой

$$ay + bx + c = 0$$

через точки (x_1, y_1) и (x_2, y_2) запишем в виде

$$y = \frac{y_1 - y_2}{x_1 - x_2}x + \frac{y_2x_1 - y_1x_2}{x_1 - x_2}.$$

Подставляя правую часть этого равенства вместо y в уравнение (W), из указанных выше теорем и формул Виетта получим

$$x_1 + x_2 + x_3 = \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2,$$

т.е.

$$x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2.$$

Аналогичным образом показывается, что

$$y_3 = y_1 + \frac{y_1 - y_2}{x_1 - x_2}(x_3 - x_1).$$

Таким образом, мы вывели формулы сложения точек абелевой группы эллиптической кривой, представленной в нормальной форме Вейерштрасса (W).

3.3.2. Представления гомоморфизмов эллиптических кривых.

Отображение одной эллиптической кривой в другую может быть задано либо в виде гомоморфизма решеток (при задании эллиптических кривых посредством решеток), либо (при использовании теоремы Римана-Роха) линейными заменами переменных вида

$$\begin{cases} x_2 = u^2 x_1 + r \\ y_2 = u^3 y_1 + s u^2 x_1 + t \end{cases} \quad (r, s, t \in K;\ u \in K \backslash \{0\}),$$

где $\mathcal{K} = (K, +, \cdot)$ – поле определения эллиптической кривой.

А так как эллиптические кривые (при добавлении к ним бесконечно удаленной точки) являются алгебраическими группами, то для сохранения групповой структуры отображение одной эллиптической кривой в другую должно отображать нейтральный элемент в нейтральный элемент.

Пример 3.1. Несложно показать, что эллиптические кривые

$$y^2 = x^3 + a_1 x + b_1$$

и

$$y^2 = x^3 + a_2 x + b_2$$

бирационально изоморфны тогда и только тогда, когда

$$\begin{cases} a_2 = c^4 a_1 \\ b_2 = c^6 b_1 \end{cases}.$$

Из формул сложения точек эллиптической кривой вытекает, что эндоморфизмами эллиптической кривой являются умножения точек на целое число (такие эндоморфизмы называются *тривиальными*).

Более того, эллиптическая кривая может иметь в качестве эндоморфизмов комплексные умножения, т.е. эндоморфизмы, соответствующие умножению точек на комплексные числа.

Однако, умножение точек не на каждое комплексное число является эндоморфизмом эллиптической кривой.

Пример 3.2. Пусть эллиптическая кривая задана решеткой

$$\Lambda = \{n + m\tau | n, m \in \mathbf{Z}\},$$

где $\tau \in \mathbf{C}$ – фиксированное комплексное число.

Предположим, что умножение точек на комплексное число $z = a + b\tau$ является эндоморфизмом эллиптической кривой.

Из равенства

$$z(n + m\tau) = n_1 + m_1\tau$$

вытекает, что комплексное число τ является корнем квадратного уравнения

$$bm\tau^2 + (bn + am - m_1)\tau + (an - n_1) = 0.$$

Если эллиптическая кривая рассматривается над полем $\mathcal{Q}$ рациональных чисел, то комплексное число τ должно принадлежать мнимому квадратному расширению поля $\mathcal{Q}$, а z должно быть элементом кольца целых над этим расширением.

Ясно, что указанными свойствами обладают не все комплексные числа $z \in \mathbf{C}$.

3.4. Степень отображения и ее применения.

Рассмотрим ту роль, которую играет понятие «степень рационального отображения» при исследовании морфизмов алгебраических кривых.

3.4.1. Основные понятия.

Общая схема исследования морфизмов многообразий основана на следующей конструкции.

Для расширения $\mathcal{E}$ поля $\mathcal{F}$ обозначим через $[\mathcal{E} : \mathcal{F}]$ – *степень* поля $\mathcal{E}$, т.е. размерность $\mathcal{E}$ как векторного пространства над $\mathcal{F}$.

Пусть X и Y – многообразия , определенные над полем $\mathcal{K} = (K, +, \cdot)$ (такое поле называется *основным полем* или *полем определения*).

Зафиксируем рациональное отображение $\varphi : X \to Y$.

Для любого множества Z отображение φ определяет следующее отображение φ^* множества всех отображений вида $Y \to Z$ во множество всех отображений вида $X \to Z$: для любого отображения $u : Y \to Z$

$$\varphi^*(u) = \varphi \circ u$$

где « ∘» – операция суперпозиции отображений.

Ясно, что гомоморфизмы (в частности, изоморфизмы) алгебраических структур, определенных на многообразии X, в алгебраические структуры, определенные на многообразие Y, представляют собой отображения вида $\varphi^* : \mathcal{K}(Y) \to \mathcal{K}(X)$, удовлетворяющие тем или иным условиям.

Степень отображения $\varphi \in \mathcal{K}(X)$ (обозначается $\deg \varphi$) определяется следующим образом

$$\deg \varphi = \begin{cases} 0, & \text{если } \dim \varphi(X) < \dim X \\ [\mathcal{K}(X) : \varphi^*(\mathcal{K}(\varphi(X))], & \text{если } \dim \varphi(X) = \dim X \end{cases},$$

где $\dim V$ – размерность многообразия V.

Охарактеризуем структуру кольца морфизмов абелевых групп, определенных на эллиптических кривых.

Известно, что если $\varphi : \Gamma_1 \to \Gamma_2$ – рациональное отображение неприводимых проективных алгебраических кривых Γ_1 и Γ_2, то $\varphi(\Gamma_1)$ или точка, или вся кривая Γ_2.

В последнем случае для полей $\mathcal{K}(\Gamma_1)$ и $\mathcal{K}(\Gamma_2)$ степень расширения $[\mathcal{K}(\Gamma_1) : \varphi^*(\mathcal{K}(\Gamma_2))]$ меньше бесконечности, т.е. $\mathcal{K}(\Gamma_1)$ является конечным расширением поля $\varphi^*(\mathcal{K}(\Gamma_2))$, причем отображение φ^* определяет вложение поля $\varphi^*(\mathcal{K}(\Gamma_2))$ в поле $\mathcal{K}(\Gamma_1)$.

Отсюда вытекает корректность следующего определения.

Определение 3.4. Степень $\deg \varphi$ рационального отображения алгебраической кривой Γ_1 в алгебраическую кривую Γ_2 определяется равенством

$$\deg \varphi = [\mathcal{K}(\Gamma_1) : \varphi^*(\mathcal{K}(\Gamma_2))].$$

3.4.2. Гомоморфизмы эллиптических кривых.

Пусть Γ_1 и Γ_2 – проективные эллиптические кривые.

Рациональное отображение $\varphi : \Gamma_1 \to \Gamma_2$ является:

1) гомоморфизмом абелевых групп $\mathfrak{G}_{\Gamma_1}$ и $\mathfrak{G}_{\Gamma_2}$ тогда и только тогда, когда $\varphi(\mathcal{O}_{\Gamma_1}) = \mathcal{O}_{\Gamma_2}$, т.е. когда нейтральный элемент группы $\mathfrak{G}_{\Gamma_1}$ отображается на нейтральный элемент группы $\mathfrak{G}_{\Gamma_2}$;

2) *сепарабельным* тогда и только тогда, когда сепарабельно расширение $[\mathcal{K}(\Gamma_1) : \varphi^*(\mathcal{K}(\Gamma_2))]$.

Замечание 3.9. Пусть $\mathcal{K} = (K, +, \cdot)$ – произвольное поле.

Неразложимый многочлен $h(x) \in K[x]$ называется *сепарабельным*, если $\mathsf{D}h(x)$ – ненулевой многочлен.

В поле $\mathcal{K}$ характеристики 0 каждый неразложимый многочлен $h(x) \in K[x]$ положительной степени является сепарабельным, а в поле $\mathcal{K}$ характеристики $p > 0$ неразложимый многочлен $h(x) \in K[x]$ является сепарабельным тогда и только тогда, когда $h(x) \notin K[x^p]$.

Произвольный многочлен $f(x) \in K[x]$ называется *сепарабельным*, если сепарабельны все его неразложимые множители.

Пусть $\mathcal{F} = (F, +, \cdot)$ – расширение поля $\mathcal{K} = (K, +, \cdot)$. Приведенный неразложимый (в кольце $\mathcal{K}[x]$) многочлен $f(x) \in K[x]$, корнем которого является элемент $a \in F$, называется *минимальным многочленом* элемента a в $\mathcal{K}[x]$ (или, иными словами, над полем $\mathcal{K}$).

Элемент $a \in F$ называется сепарабельным над полем $\mathcal{K}$ тогда и только тогда, когда сепарабелен его минимальный многочлен над полем $\mathcal{K}$.

Расширение $\mathcal{F}$ поля $\mathcal{K}$ называется сепарабельным, если каждый элемент $a \in F$ сепарабелен над полем $\mathcal{K}$.

Пусть Γ_1 и Γ_2 – эллиптические кривые.

Обозначим через $\mathtt{Hom}(\Gamma_1, \Gamma_2)$ множество всех гомоморфизмов абелевой группы $\mathfrak{G}_{\Gamma_1}$ в абелеву группу $\mathfrak{G}_{\Gamma_2}$. Истинна следующая теорема.

Теорема 3.3. Если $\varphi \in \mathtt{Hom}(\Gamma_1, \Gamma_2)$ – сепарабельный гомоморфизм, то

$$\deg \varphi = |\ker \varphi|,$$

а дифференциал $\mathsf{d}_{\mathbf{x}}\varphi$ является изоморфизмом касательных пространств $\Theta_{\mathbf{x},\Gamma_1}$ и $\Theta_{\varphi(\mathbf{x}),\Gamma_2}$ для любой точки $\mathbf{x} \in \Gamma_1$.

Если же $\varphi \in \mathtt{Hom}(\Gamma_1, \Gamma_2)$ $(\varphi \neq 0)$ – несепарабельный гомоморфизм, то он может быть представлен в виде

$$\varphi = \varphi_0 \circ \pi^h \ (h \in \mathbf{N}),$$

где $\varphi_0 \in \mathtt{Hom}(\Gamma_1, \Gamma_2)$ – сепарабельный гомоморфизм, а π – гомоморфизм Фробениуса.

Замечание 3.10. Пусть $\mathcal{K} = (K, +, \cdot)$ – произвольное поле.

Отображением Фробениуса называется отображение

$$\pi^h : K^n \to K^n \ (n, h \in \mathbf{N}),$$

определенное равенством

$$\pi^h(x_1, \ldots, x_n) = (x_1^h, \ldots, x_n^h).$$

Одно из основных применений этого отображения состоит в следующем.

Рассмотрим над полем $\mathcal{R} = (\mathbf{R}, +, \cdot)$ действительных чисел такое произвольное многообразие

$$V = V(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in \mathbf{R}^n | f_i(a_1, \ldots, a_n) = 0 \text{ для всех } i = 1, \ldots, m\},$$

что $f_1, \ldots f_m \in \mathbf{Z}[x_1, \ldots, x_n]$.

Точки многообразия, координаты которых принадлежат полю $\mathcal{GF}(p^k)$ ($k \in \mathbf{N}$, а p – простое число) являются неподвижными точками отображения π^{p^k}.

Когда отображение π^h рассматривается как гомоморфизм абелевой группы $\mathfrak{G}_{\Gamma_1}$ в абелеву группу $\mathfrak{G}_{\Gamma_2}$, то отображение π^h доопределяется в бесконечно удаленной точке равенством

$$\pi^h(\mathcal{O}_{\Gamma_1}) = \mathcal{O}_{\Gamma_2}.$$

3.4.3. Кольцо эндоморфизмов эллиптической кривой.

Если $\varphi \in \mathtt{Hom}(\Gamma_1, \Gamma_2)$ и $\psi \in \mathtt{Hom}(\Gamma_2, \Gamma_3)$, то определена композиция $\psi \circ \varphi \in \mathtt{Hom}(\Gamma_1, \Gamma_3)$.

В частности, в случае, когда

$$\Gamma_1 = \Gamma_2 = \Gamma_3 = \Gamma,$$

мы получаем кольцо эндоморфизмов (т.е. гомоморфизмов в себя)

$$\mathcal{ENDO}(\Gamma) = (\mathtt{End}(\Gamma), +, \circ) \ (\mathtt{End}(\Gamma) = \mathtt{Hom}(\Gamma, \Gamma))$$

абелевой группы $\mathfrak{G}_\Gamma$.

Пусть $\varphi \in \mathtt{End}(\Gamma)$. Положим $\nu(\varphi) = \deg \varphi$. Из вышеизложенного вытекает, что $\nu(\varphi) > 0$, если $\varphi \neq 0$ и $\nu(0) = 0$.

Ясно, что ν – мультипликативная функция, т.е.

$$\nu(\varphi \circ \varphi) = \nu(\varphi) \cdot \nu(\varphi).$$

Истинна следующая теорема.

Теорема 3.4. На аддитивной группе $(\mathtt{End}(\Gamma), +)$ кольца $\mathcal{ENT}(\Gamma)$ существует такое скалярное произведение (φ, ψ), что

$$(\varphi, \varphi) = \nu(\varphi).$$

Указанное в теореме 3.11 скалярное произведение определяется равенством

$$(\varphi, \psi) = \frac{1}{2}(\nu(\varphi + \psi) - \nu(\varphi) - \nu(\psi)) \ (\varphi, \psi \in \mathtt{End}(\Gamma)).$$

Существование этого скалярного произведения дает возможность описать структуру кольца $\mathcal{ENT}(\Gamma)$.

Исследуем вначале характеристический многочлен эндоморфизма.

Пусть $\varphi \in \mathtt{End}(\Gamma)$ и $n \in \mathbf{Z}$. Тогда

$$\nu(\varphi - n) = (\varphi - n, \varphi - n) = n^2 - 2n(\varphi, \varepsilon) + \nu(\varphi) = h_\varphi(n), \qquad (3.19)$$

где ε – единица кольца $\mathcal{ENT}(\Gamma)$.

Целое число $2(\varphi, \varepsilon)$ называется *следом* эндоморфизма φ и обозначается $sp(\varphi)$.

Таким образом,

$$h_\varphi(x) = x^2 - sp(\varphi) \cdot x + \nu(\varphi).$$

Из (3.19) вытекает, что истинна следующая теорема.

Теорема 3.5. Эндоморфизм φ является корнем своего характеристического многочлена, т.е.

$$h_\varphi(\varphi) = 0.$$

Покажем, что для произвольного приведенного разложимого многочлена с целыми коэффициентами (такие многочлены называются *унитальными* многочленами)

$$g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

истинна формула

$$\nu(g(\varphi)) = \prod_{i=1}^{n} h_\varphi(\alpha_i) = \mathrm{Res}(h_\varphi, g, \varphi),$$

где α_i $(i = 1, \ldots, n)$ – корни многочлена g.

Пусть

$$g(x) = x - b.$$

Тогда

$$\mathrm{Res}(h_\varphi, g, x) = \det(\mathrm{Syl}(h_\varphi, g, x)) =$$

$$= \begin{vmatrix} 1 & 0 & 1 \\ -b & 1 & -sp(\varphi) \\ 0 & -b & \nu(\varphi) \end{vmatrix} = b^2 - bsp(\varphi) + \nu(\varphi).$$

Следовательно,

$$\mathrm{Res}(h_\varphi, g, x) = h_\varphi(b). \tag{3.20}$$

Из (3.20) вытекает, что для произвольного унитального многочлена

$$g(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

истинно равенство

$$\nu(g(x)) = \nu(\prod_{i=1}^{n}(x - \alpha_i)) = \prod_{i=1}^{n} h_\varphi(\alpha_i),$$

что и требовалось показать.

Основной результат о кольце изоморфизмов $\mathcal{ENP}(\Gamma)$ содержится в следующей теореме.

Теорема 3.6. Для кольца эндоморфизмов $\mathcal{ENP}(\Gamma)$ имеет место одна из следующих трех ситуаций:

1) кольцо $\mathcal{ENP}(\Gamma)$ изоморфно кольцу $\mathcal{Z}$ целых чисел;

2) кольцо $\mathcal{ENP}(\Gamma)$ изоморфно некоторому мнимому квадратичному полю, т.е. некоторому подполю поля $\mathcal{C}$ комплексных чисел;

3) кольцо $\mathcal{ENP}(\Gamma)$ изоморфно некоторой алгебре кватернионов.

Замечание 3.11. Последняя ситуация, указанная в теореме 3.6 реализуется только в полях характеристики $p > 0$ (p – простое число).

3.5. Изогении.

Рассмотрим связь между ненулевыми гомоморфизмами эллиптических кривых (такие гомоморфизмы называют *изогениями*), группой дивизоров эллиптической кривой, соответствующей ей группой Пикара, а также обобщение этой связи на неособые алгебраические кривые рода g, большего, чем 1.

3.5.1. Основные понятия.

Гомоморфизм (морфизм) абелевой группы $\mathcal{G}_1 = (G_1, +_1)$ в абелеву группу $\mathcal{G}_2 = (G_2, +_2)$ называется *изогенией*, если он имеет конечные ядро и коядро.

Замечание 3.12. Охарактеризуем понятия *ядро* и *коядро* морфизма в терминах теории категорий.

В любой категории $\mathcal{A}$ запись $A \xrightarrow{f} B$ означает утверждение «$f \in \mathtt{Mor}(A, B)$».

В любой категории для каждого морфизма $A \xrightarrow{f} B$ и каждого объекта C *индуцированный морфизм* $\mathtt{Mor}(B, C) \to \mathtt{Mor}(A, C)$ (его также называют *обращением стрелки*) определен правилом $g \mapsto g \circ f$ ($g \in \mathtt{Mor}(B, C)$).

Копроизведением семейства объектов $\{A_i\}_{i \in I}$ называется пара

$$(S, \{f_i\}_{i \in I}),$$

где S – объект, а $\{A_i \xrightarrow{f_i} S | i \in I\}$ – такое семейство морфизмов, что для любого объекта C и каждого семейства морфизмов $\{A_i \xrightarrow{g_i} C | i \in I\}$ существует единственный такой морфизм $S \xrightarrow{h} C$, что

$$h \circ f_i = g_i$$

для всех $i \in I$.

Известно, что копроизведения в категории групп существуют, а копроизведения в категории абелевых групп представляют собой, по своей сути, *прямые суммы* абелевых групп.

Категория абелевых групп относится к классу *аддитивных категорий*, т.е категорий, объектами которых являются алгебраические системы, построенные на основе абелевых групп. Формально последние определяются следующим образом.

Категория $\mathcal{A}$ называется *аддитивной*, если она удовлетворяет следующим четырем аксиомам:

A1: $\mathcal{MOR}(A, B) = (\mathtt{Mor}(A, B), +)$ является абелевой группой для каждой пары объектов A и B;

A2: закон композиции морфизмов билинеен (напомним, что билинейное отображение называется *спариванием*);

A3: существует *нулевой объект* 0, т.е. такой объект, что как множество $\mathtt{Mor}(A, 0)$, так и множество $\mathtt{Mor}(0, A)$ состоит из одного элемента для любого объекта A;

A4: в категории $\mathcal{A}$ существуют конечные произведения и копроизведения объектов.

В аддитивной категории последовательность морфизмов

$$A_1 \stackrel{f_1}{\to} A_2 \stackrel{f_2}{\to} \ldots \stackrel{f_{n-2}}{\to} A_{n-1} \stackrel{f_{n-1}}{\to} A_n \ (n \geq 3)$$

называется *точной*, если образ f_i совпадает с ядром f_{i+1} для всех $i = 1, \ldots, n-2$.

Известно, что в аддитивной категории истинны следующие два утверждения:

1) для всякой точной последовательности морфизмов

$$A \stackrel{f}{\to} B \stackrel{g}{\to} C \to 0$$

индуцированная последовательность

$$\mathtt{Mor}(A, D) \leftarrow \mathtt{Mor}(B, D) \leftarrow \mathtt{Mor}(C, D) \leftarrow 0$$

является точной;

2) для всякой точной последовательности морфизмов

$$0 \to A \stackrel{f}{\to} B \stackrel{g}{\to} C$$

индуцированная последовательность

$$0 \to \mathtt{Mor}(D, A) \to \mathtt{Mor}(D, B) \to \mathtt{Mor}(D, C)$$

является точной.

В аддитивной категории для морфизма $A \stackrel{f}{\to} B$:

1) *ядром* называется такой морфизм $C \stackrel{g}{\to} A$, что для каждого объекта X точной является индуцированная последовательность

$$0 \to \mathtt{Mor}(X, C) \to \mathtt{Mor}(X, A) \to \mathtt{Mor}(X, B);$$

2) *коядром* называется такой морфизм $B \xrightarrow{g} C$, что для каждого объекта X точной является индуцированная последовательность

$$\mathtt{Mor}(A, X) \leftarrow \mathtt{Mor}(B, X) \leftarrow \mathtt{Mor}(C, X) \leftarrow 0.$$

Известно, что если в аддитивной категории существуют ядра и коядра, то они единственны с точностью до изоморфизма.

Отметим, что категория абелевых групп (а также комплексы модулей и категория векторных пространств), кроме перечисленных выше четырех аксиом аддитивной категории, удовлетворяет также следующим трем аксиомам:

A5: существуют ядра и коядра морфизмов;

A6: если ядром морфизма $A \xrightarrow{f} B$ является 0, то f является ядром своего коядра;

A7: если коядром морфизма $A \xrightarrow{f} B$ является 0, то f является коядром своего ядра.

Категории, удовлетворяющие аксиомам A1 - A7 называются *абелевыми*.

Абелевы группы $\mathcal{G}_1 = (G_1, +_1)$ и $\mathcal{G}_2 = (G_2, +_2)$ называются *изогенными*, если существует такая абелева группа $\mathcal{G} = (G, +)$, что морфизмы $\varphi : G \to G_1$ и $\psi : G \to G_2$ являются изогениями.

Если φ – гомоморфизм абелевой группы $\mathcal{G}_1 = (G_1, +_1)$ в абелеву группу $\mathcal{G}_2 = (G_2, +_2)$, то будем писать

$$\mathcal{G}_1 \xrightarrow{\varphi} \mathcal{G}_2.$$

Говорят, что последовательность абелевых групп

$$\mathcal{G}_1 \xrightarrow{\varphi} \mathcal{G}_2 \xrightarrow{\psi} \mathcal{G}_3$$

является *точной с точностью до изогении*, если пересечение образа гомоморфизма φ и ядра гомоморфизма ψ является изогенией.

Замечание 3.13. Отношение изогении является отношением эквивалентности на множестве всех абелевых групп.

3.5.2. Изогении эллиптических кривых.

Так как каждой эллиптической кривой Γ соответствует абелева группа $\mathfrak{G}_\Gamma = (\Gamma \cup \{\mathcal{O}\}, +_{\mathfrak{G}_\Gamma})$, а для двух эллиптических кривых может быть

определен морфизм, являющийся морфизмом соответствующих абелевых групп, то можно говорить об *изогениях эллиптических кривых*.

Любой ненулевой гомоморфизм эллиптических кривых является изогенией. Из ранее изложенных результатов о рациональных отображениях эллиптических кривых, вытекает, что изогения является конечным отображением.

Замечание 3.14. Напомним, что отображение алгебраических кривых называется *конечным*, если конечна его степень.

Пусть Γ_1 и Γ_2 – такие эллиптические кривые, что

$$\mathfrak{G}_{\Gamma_1} \xrightarrow{\varphi} \mathfrak{G}_{\Gamma_2},$$

где φ – изогения эллиптических кривых (далее будем просто говорить «изогения»). Тогда определено вложение

$$\varphi^* : \overline{\mathcal{K}}(\Gamma_2) \to \overline{\mathcal{K}}(\Gamma_1)$$

полей функций, где $\overline{\mathcal{K}}$ – алгебраическое замыкание поля $\mathcal{K}$.

Изогении определяют конечные подгруппы группы $\mathfrak{G}_{\Gamma(\overline{\mathcal{K}})}$ и сами определяются ими. Истинна следующая теорема.

Теорема 3.7. Пусть Γ – эллиптическая кривая, а $\widetilde{\mathfrak{G}}_\Gamma = (G, +)$ – конечная подгруппа группы $\mathfrak{G}_\Gamma$. Тогда существует такая единственная с точностью до изоморфизма эллиптическая кривая Γ_1, что

$$\mathfrak{G}_\Gamma \xrightarrow{\varphi} \mathfrak{G}_{\Gamma_1},$$

где φ – сепарабельная изогения, и

$$\ker \varphi = G.$$

Пусть Γ_1 и Γ_2 – такие эллиптические кривые, что

$$\mathfrak{G}_{\Gamma_1} \xrightarrow{\varphi} \mathfrak{G}_{\Gamma_2},$$

где φ – изогения. Тогда существует такая *двойственная* изогения $\widehat{\varphi}$, что

$$\mathfrak{G}_{\Gamma_2} \xrightarrow{\widehat{\varphi}} \mathfrak{G}_{\Gamma_1}.$$

Замечание 3.15. Для формулировки свойств двойственной изогении, нам понадобятся следующие понятия.

Пусть Γ – эллиптическая кривая над алгебраически замкнутым полем $\mathcal{K}$.

Группой дивизоров на кривой Γ называется свободная абелева группа

$$\mathcal{DIV}(\Gamma) = (Div(\Gamma), +),$$

порожденная элементами множества $\Gamma \cup \{\mathcal{O}\}$.

Таким образом, каждый дивизор $D \in Div(\Gamma)$ представляет собой формальную сумму

$$D = \sum_{P \in \Gamma \cup \{\mathcal{O}\}} n(P) \cdot P,$$

в которой равны нулю почти все коэффициенты $n(P)$ (их также обозначают n_P).

Величина

$$deg(D) = \sum_{P \in \Gamma \cup \{\mathcal{O}\}} n(P)$$

называется *степенью* дивизора D.

Дивизор, у которого все коэффициенты неотрицательны называется *эффективным.*

Дивизоры степени 0 образуют подгруппу

$$\mathcal{DIV}^{(0)}(\Gamma) = (Div^{(0)}(\Gamma), +)$$

группы $\mathcal{DIV}(\Gamma)$.

Каждому рациональному отображению f, определенному на множестве $\Gamma \cup \{\mathcal{O}\}$, может быть сопоставлен дивизор

$$div(f) = \sum_{P \in \Gamma \cup \{\mathcal{O}\}} ord_P(f) \cdot P, \tag{3.21}$$

где $ord_P(f)$ – порядок отображения f в точке P.

Дивизоры, определяемые равенством (3.21) называются *главными.*

Нетрудно понять, что главные дивизоры образуют подгруппу группы $\mathcal{DIV}(\Gamma)$.

Дивизоры $D_1, D_2 \in Div(\Gamma)$ называются *линейно эквивалентными* (обозначается, $D_1 \sim D_2$), если существует такое рациональное отображение, определенное на множестве $\Gamma \cup \{\mathcal{O}\}$, что

$$D_1 - D_2 = div(f).$$

Группой Пикара $\mathcal{PIC}(\Gamma)$ эллиптической кривой Γ называется фактор-группа группы $\mathcal{DIV}(\Gamma)$ по подгруппе главных дивизиров.

Обозначим через $\mathcal{PIC}^{(0)}(\Gamma)$ фактор-группу группы дивизоров степени 0 по подгруппе главных дивизиров.

Пусть Γ_1 и Γ_2 – такие эллиптические кривые, что

$$\mathfrak{G}_{\Gamma_1} \xrightarrow{\varphi} \mathfrak{G}_{\Gamma_2},$$

где φ – изогения. Последняя индуцирует отображение групп

$$\varphi^* : \mathcal{PIC}^{(0)}(\Gamma_2) \to \mathcal{PIC}^{(0)}(\Gamma_1).$$

С другой стороны существуют изоморфизмы групп

$$\mathfrak{G}_{\Gamma_i} \xrightarrow{\psi_i} \mathcal{PIC}^{(0)}(\Gamma_i) \ (i = 1, 2),$$

определяемые формулой

$$P \to (P) - (0),$$

где P – класс дивизора, содержащего точку P, а (0) – класс нейтрального элемента группы $\mathfrak{G}_{\Gamma_i}$.

Вышеуказанные группы и отображения между ними определяют последовательность отображений

$$\mathfrak{G}_{\Gamma_2} \xrightarrow{\psi_2} \mathcal{PIC}^{(0)}(\Gamma_2) \xrightarrow{\varphi^*} \mathcal{PIC}^{(0)}(\Gamma_1) \xrightarrow{\psi_1^{-1}} \mathfrak{G}_{\Gamma_1}.$$

Если $Q \in \mathfrak{G}_{\Gamma_2}$, то

$$\psi_1^{-1} \circ \varphi^* \circ \psi_2(Q) = [deg\varphi]P,$$

где $[m]$ – изогения умножения на m в группе точек эллиптической кривой.

Основной результат о двойственной изогении содержится в следующей теореме.

Теорема 3.8. Пусть $\mathfrak{G}_{\Gamma_1} \xrightarrow{\varphi} \mathfrak{G}_{\Gamma_2}$, где φ есть изогения степени m эллиптических кривых Γ_1 и Γ_2. Тогда:

1) существует единственная такая изогения $\widehat{\varphi}$, что

$$\mathfrak{G}_{\Gamma_2} \xrightarrow{\widehat{\varphi}} \mathfrak{G}_{\Gamma_1},$$

$$\widehat{\widehat{\varphi}} = \varphi,$$

и

$$\widehat{\varphi} \circ \varphi = [m];$$

2) как групповой гомоморфизм изогения $\widehat{\varphi}$ является композицией отображений

$$\Gamma_2 \cup \{\mathcal{O}_{\Gamma_2}\} \xrightarrow{r} Div^{(0)}(\Gamma_2) \xrightarrow{\varphi^*} Div^{(0)}(\Gamma_1) \xrightarrow{s} \Gamma_1 \cup \{\mathcal{O}_{\Gamma_1}\},$$

где отображения r и s определяются формулами

$$r(Q) = (Q) - (0),$$

$$s\left(\sum n_P \cdot (P)\right) = \sum [n_P] \circ P.$$

3.5.3. Изогении неособых алгебраических кривых рода $g > 1$.

Рассмотрим теперь известное обобщение результатов об изогениях и группе Пикара на неособую проективную кривую C рода $g > 1$.

Для кривой C обычным образом определяются дивизоры, главные дивизоры, группа дивизоров

$$\mathcal{DIV}(C) = (Div(C), +)$$

и ее подгруппа

$$\mathcal{DIV}^{(0)}(C) = (Div^{(0)}(C), +)$$

дивизоров степени 0.

Известными способами (см., напр., [27]) с неособой проективной кривой C рода $g > 1$ над полем комплексных чмсел сопоставляется риманова поверхность S рода g и якобиево многообразие $J(C)$.

Построение группы Пикара $\mathcal{PIC}(C)$ кривой C основано на использовании якобиевого многообразия (Якобиана) $J(C)$ кривой C.

Пусть S есть компактная риманова поверхность рода g.

На римановой поверхности S обычным образом определяются дивизоры, главные дивизоры, группа дивизоров

$$\mathcal{DIV}(S) = (Div(S), +)$$

и ее подгруппа

$$\mathcal{DIV}^{(0)}(S) = (Div^{(0)}(S), +)$$

дивизоров степени 0.

С римановой поверхностью S связана группа 1-циклов $\mathcal{H}_1(S, \mathbf{Z})$ с каноническим базисом

$$c_1, \ldots, c_{2g}$$

и пространство голоморфных 1-форм $\mathcal{H}^{(0)}(S, \Omega^{(1)})$, порожденное голоморфными формами

$$\omega_1, \ldots, \omega_g.$$

Векторы

$$\Pi_i = \left(\int\limits_{c_i} \omega_1, \ldots, \int\limits_{c_i} \omega_g \right) \in \mathbf{C}^g \ (i = 1, \ldots, 2g)$$

называются периодами.

Решетка периодов Λ порождается $2g$ периодами Π_i $(i = 1, \ldots, 2g)$ в пространстве $\mathbf{C}^{2g}$.

Якобиево многообразие $J(S)$ определяется как комплексный тор $\mathbf{C}^g/_\Lambda$.

Отображение

$$\mu : Div^{(0)}(S) \to J(S)$$

определяется следующим образом: если

$$D = \sum_i (p_i - q_i) \in Div^{(0)}(S),$$

то

$$\mu(D) = \left(\sum_i \int\limits_{q_i}^{p_i} \omega_1, \ldots, \sum_i \int\limits_{q_i}^{p_i} \omega_g \right).$$

Дивизор D называется главным, если существует такая мероморфная функция f на S, что

$$D = div(f).$$

Истинны следующие две теоремы

Теорема 3.9. (*Теорема Абеля*). Дивизор $D \in Div^{(0)}(S)$ является главным дивизором тогда и только тогда, когда

$$\mu(D) \equiv \mathbf{0}\ (mod\ \Lambda).$$

Теорема 3.10. (*Теорема обращения Якоби*). Отображение μ является эпиморфизмом (т.е. сюръективным гомоморфизмом).

Пусть $\sim$ – отношение линейной эквивалентности на множестве $Div^{(0)}(S)$.

Из приведенных выше двух теорем вытекает следующая теорема.

Теорема 3.11. Факторгруппа $\mathcal{DIV}^{(0)}(S)/_{\sim}$ изоморфна якобиевому многообразию $J(S)$.

Группой Пикара $\mathcal{PIC}(C)$ алгебраической кривой C называют факторгруппу группы $\mathcal{DIV}(C)$ по отношению линейной эквивалентности дивизоров.

Известно, что группа Пикара является градуированной группой вида

$$\mathcal{PIC}(C) = \oplus\mathcal{PIC}^{(d)}(C),$$

где суммирование осуществляется по степеням d.

Замечание 3.16. Пусть $\mathcal{G}$ есть коммутативная группа, записанная аддитивно, а $\{\mathcal{G}_n\}_{n\in\mathbf{Z}}$ есть фильтрация группы $\mathcal{G}$. Полагая

$$\mathcal{GRAD}_n(\mathcal{G}) = \mathcal{G}_n/_{\mathcal{G}_{n+1}}\ \ (n \in \mathbf{Z}),$$

получим *градуированную группу*

$$\mathcal{GRAD}(\mathcal{G}) = \bigoplus_{n\in\mathbf{Z}} \mathcal{GRAD}_n(\mathcal{G}),$$

ассоциированную с фильтрацией $\{\mathcal{G}_n\}_{n\in\mathbf{Z}}$.

Возрастающей (соответственно, *убывающей*) фильтрацией на группе $\mathcal{G}$ называют возрастающую (соответственно, убывающую) последовательность $\{\mathcal{G}_n\}_{n\in\mathbf{Z}}$ подгрупп группы $\mathcal{G}$.

Группа дивизоров $\mathcal{DIV}(\mathcal{C})$ является в этом смысле градуированной группой, в которой $\mathcal{GRAD}_n(\mathcal{DIV}(\mathcal{C}))$ есть группа $\mathcal{DIV}^{(n)}(\mathcal{C})$ дивизоров степени n.

Факторизация группы

$$\mathcal{DIV}(\mathcal{C}) = \bigoplus_{n\in\mathbf{Z}} \mathcal{DIV}^{(n)}(\mathcal{C})$$

по отношению линейной эквивалентности и дает приведенное выше разложение группы Пикара.

3.6. Модулярные функции и модулярные формы.

Рассмотрим понятия модулярной функции в классическом виде, а также некоторые более современные формулировки.

Классическое определение модулярной функции соответствует в современной интерпретации модулярным функциям веса 0.

Рассмотрим, каким образом модулярные функции и модулярные формы веса $2k$ связаны с эллиптическими кривыми.

3.6.1. Двумерные решетки и мероморфные функции на них.

Как было отмечено ранее, любые два таких комплексных числа $\omega_1, \omega_2 \in \mathbf{C}$, что их отношение не является действительным числом, задают в множестве комплексных чисел $\mathbf{C}$ двумерную решетку

$$\Lambda = \{n\omega_1 + m\omega_2 | n, m \in \mathbf{Z}\}.$$

Элементарной степенной суммой точек решетки Λ называется ряд вида

$$c_n = \sum_{\alpha\in\Lambda}{}' \frac{1}{\alpha^{2n}} \ (n \in \mathbf{N}\backslash\{1\}),$$

где $\alpha = n\omega_1 + m\omega_2$, а штрих у знака суммы означает, что $\alpha \neq 0$.

Известно, что (см., напр., [28]) ряды c_n сходятся абсолютно. Более того, можно показать, что при нечетном $r \in \mathbf{N}$ истинно равенство

$$\sum_{\alpha\in\Lambda}{}' \frac{1}{\alpha^r} = 0.$$

Ясно, что каждый ряд c_n является функцией от решетки Λ.

Исследуем, как меняются значения ряда c_n на подобных решетках.

Преобразование подобия решеток имеет вид

$$\Lambda \to \lambda\Lambda \ (\lambda \in \mathbf{C}).$$

Следовательно,

$$c_k(\lambda\Lambda) = \lambda^{-2k} c_k(\Lambda) \ (k = 2, 3, \dots),$$

т.е. каждый ряд c_k является функцией веса $2k$ от решетки.

Рассмотрим кривую

$$y^2 = 4x^3 - g_2 x - g_3, \tag{3.22}$$

представленную в нормальной форме (W), где $g_2 = 60c_2$ и $g_3 = 140c_3$, а

$$\Delta = g_2^3 - 27g_3^2.$$

Так как функция g_2 имеет вес 4, а функция g_3 – вес 6, то дискриминант Δ имеет вес 12.

Эллиптической функцией называется мероморфная функция $f(z)$ комплексного переменного z, удовлетворяющая условию

$$f(z + \alpha) = f(z),$$

где $\alpha \in \Lambda$, а Λ – двумерная решетка в $\mathbf{C}$.

Замечание 3.17. *Мероморфной* называют функцию, которую можно представить в виде отношения двух целых функций.

Простейшим примером мероморфных функций является класс рациональных функций.

В силу теоремы Лиувилля, ограниченная целая функция постоянна. Поэтому эллиптическая функция, не сводящаяся к константе должна иметь полюса.

В п.3.1.2 приведено следующее выражение для $\wp$-функция Вейерштрасса $\wp = \wp(z)$ $(z \in \mathbf{C})$, имеющее следующий вид

$$\wp(z) = \frac{1}{z^2} + \sum_{\alpha \in \Lambda}{}' \left(\frac{1}{(z+\alpha)^2} - \frac{1}{\alpha^2} \right).$$

Докажем мероморфность функции $\wp(z)$, основываясь на приведенном выше факте о сходимости рядов c_n.

В круге радиуса r получаем следующую оценку

$$\left|\frac{1}{(z+\alpha)^2}-\frac{1}{\alpha^2}\right|=\left|\frac{z^2+2\alpha z}{\alpha^2(z+\alpha)^2}\right|\leq\frac{z^2}{|\alpha|^4}+\frac{2r\alpha}{|\alpha|^4}.$$

Следовательно,

$$|\wp(z)|<\sum_{\alpha\in\Lambda}{}'\frac{r^2}{|\alpha|^4}+\sum_{\alpha\in\Lambda}{}'\frac{2r}{|\alpha|^3},$$

где в правой части неравенства – абсолютно сходящиеся ряды.

Мероморфность функции $\wp(z)$ доказана.

Известно, что (см., напр., [28]) множество эллиптических функций с данной решеткой периодов Λ образуют поле

$$\mathcal{K}_\Lambda=\mathcal{C}(\wp,\wp')\supset\mathcal{C}(\wp),$$

где $\mathcal{C}(\wp)$ есть поле четных эллиптических функций.

Легко доказать (для этого достаточно использовать выражения эллиптических функций и их производных), что для кривой (3.22), представленной в нормальной форме (W), истинно неравенство

$$\Delta\neq 0.$$

Величину

$$J=\frac{g_2^3}{\Delta}$$

называют *инвариантом* эллиптической кривой, представленной в нормальной форме (W). Как отношение двух однородных функций веса 12, он имеет степень однородности 0.

Известно, что если J – модулярный инвариант, то существует эллиптическая кивая с модулярным инвариантом

$$j=2^6 3^3 J$$

над полем $\mathcal{Q}(j)$, а именно кривая

$$y^2 = 4x^3 - h(x+1),$$

где

$$h = 27j(j - 2^6 3^3).$$

Отметим, что

$$j = 1728J.$$

3.6.2. Приведение решеток.

Так как мы рассматриваем решетки с точностью до подобия, то любую невырожденную решетку

$$\Lambda = \{n\omega_1 + m\omega_2 | n, m \in \mathbf{Z}\}$$

можно привести к виду

$$\Lambda = \{n \cdot 1 + m \cdot \tau | Im\, \tau > 0;\ n, m \in \mathbf{Z}\}. \tag{3.23}$$

Замечание 3.18. Если $Im\, \frac{\omega_1}{\omega_2} > 0$, то достаточно умножить Λ на $\frac{1}{\omega_2}$. Если же $Im\, \frac{\omega_1}{\omega_2} < 0$, то достаточно умножить Λ на $-\frac{1}{\omega_2}$.

Можно показать, что, с точностью до подобия, множество всех решеток вида (3.23) параметризуется в комплексной плоскости областью

$$D = \left\{\tau \in H | -\frac{1}{2} < Re\, \tau < \frac{1}{2},\ |\tau| > 1\right\} \cup$$

$$\cup \left\{\tau = \cos\varphi + i \sin\varphi | \frac{\pi}{3} \leq \varphi \leq \frac{\pi}{2}\right\},$$

где

$$H = \{z \in \mathbf{C} | Im\, z > 0\},$$

т.е. H – верхняя комплексная полуплоскость.

В дальнейшем (если не указано иное) считаем, что решетка Λ имеет вид (3.23), где $\tau \in D$.

Таким образом, модулярный инвариант, как функция от τ, имеет следующий вид

$$J = \frac{g_2^3(\tau)}{g_2^3(\tau) - 27g_3^2(\tau)}.$$

Рассмотрим группу

$$\mathcal{SL}_2(\mathbf{Z}) = (SL_2(\mathbf{Z}), \cdot),$$

где

$$SL_2(\mathbf{Z}) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \middle| a, b, c, d \in \mathbf{Z};\ ad - bc = 1 \right\}.$$

Действие группы $\mathcal{SL}_2(\mathbf{Z})$ на верхней полуплоскости H определяется в соответствии со следующим правилом

$$\left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \cdot z = \frac{az + b}{cz + d}.$$

Так как матрица

$$\left(\begin{array}{cc} -1 & 0 \\ 0 & -1 \end{array} \right) \in SL_2(\mathbf{Z})$$

действует на множестве H тривиально, то естественно рассмотреть фактор-группу $\mathcal{G} = (G, \cdot)$ группы $\mathcal{SL}_2(\mathbf{Z})$ по нормальной подгруппе

$$\left(\left\{ \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right), \left(\begin{array}{cc} -1 & 0 \\ 0 & -1 \end{array} \right) \right\}, \cdot \right).$$

Фактор-группа $\mathcal{G}$ называется *модулярной группой*.

Множество D называется *фундаментальной областью* группы $\mathcal{G}$.

Решетки Λ и Λ' называются *эквивалентными*, если существует такой элемент $g \in G$, что

$$\Lambda' = g\Lambda.$$

Пусть $Im\, \frac{\omega_1}{\omega_2} = \tau > 0$, т.е. $\tau = \frac{\omega_1}{\omega_2}$.

Для фиксированного $\tau \in H$ орбита $g \cdot \tau$ ($g \in SL_2(\mathbf{Z})$) порождает все эквивалентные решетки.

По этой причине указанную орбиту называют *классом эквивалентных решеток.*

Классы эквивалентных решеток, как точечные множества, совпадают, различаясь только базисными элементами.

Отсюда следует, что функции c_k точек решетки не меняются на классе эквивалентных решеток.

Следовательно, не меняется и выражающийся через них модулярный инвариант J.

В частности, функция J является периодической

$$J(\tau) = J(\tau + 1).$$

Здесь

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbf{Z}).$$

3.6.3. Разложение модулярного инварианта по параметру.

Рассмотрим периодическую, с периодом 1, функцию

$$q = e^{2\pi i \tau}.$$

Эта функция отображает верхнюю комплексную полуплоскость H в проколотый круг с центром в начале координат.

Найдем разложение J по параметру q.

Исходим из известного тождества

$$\pi \cdot \operatorname{ctg}\, \pi z = \frac{1}{z} + \sum_{n \in \mathbf{N}} \left(\frac{1}{z+n} + \frac{1}{z-n} \right). \tag{3.24}$$

Продифференцировав тождество (3.24) по z, получим

$$-\pi^2 \frac{1}{\sin^2 \pi z} = -\sum_{n \in \mathbf{Z}} \frac{1}{(z+n)^2}.$$

Воспользовавшись представлением

$$\sin \pi z = \frac{e^{\pi i z} - e^{-\pi i z}}{2i},$$

получим

$$-\pi^2 \frac{1}{\sin^2 \pi z} = (2\pi)^2 \frac{1}{(e^{\pi i z} - e^{-\pi i z})^2} = \frac{(2\pi)^2 q}{(1-q)^2} = (2\pi)^2 \sum_{n \in \mathbf{N}} n q^n.$$

Таким образом,

$$(2\pi)^2 \sum_{n \in \mathbf{N}} n q^n = -\sum_{n \in \mathbf{Z}} \frac{1}{(z+n)^2}.$$

Продолжая дифференцирование тождества (3.24), аналогичным образом получим, что для всех $s \geq 2$

$$\sum_{n \in \mathbf{Z}} \frac{1}{(z+n)^s} = \frac{(-2\pi i)^s}{(s-1)!} \sum_{n \in \mathbf{N}} n^{s-1} \cdot q^n. \tag{3.25}$$

Выразим q через функции c_k.

Полагая $s = 2k$ и $z = m\tau$ в (3.25), получим

$$\sum_{n \in \mathbf{Z}} \frac{1}{(n+m\tau)^{2k}} = \frac{(-2\pi i)^{2k}}{(2k-1)!} \sum_{n \in \mathbf{N}} n^{2k-1} \cdot q^n. \tag{3.26}$$

А так как $m\tau \neq 0$ и $e^{2\pi i m \tau n} = q^{nm}$, то

$$c_k = 2\zeta(2k) + 2\frac{(-2\pi i)^{2k}}{(2k-1)!} \sum_{n,m \in \mathbf{N}} n^{2k-1} \cdot q^{nm},$$

где $\zeta(2k)$ – дзета-функция Римана в точке $2k$.

Таким образом, функция

$$J(\tau) = J\left(\frac{1}{2\pi i} \log q\right)$$

разлагается по параметру q.

Можно показать, что (см., напр., [48])

$$J = \frac{g_2^3}{\Delta} = \frac{1}{2^6 3^3}\left(\frac{1}{q} + u_0 + u_1 q + \dots\right).$$

При этом, в разложении

$$j = 2^6 3^3 J = \frac{1}{q} + u_0 + u_1 q + \dots$$

коэффициенты u_i удовлетворяют условиям: $u_i \in \mathbf{Z}$ $(i \in \mathbf{N})$ и $u_0 = 0$.

Определение 3.5. ([28] *Модулярной функцией* называется такая аналитическая функция $f(\tau)$, однозначная в верхней комплексной полуплоскости $Im\,\tau > 0$, не имеющая в ней особых точек, отличных от полюсов $q = e^{2\pi i\tau} = 0$, и инвариантная относительно модулярной группы $\mathcal{G}$.

Рассмотренные выше функции J и j являются примерами модулярных функций.

Истинна следующая теорема.

Теорема 3.12. Любая модулярная функция является рациональной функцией от j.

3.6.4. Слабо модулярные функции и модулярные формы.

При исследовании эллиптических кривых, а также других алгебраических кривых, помимо модулярных в классическом смысле функций, возникают слабомодулярные функции и модулярные формы.

Приведем соответствующее определение.

Определение 3.6. *Слабо модулярной функцией веса* $2k$ $(k \in \mathbf{Z})$ называется мероморфная на верхней комплексной полуплоскости H функция, удовлетворяющая соотношению

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z), \tag{3.27}$$

для любой матрицы

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}).$$

Обозначив через g образ матрицы в группе G, получим

$$\frac{d(gz)}{dz} = (cz+d)^{-2}. \tag{3.28}$$

С использованием раенства (3.28) равенство (3.27) может быть переписано в виде

$$f(z) = \left(\frac{d(gz)}{dz}\right)^k f(gz). \tag{3.29}$$

Распределяя дифференциалы в (3.29), получим

$$f(z)(dz)^k = f(gz)(d(gz))^k.$$

Таким образом, дифференциальная форма $f(z)(dz)^k$ инвариантна относительно группы $\mathcal{G}$.

Так как группа $\mathcal{G}$ порождается элементами

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

и

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

то для слабомодулярности заданной на верхней комплексной полуплоскости мероморфной функции $f(z)$ достаточно, чтобы выполнялись два соотношения

$$f(Sz) = f\left(-\frac{1}{z}\right) = z^{2k} f(z),$$

$$f(Tz) = f(z+1) = f(z). \tag{3.30}$$

Из (3.30) вытекает, что слабо модулярная функция $f(z)$ разлагается в ряд Лорана по параметру $q = e^{2\pi i\tau}$, т.е.

$$\widetilde{f}(q) = \sum_{n=n_0}^{\infty} a_n q^n \ (n_0 \le 0,\ n_0 \in \mathbf{Z}).$$

Слабо модулярная функция назыавается *модулярной*, если она голоморфна в бесконечности.

Для слабо модулярной функции $f(z)$ условие ее модулярности записывается в виде

$$f(\infty) = \widetilde{f}(0), \tag{3.31}$$

т.е. если функция f продолжается до мероморфной функции в начале координат.

Определение 3.7. [48]. *Модулярной формой* называется любая модулярная функция, которая голоморфна всюду, включая бесконечность.

Если такая функция обращается в нуль на бесконечности, то она называется *параболической формой*.

Пример 3.3. Модулярными формами являются *ряды Эйзенштейна*

$$E_{2k} = E_{2k}(z) = \sum_{\substack{c,d\in\mathbf{Z}\\(a,b)\neq(0,0)}} (cz+d)^{-2k}, \tag{3.32}$$

так как

$$E_{2k}\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} E_{2k}(z)$$

для всех $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$.

Для мероморфной в верхней комплексной полуплоскости H функции $f(z)$, не являющейся тождественным нулем, порядком в точке $p \in H$ (обозначается $\nu_p(f)$) называется такое целое число n, что функция

$$\frac{f(z)}{(z-p)^n}$$

голоморфна и не обращается в нуль в точке p.

Если f – модулярная веса $2k$ функция, то из (3.27) вытекает, что

$$\nu_p(f) = \nu_{g(p)}(f) \ (g \in G).$$

Следовательно, порядок $\nu_p(f)$ функции $f(z)$ зависит только от образа точки p.

По определению полагают, что $\nu_\infty(f)$ есть порядок функции $\widetilde{f}(q)$ в точке $q = 0$.

Стабилизатором точки $p \in H$ называется подгруппа

$$\mathcal{I}(p) = (I(p), \cdot)$$

группы $\mathcal{G}$, состоящая из таких элементов $g \in G$, что

$$g(p) = p.$$

Обозначим через $e(p)$ $(p \in H)$ – порядок стабилизатора точки p.

Несложно показать, что порядок стабилизатора точки, принадлежащей фундаментальной области D группы $\mathcal{G}$ отличен от единицы только для трех точек, а именно: для точек $i = \sqrt{-1}$, $\rho = e^{\frac{2\pi i}{3}}$ и $-\widetilde{\rho} = e^{\frac{\pi i}{3}}$.

При этом,

$$I(i) =< S >, \quad e(i) = 2,$$
$$I(\rho) =< ST >, \quad e(\rho) = 3,$$
$$I(-\widetilde{\rho}) =< TS >, \quad e(-\widetilde{\rho}) = 3.$$

Обозначим через $H/_G$ множество орбит точек, принадлежащих фундаментальной области D.

Истинна следующая теорема.

Теорема 3.13. [48]. Если $f(z)$ – модулярная функция веса $2k$, не равная тождественно нулю, то

$$\nu_\infty(f) + \sum_{p \in H/_G} \frac{1}{e_p} \nu_p(f) = \frac{k}{6}, \tag{3.33}$$

где $\sum\limits_{p \in H/_G}$ означает суммирование по классам фактор-множества $H/_G$.

Принимая во внимание установленные выше порядки стабилизаторов, равенство (3.33) можно переписать в виде

$$\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_i(f) + \sum_{p \in H/_G}{}^{*} \frac{1}{e_p} \nu_p(f) = \frac{k}{6}, \tag{3.34}$$

где $\sum\limits_{p \in H/_G}{}^{*}$ означает суммирование по классам точек, отличных от классов точек i и ρ.

Формулы (3.33) и (3.34) дают возможность описать векторное пространство M_{2k} модулярных форм веса $2k$ и, в частности, определить его размерность

$$dim_{\mathbf{C}} M_{2k} = d_{2k}.$$

Действительно, так как, по определению, модулярная форма не имеет полюсов, то $k \geq 0$ в (3.34), т.е. при $k < 0$ модулярных форм нет, так как

$$M_{2k} = \{0\} \ (k < 0).$$

Если $k = 1$, то

$$M_2 = \{0\}.$$

Если $k = 2$, то

$$M_4 = \mathbf{C}E_4,$$

где E_4 определяется равенством (3.32).

Аналогичным образом

$$M_6 = \mathbf{C}E_6,$$
$$M_8 = \mathbf{C}E_8,$$
$$M_{10} = \mathbf{C}E_{10}.$$

Размерность векторного пространства M_{2k} определяется следующей теоремой.

Теорема 3.14. Для всех $k \geq 0$

$$d_{2k} = \begin{cases} \lfloor \frac{k}{6} \rfloor, & \text{если } k \equiv 1 \ (mod\, 6) \\ \lfloor \frac{k}{6} \rfloor + 1, & \text{если } k \not\equiv 1 \ (mod\, 6) \end{cases}.$$

Рассмотрим производящую функцию

$$P_M(t) = \sum_{k=-\infty}^{\infty} d_{2k} t^{2k}.$$

Ясно, что

$$P_M(t) = \sum_{k=0}^{\infty} d_{2k} t^{2k}. \tag{3.35}$$

Ряд (3.35) называется *рядом Пуанкаре* градуированного модуля

$$M = \bigoplus_{k \in \mathbf{Z}_+} M_{2k}.$$

Отметим, что

$$P_M(t) = (1 - t^4)^{-1}(1 - t^6)^{-1}.$$

Положим $Q = E_4$ и $R = E_6$.

Истинна следующая теорема.

Теорема 3.15. 1. Мономы $Q^a R^b$ $(4a + 6b = 2k)$ порождают базис модуля M_{2k}.

2. Гомоморфизм $\mathbf{C}[Q, R] \to M$ является изоморфизмом градуированных алгебр.

Замечание 3.19. Пусть $\mathcal{K}$ есть коммутативное кольцо с единицей, $\mathcal{A}$ – алгебра над $\mathcal{K}$, а $\mathcal{G} = (G, +)$ – аддитивно записываемый коммутативный моноид.

Градуировкой алгебры $\mathcal{A}$ со значением в моноиде $\mathcal{G}$ называют семейство $\{\mathcal{M}_\alpha\}_{\alpha \in G}$ $\mathcal{K}$-модулей алгебры $\mathcal{A}$, удовлетворяющих условиям:

1) $\mathcal{A}$ есть прямая сумма $\mathcal{M}_\alpha$;

2) $\mathcal{M}_\alpha \mathcal{M}_\beta \subseteq \mathcal{M}_{\alpha+\beta}$.

Множество A, наделенное структурой алгебры и градуировкой $\{\mathcal{M}_\alpha\}_{\alpha \in G}$ называют *градуированной алгеброй*.

Обозначим через M_{2k}^0 векторное пространство параболических модулярных форм веса $2k$.

Можно показать, что

$$\Delta = g_2^3 - 27 g_3^2 \in M_{12}^0.$$

Отсюда вытекает, что истинно следующее утверждение.

Утверждение 3.3. Умножение на Δ определяет изоморфизм векторного пространства $M_{2(k-6)}$ на векторное пространство M^0_{2k}.

В заключение приведем следующую оценку порядка роста коэффициентов параболических модулярных форм.

Теорема 3.16. (Гекке). Для параболической формы

$$f(z) = \sum_{n=1}^{\infty} a_n q^n$$

истинно асимптотическое равенство

$$|a_n| = O(n^k) \ (n \to \infty).$$

3.7. Генерация пседослучайных последовательностей.

Рассмотрим два метода: кодирование, основанное на использовании накрытий Артина-Шнайера и эллиптических кривых (функциональный метод) и кодирование, основанное на на использовании арифметических поверхностей Артина-Шнайера и эллиптических поверхностей над кольцом целых чисел (арифметическое кодирование).

В обоих случаях используется нормальная форма (E) эллиптических кривых.

Варьируя нормальную форму эллиптической кривой, а также порядки вычисления бесконечных в обе стороны последовательностей (эллиптическая кривая – накрытие Артина-Шнайера, накрытие Артина-Шнайера – эллиптическая кривая), можно расширить класс достаточно сложно декодируемых последовательностей.

3.7.1. Основные понятия.

Понятия арифметического и автоматного моделирования [45,110] не являются независимыми, и, во многих случаях, дополняют друг друга.

Последовательность $\{a_n\}_{n\in\mathbf{Z}_+}$ над конечным алфавитом A называется *k-автоматной* ($k \geq 2$), если существует такой автомат, что при входном значении $n \in \mathbf{Z}_+$ на основе числа k, автомат переходит в состояние, в котором выдается выходной символ a_n.

Арифметическим моделированием числовой последовательности называют последовательность, построенную арифметическими средствами.

Замечание 3.20. *Последовательностью, построенную арифметическими средствами* называют любую последовательность, заданную с помощью примитивно рекурсивной функции.

Пример 3.4. Пусть ξ – иррациональное число. Тогда последовательность

$$\{\alpha_n\}_{n\in\mathbf{N}},$$

определяемая соотношением

$$\alpha_n = n\xi \ (mod\, 1) \ (n \in \mathbf{N}),$$

является арифметической.

Более того, эта последовательность имеет равномерное распределение на промежутке $[0, 1)$.

Важный для математических исследований и приложений класс арифметически моделируемых последовательностей образуют последовательности, элементы которых вычисляются на основе арифметических характеристик алгебраических кривых.

Примерами таких последовательностей являются последовательности углов элементов Фробениуса [49].

Ниже будут рассмотрены эти и другие последовательности, а также предложены методы их кодирования.

3.7.2. Бесконечные числовые последовательности, цилиндрические множества, меры и случайные процессы.

Пусть $g \geq 2$ – натуральное число, $X = \{1, 2, \ldots, g-1\}$ – алфавит, а X^ω – множество всех составленных из знаков $1, 2, \ldots, g-1$ бесконечных последовательностей.

Замечание 3.21. Множество X^ω называется также *пространством сверхслов* в алфавите X.

Элементарно цилиндрическим множеством (э.ц.-множеством) *ранга* r $(r \in \mathbf{N})$ называется множество вида

$$a_1 \ldots a_r X^\omega,$$

где $a_i \in X$ $(i = 1, \ldots, r)$.

К э.ц.-множествам относят также само множество X^ω и пустое множество.

Цилиндрическим множеством (*ц.-множеством*) называют множество, которое может быть представлено как конечное объединение э.ц.-множеств.

Истинно следующее утверждение.

Утверждение 3.4. Пересечение двух ц.-множеств является ц.-множеством. Дополнение к ц.-множеству является ц.-множеством.

Таким образом, ц.-множества образуют алгебру.

Мера μ определяется на классе э.ц.-множеств следующим образом:

$$\mu(X^\omega) = 1,$$

$$\mu(\emptyset) = 0,$$

$$\mu(a_1 \dots a_r X^\omega) = \frac{1}{g^r} \quad (r \in \mathbf{N}, a_i \in X \ (i = 1, \dots, r)).$$

Функция μ обычным образом продолжается на ц.-множества.

Истинно следующее утверждение.

Утверждение 3.5. Функция μ неотрицательна, определена на алгебре ц.-множеств, счетно-аддитивна, т.е. является мерой.

Из теории меры известно [80], что существует однозначно определенная минимальная σ-алгебра $\widetilde{S}$, содержащая алгебру цилиндрических множеств, на которую однозначно продолжается мера μ.

Множества из σ-алгебра $\widetilde{S}$ называются *измеримыми*.

Функция f, определенная напространстве X^ω, называется *измеримой*, если для любого $\alpha \in \mathbf{R}$ множество точек $x \in X^\omega$, удовлетворяющих неравенству $f(x) \leq \alpha$, измеримо.

Пусть S является пополнением σ-алгебры $\widetilde{S}$ по мере μ. Тройка

$$(X^\omega, S, \mu)$$

называется *стационарным случайным процессом с дискретным временем*.

Приведенное определение стационарного случайного процесса может быть обобщено, по крайней мере, в следующих трех направлениях:

1) вместо алфавита X берется некоторе измеримое пространство (Y, Σ), где Σ есть σ-алгебра подмножеств на Y;

2) вместо пространства X^ω берется пространство A^ω бесконечных в обе стороны последовательностей

$$y = (\dots, y_{-1}, y_0, y_1, y_2, \dots);$$

3) ц.-множества, определяющие σ-алгебру $\widetilde{S}$ на A^ω, определяются как множества вида

$$A = \{y | y = (\dots, y_{i_1}, \dots, y_{i_2}, \dots, y_{i_r}, \dots) \in A^\omega | y_{i_j} \in Y_j \ (j = 1, \dots, r)\},$$

где $i_1, \dots, i_r \in \mathbf{Z}$ $(i_1 < \dots < i_r)$ – фиксированные числа, а $Y_j \in \Sigma$ $(j = 1, \dots, r)$.

В последних двух случаях тройка

$$(X^\omega, S, \mu)$$

называется *стационарным случайным процессом с дискретным временем.*

Условие стационарности состоит в том, что мера ц.-множества не зависит от сдвига на конечное число позиций влево или вправо всех последовавтельностей, принадлежащих этому ц.–множеству.

Функцию, определенную на случайном пространстве и принимающую значения в некотором измеримом пространстве, называют *случайной функцией.*

3.7.3. Меры Дирака.

Будем считать, что любое отображение $T : [0, 1) \to [0, 1)$ расширяется на отрезок $X = [0, 1]$ равенством

$$T(1) = 1.$$

В дальнейшем рассматриваем только T-инвариантные меры.

Во многих случаях, например, при $\times 2$-инвариантном отображении [108], класс T-инвариантных борелевских вероятностных мер на X можно отождествить с инвариантными относительно сдвига Борелевскими вероятностными мерами на $\{0, 1\}^{\mathbf{N}}$.

Если у нас есть бесконечная числовая последовательность с оператором сдвига, то траекторией этой последовательности называется множество последовательностей, полученных из нее итерацией оператора сдвига.

Отметим, что на отрезке X имеются две граничные меры Дирака δ_0 и δ_1, а также класс мер, параметризованных действительными числами $\rho \in X$, и имеющих вид

$$\nu_\rho = (1-\rho)\delta_0 + \rho\delta_1.$$

Пусть

$$(M, \Sigma, \mu)$$

есть вероятностное пространство, на котором определена полугруппа

$$\mathcal{T} = (\{T^k | k \in \mathbf{Z}_+\}, \circ)$$

таких преобразований пространства M в себя, что для любого множества $U \in \Sigma$ его полный прообраз при любом отображении T^k $(k \in \mathbf{Z}_+)$ принадлежит Σ и для любого множества $U \in \Sigma$

$$\mu T^{-1} U = \mu U. \tag{3.36}$$

Замечание 3.22. Равенство (3.36) является условием инвариантности меры μ относительно рассматриваемой полугруппы преобразований.

В эргодической теории вероятностное пространство вместе с полугруппой преобразований $\mathcal{T}$ называют *динамической системой*.

Подмножество $X \subset M$ называется *инвариантным*, если

$$TX = X.$$

Далее, динамическую систему обозначаем тройкой (M, μ, T), если не оговорено противное.

Если множество M не представимо в виде суммы непересекающихся инвариантных множеств положительной меры, то говорят, что динамическая система (M, μ, T) *неразложима* или *эргодична*.

3.7.4. Преобразования Бейкера, β-преобразования и их расширения.

β-преобразование $(\beta > 1)$ определяется равенством

$$T_\beta(x) = \beta x \,(mod\, 1) \;\; (x \in [0,1]),$$

а *β-расширение* определяется равенством

$$d_\beta(x) = (x_i)_{i\in\mathbf{N}}\ (x_i = \lfloor \beta T_\beta^{i-1}(x)\rfloor).$$

Понятие β-преобразование введено в [114], где исследована символьная динамика β-преобразований, а также доказана эргодичность β-преобразования.

В [113] описаны возможные последовательности, которые могут быть β-разложениями.

Ключевая роль величины $d_\beta(x)$ указана в [86].

В [84] и [90] исследованы, соответственно, толстые преобразования Бейкера (the fat baker's transformations) и обобщенные преобразования Бейкера (generalized baker's transformations).

Натуральные (natural) расширения β-преобразований охарактеризованы в [94].

В [91] исследовано множество $\mathtt{S}$ всех таких β, что натуральное расширение T_β может быть представлено посредством отображений

$$\mathtt{T}_\beta(x,y) = \left(T_\beta, \frac{\lfloor \beta x\rfloor + y}{\beta}\right),$$

определенных на просто связных подмножествах единичного квадрата, и с инвариантной мерой, являющейся константной кратной 2-мерной меры Лебега на $[0,1]^2$.

В [111] исследованы достаточные условия для существования таких β-преобразований, для которых их натуральные расширения могут быть представлены как обобщенные преобразования Бейкера, а также охарактеризовано множество таких чисел β.

3.7.5. Отображения Клостермана-Хассе.

В [45] представлены и исследованы функции, определенные на целых числах, на классах вычетов по простым модулям со значениями в единичном отрезке, а также рассмотрены некоторые вопросы кодирования отображений бесконечными в одну сторону последовательностями.

Замечание 3.23. Ниже выделяется класс отображений в квадрат

$$\Pi = [0,\pi]\times[0,\pi],$$

допускающих их кодирование продолжающимися (в том числе и бесконечными) в обе стороны последовательностями.

Конструируемые отображения, их мы называем *отображения Клостермана-Хассе* (КХ-отображения), строятся на основе сумм Клостермана и кубических кривых. Будут построены *функциональное* и *арифметическое* КХ-отображения.

Определяется и исследуется целочисленное кодирование КХ-отображений на основе прямого произведения конечных равномощных разбиений отрезка $[0, \pi]$ и интерпретация этого кодирования точками единичного квадрата.

Предварительно напомним понятие последовательности, равнораспределенной с данной функцией плотности, или равномерно распределенной с данной функцией плотности.

Пусть дана последовательность α вещественных чисел (α_i) такая, что все ее значения принадлежат некоторому компактному замкнутому интервалу Π вещественной прямой. Для наших целей достаточно следующего понятия функции плотности распределения последовательности α. Пусть $N = (n_i)_{i=1}^{\infty}$ есть последовательность натуральных чисел, такая, что $\lim_{i\to\infty} n_i = \infty$.Вещественную непрерывную функцию $\theta(u)$ на Π называют называют функцией плотности для $\alpha = (\alpha_{n_1}, \dots, \alpha_{n_i}, \dots)$ если она удовлетворяет следующему условию:

(D) для всякого открытого интервала $\gamma \subset \Pi$ и натурального числа i пусть $\#\alpha_{n_i}(\gamma)$ есть число j таких α_{n_j},которые принадлежат γ. Тогда должно выполняться

$$\lim_{i\to\infty} \frac{\#\alpha_{n_i}(\gamma)}{n_i} = \int\limits_{\gamma} \theta(u)du.$$

Последовательность $\alpha = (\alpha_i)$ называется равнораспределенной с данной функцией плотности, или равномерно распределенной с данной функцией плотности, если выполнено вышеприведенное условие (D).

Построим вначале функциональное КХ-отображение.

1. *Компонента Хассе.*

Зафиксируем простое число $p \in \mathbf{N}$.

Рассмотрим над полем $\mathcal{F}_p = (\mathbf{Z}_p, \oplus, \circ)$ кривую Γ, определенную уравнением

$$y^2 = f(x),$$

где

$$f(x) = x^3 \oplus c \circ x \oplus d.$$

По аналогии с тем, как это сделано в п. 2.3.4, получаем

$$|\Gamma \cup \{\mathcal{O}\}| = 1 + \sum_{x=0}^{p-1} \left(1 + \left(\frac{x^3 + cx + d}{p}\right)\right) =$$

$$= 1 + p + \sum_{x=0}^{p-1} \left(\frac{x^3 + cx + d}{p}\right) = 1 - p - a_p,$$

где

$$a_p = -\sum_{x=0}^{p-1} \left(\frac{x^3 + cx + d}{p}\right).$$

Известно, что

$$a_p = 2\sqrt{p}\cos\varphi_p. \tag{3.37}$$

Замечание 3.24. В [46] показано, что если Γ не является эллиптической кривой, то $a_p \in \{-1, 0, 1\}$, причем значение a_p легко вычисляется.

Из (3.37) вычисляем

$$\varphi_p = \arccos\left(\frac{a_p}{2\sqrt{p}}\right),$$

и приводим вычисленное значение к отрезку $[0, \pi]$.

Гипотеза Сато-Тейта [49] (в функциональном случае это теорема Берча [89]) утверждает, что для эллиптических кривых без комплексных умножений углы φ_p, соответствующие a_p, равнораспределены на отрезке $[0, \pi]$ с плотностью $\frac{2}{\pi}\sin^2 t$.

2. *Компонента Клостермана.* Пусть

$$cd \not\equiv 0 \,(mod\, p).$$

Рассмотрим сумму Клостермана

$$T_p(c, d) = \sum_{x=1}^{p-1} e^{2\pi i \frac{cx + \frac{d}{x}}{p}}.$$

Согласно А. Вейлю (см., напр., [49])

$$T_p(c, d) = 2\sqrt{p}\cos\theta_p(c, d). \tag{3.38}$$

Вычисляя $T_p(c,d)$ и $\cos\theta_p(c,d)$, находим из (3.38)

$$\theta_p = \theta_p(c,d),$$

и приводим вычисленное значение к отрезку $[0,\pi]$.

В функциональном случае теорема Делиня-Каца-Адольфсона [109] утверждает, что углы θ_p равнораспределены на отрезке $[0,\pi]$ с плотностью $\frac{2}{\pi}\sin^2 t$.

Экспериментальное исследование распределения углов сумм Клостермана в функцианальном случае представлено в [20].

Функциональное КХ-отображение $hc : \mathbf{Z}_p \times \mathbf{Z}_p \to \Pi$ определим равенством

$$hk(c,d) = (\varphi_p(c,d), \theta_p(c,d)).$$

Кодирование функционального КХ-отображения числовой последовательностью осуществляется следующим образом.

Пусть π_1 и π_2 – два d-блочных ($d \in \mathbf{N}$ разбиения отрезка $[0,\pi]$.

Назовем π_1 горизонтальным, π_2 вертикальным разбиением отрезка $[0,\pi]$, а саму пару разбиений (π_1,π_2) – p-парой.

Обозначим блоки разбиения π_i $(i=1,2)$ числами $0,1,\ldots,d-1$.

Кодом функционального КХ-отображения является конечная последовательность

$$b_s b_{s-1} \ldots b_1 b_0 . a_1 a_2 \ldots a_r.$$

Значение этой последовательности может быть интерпретировано как рациональная точка (x,y), принадлежащая единичному квадрату, если положить

$$x = \sum_{i=1}^{r} \frac{a_i}{d^i},$$

$$y = \sum_{i=1}^{s} \frac{b_{i-1}}{d^i}.$$

Построим теперь арифметическое КХ-отображение.

Напомним, что спектром коммутативного кольца с единицей называют множество его простых идеалов. Для кольца целых рациональных чисел его спектр обозначают $Spec\,\mathcal{Z}$; Обозначим через d_1 – множество точек спектра, в которых

$$c \equiv 0\ (mod\, p),$$

$$d \equiv 0 \,(mod\, p).$$

Множество точек спектра, входящих в множество d_1 , есть множество простых идеалов, которые соответствуют простым числам, делящим c или d.

1. *Компонента Хассе.* Пусть Γ – эллиптическая кривая над кольцом $\mathcal{Z}$ целых чисел.

Вне конечного множества простых чисел, являющихся делителями дискриминанта, кривая Γ имеет хорошую редукцию в поле $\mathcal{F}_p = (\mathbf{Z}_p, \oplus, \circ)$.

Для локализации Γ_p кривой Γ по $mod\, p$ истинна формула

$$|\Gamma \cup \{\mathcal{O}\}| = 1 - p - a_p,$$

где a_p вычисляется в соответствии с формулой (3.37), а сама кривая Γ рассматривается как проективная.

Если локализация Γ_p кривой Γ не является эллиптической кривой, то $a_p \in \{-1, 0, 1\}$, причем значение a_p легко вычисляется [46].

В обоих случаях вычисляется

$$\varphi_p = \arccos\left(\frac{a_p}{2\sqrt{p}}\right),$$

а вычисленное значение приводится к отрезку $[0, \pi]$.

2. *Компонента Клостермана* вычисляется как и в предыдущем случае.

Обозначим через $Spec\, \mathcal{Z}$ аффинную схему над кольцом целых чисел $\mathcal{Z}$ и положим

$$Sp = Spec\, \mathcal{Z} \backslash d_1.$$

Арифметическое КХ-отображение $hc : Sp \times Sp \to \Pi$ определим равенством

$$hk(c, d) = (\varphi_p(c, d), \theta_p(c, d)).$$

В проведенном экспериментальном исследовании с суммой Клостермана $T_p = T_p(1, 1)$, представленном в [20], схема Sp совпадает с $Spec\, \mathcal{Z}$.

Кодирование арифметического КХ-отображения числовой последовательностью осуществляется следующим образом.

Определение p-пары и обозначение блоков разбиения аналогично функциональному случаю.

Кодом арифметического КХ-отображения является бесконечная последовательность

$$\ldots\ldots b_1 b_0 . a_1 a_2 \ldots .$$

Значение этой последовательности может быть интерпретировано как точка (x, y), принадлежащая единичному квадрату, если положить

$$x = \sum_{i=1}^{\infty} \frac{a_i}{d^i},$$

$$y = \sum_{i=1}^{\infty} \frac{b_{i-1}}{d^i}.$$

Эти числа x и y естественно назвать числами, соответственно, Клостермана и Хассе.

Отметим, что арифметическому КЧ-отображению $hk(c, d)$ и его кодированию посредством заданной p-пары соответствует двусторонний сдвиг

$$\sigma(\ldots\ldots b_1 b_0 . a_1 a_2 \ldots) = \ldots\ldots b_1 b_0 a_1 . a_2 \ldots .$$

Замечание 3.25. В качестве заслуживающей внимания и неисследованной проблемы, возникающей в связи с предложенными методами арифметического отображения и кодирования, отметим следующую:

Какие числа (*рациональные*, *иррациональные или трансцендентные*) *определяют предельные последовательности*?

Под предельной последовательностью мы понимаем последовательность, возникающую при стремлении количества различных простых чисел к бесконечности.

4. РЕШЕНИЕ УРАВНЕНИЙ НАД КОНЕЧНЫМИ КОЛЬЦАМИ

Необходимость решения уравнений и систем уравнений над конечными кольцами возникает не только в процессе качественного анализа структуры алгебраических многообразий, но и при построении в явном виде таких многообразий, в частности, алгебраических кривых над конечными кольцами. Неисчерпаемым поставщиком различных систем уравнений над конечными кольцами, являются задачи идентификации алгебраически-автоматных моделей, определенных в терминах конечных колец.

Поэтому, исследование методов решения уравнений и систем уравнений над конечными кольцами актуально как с теоретической, так и прикладной точки зрения.

Цель настоящего раздела и состоит в исследование методов решения уравнений и систем уравнений над конечными кольцами.

В настоящем разделе под кольцом $\mathcal{K} = (K, +, \cdot)$ понимается ассоциативно-коммутативное кольцо с единицей.

В п.4.1 исследовано соотношение между множествами отображений абстрактного множества S в полные системы вычетов по конечному набору попарно взаимно простых элементов дедекиндового кольца и множествами отображений множества S в полную систему вычетов по произведению этих элементов. Рассмотрено применение полученных результатов при комбинаторном анализе объектов, построенных в терминах числовых колец, и используемых при решении прикладных задач преобразования информации. В п.4.2 предложена общая схема решения систем полиномиальных уравнений с параметрами над кольцом $\mathcal{K}$. В п.4.3 рассмотрено применение этой схемы к решению систем полиномиальных уравнений с параметрами над кольцом вычетов $\mathcal{Z}_{p^k}$.

Результаты авторов, представленные в разделе, опубликованы в [53-60].

Известные результаты изложены в соответствии с [7,32,36,42].

4.1. Отображения абстрактных множеств в дедекиндовы кольца.

Устойчивая тенденция к применению алгебраических моделей и методов в процессе решения задач криптографии сделала актуальной разработку комбинаторных схем, предназначенных для подсчета или оценки числа тех или иных комбинаторных объектов, построенных с помощью теории колец. В частности, схем, предназначенных для оценки количества элементов, принадлежащих алгебраическим многообразиям.

Ясно, что любую такую схему можно представить в терминах отображений абстрактных множеств в соответствующее кольцо. Такое представление дает возможность установить внутренние связи между теорией колец, комбинаторным анализом и прикладными задачами преобразования информации, в частности, криптографии.

В качестве кольца естественно выбрать кольцо наиболее общего вида, в рамки которого укладываюся основные теоретико-числовые конструкции, используемые в криптографии (по крайней мере конструкции, представленные системами линейных сравнений). К такому типу колец относятся дедекиндовы кольца.

Исходя из сказанного выше, в настоящем пункте исследуются соотношения между двумя последовательностями множеств отображений абстрактного множества в дедекиндово кольцо $\mathcal{K} = (K, +, \cdot)$, определенные в терминах полной системы вычетов по попарно взаимно простым модулям.

4.1.1. Основные понятия.

Так как $\mathcal{K} = (K, +, \cdot)$ – дедекиндово кольцо, то каждый собственный идеал J представим в виде произведения конечного числа простых идеалов, т.е.

$$J = (p_1) \dots (p_n) \ (n \in \mathbf{N}),$$

где $p_1, \dots, p_n$ – простые элементы кольца $\mathcal{K}$.

Замечание 4.1. Элемент $p \in K$, не являющийся делителем единицы, называется простым, если произведение ab $(a, b \in K)$ делится на p тогда и только тогда, когда a или b делится на p.

Отличные от нуля, не являющиеся делителями единицы, элементы $a, b \in K$ назовем *взаимно простыми*, если наибольший общий делитель идеалов (a) и (b) совпадает с K.

Замечание 4.2. По определению, наибольший общий делитель идеалов J_1 и J_2 – это идеал, порожденный теоретико-множественным объединением идеалов J_1 и J_2.

Из этого определения следует, что если $a, b \in K$ – взаимно простые элементы кольца $\mathcal{K}$ и ax $(x \in K)$ делится на b, то x делится на b.

Для любого идеала J кольца $\mathcal{K}$ бозначим через $\pi(K, J)$ фактор-множество $K/_J$, рассматриваемое как разбиение множества K.

В дальнейшем нам понадобится следующая лемма.

Лемма 4.1. Если $a, b \in K$ – взаимно простые элементы дедекиндового кольца $\mathcal{K}$, то истинно равенство

$$\pi(K, (ab)) = \pi(K, (a)) \cdot \pi(K, (b)), \tag{4.1}$$

где «$\cdot$» – операция умножения разбиений.

Доказательство. Пусть $a, b \in K$ – взаимно простые элементы кольца $\mathcal{K}$.

Докажем, что истинно неравенство

$$\pi(K,(ab)) \leq \pi(K,(a)) \cdot \pi(K,(b)). \tag{4.2}$$

Пусть $x \equiv y\,(\pi(K,(ab)))$. Тогда $x - y \in (ab)$.

Следовательно, существует такой элемент $z \in K$, что

$$x - y = abz.$$

Отсюда вытекает, что $x \equiv y\,(\pi(K,(a)))$ и $x \equiv y\,(\pi(K,(b)))$, т.е.

$$x \equiv y\,(\pi(K,(a)) \cdot \pi(K,(b))),$$

что и требовалось доказать.

Докажем, что истинно неравенство

$$\pi(K,(ab)) \geq \pi(K,(a)) \cdot \pi(K,(b)). \tag{4.3}$$

Предположим, что $x \equiv y\,(\pi(K,(a)) \cdot \pi(K,(b)))$. Тогда $x \equiv y\,(\pi(K,(a)))$ и $x \equiv y\,(\pi(K,(b)))$.

Следовательно, существуют такие элементы $u, v \in K$, что

$$x - y = au,$$

$$x - y = bv.$$

Так как au делится на b, а a и b – взаимно-простые элементы кольца $\mathcal{K}$, то u делится на b.

Следовательно, $u = bw$, т.е.

$$x - y = abw,$$

откуда вытекает, что

$$x \equiv y\,(\pi(K,(ab))),$$

что и требовалось доказать.

Из (4.2) и (4.3) вытекает (4.1).

□

Воспользовавшись леммой 4.1, индукцией по числу $m \in \mathbf{N}$ несложно доказать, что истинно следующее следствие.

СЛЕДСТВИЕ 4.1. Если $a_1, \ldots, a_m$ $(m \in \mathbf{N})$ – попарно простые элементы дедекиндового кольца $\mathcal{K}$, то истинно равенство

$$\pi\left(K, \left(\prod_{i=1}^{m} a_i\right)\right) = \prod_{i=1}^{m} \pi(K, (a_i)). \tag{4.4}$$

Зафиксировав в каждом блоке разбиения $\pi(K, (a))$ $(a \in K)$ по одному элементу, получим *полную систему вычетов* $\mathrm{MOD}(a)$ по модулю a.

Обозначим через $b < \mathrm{mod}\, a > (a, b \in K)$ такой единственный элемент $c \in \mathrm{MOD}(a)$, что элементы b и c принадлежат одному и тому же блоку разбиения $\pi(K, (a))$.

Пусть S – произвольное абстрактное множество, а $a_1, \ldots, a_m$ $(m \in \mathbf{N})$ – попарно взаимно-простые элементы кольца $\mathcal{K}$.

Положим

$$F_{a_i}(S) = \{f | f : S \to \mathrm{MOD}(a_i)\}\ (i = 1, \ldots m),$$

$$F(S) = \left\{ f \,\middle|\, f : S \to \mathrm{MOD}\left(\prod_{i=1}^{m} a_i\right) \right\}.$$

Зафиксируем подмножества отображений

$$\widehat{F}_{a_i}(S) \subseteq F_{a_i}(S)\ (i = 1, \ldots m)$$

и положим

$$\widetilde{F}_{a_i}(S) = \{f \in F(S) | f_{\mathrm{mod}\, a_i} \in \widehat{F}_{a_i}(S)\}\ (i = 1, \ldots m),$$

где отображение $f_{\mathrm{mod}\, a_i}$ $(i = 1, \ldots m)$ определяется равенством

$$f_{\mathrm{mod}\, a_i}(s) = f(s) < \mathrm{mod}\, a_i >\ \ (s \in S).$$

4.1.2. Соотношение между последовательностями множеств отображений $\widehat{F}_{a_i}(S)$ $(i = 1, \ldots m)$ и $\widetilde{F}_{a_i}(S)$ $(i = 1, \ldots m)$.

Ясно, что определенные выше последовательности множеств отображений $\widehat{F}_{a_i}(S)$ $(i = 1, \ldots m)$ и $\widetilde{F}_{a_i}(S)$ $(i = 1, \ldots m)$ могут быть использованы для построения различных комбинаторных схем, определяемых в терминах вычетов по модулю идеалов дедекиндового кольца.

Следующая теорема определяет одно из основных соотношений между этими последовательностями множеств отображений.

Теорема 4.1. Для любого множества S и произвольных попарно взаимно простых элементов $a_1, \ldots, a_m$ ($m \in \mathbf{N}$) дедекиндового кольца $\mathcal{K}$ истинно равенство

$$|\widehat{F}_{a_1}(S) \times \cdots \times \widehat{F}_{a_m}(S)| = \left| \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \right|. \tag{4.5}$$

Доказательство. Для того, чтобы доказать равенство (4.5), достаточно построить инъекции

$$\varphi : \widehat{F}_{a_1}(S) \times \cdots \times \widehat{F}_{a_m}(S) \to \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \tag{4.6}$$

и

$$\psi : \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \to \widehat{F}_{a_1}(S) \times \cdots \times \widehat{F}_{a_m}(S). \tag{4.7}$$

Построим инъекцию φ.

Для любых $(f_1, \ldots f_m) \in \widehat{F}_{a_1}(S) \times \cdots \times \widehat{F}_{a_m}(S)$ положим

$$\varphi(f_1, \ldots f_m) = f,$$

где $f \in F(S)$ – такое отображение, что $f(s)$ ($s \in S$) представляет собой элемент $a \in \mathrm{MOD}\left(\prod_{i=1}^{m} a_i\right)$, содержащийся в блоке

$$B = \bigcap_{i=1}^{m} B_i$$

разбиения $\pi\left(K, \left(\prod_{i=1}^{m} a_i\right)\right)$, где $B_1, \ldots, B_m$ – такие блоки, соответственно, разбиений

$$\pi(K, (a_1)), \ldots, \pi(K, (a_m)),$$

что элемент $f_i(s) \in \mathrm{MOD}(a_i)$ принадлежит блоку B_i.

Такое определение отображения φ корректно в силу следствия 4.1.

Так как

$$f_{\bmod a_i} = f_i \ (i = 1, \ldots, m),$$

то $f \in \widehat{F}_{a_i}(S)$ $(i = 1, \ldots, m)$.

Следовательно, $f \in \bigcap\limits_{i=1}^{m} \widetilde{F}_{a_i}(S)$, т.е. отображение φ является отображением вида (4.6).

А так как

$$(f_1^{(1)}, \ldots, f_m^{(1)}) \neq (f_1^{(2)}, \ldots, f_m^{(2)}) \Rightarrow \varphi(f_1^{(1)}, \ldots, f_m^{(1)}) \neq \varphi(f_1^{(2)}, \ldots, f_m^{(2)}),$$

то отображение φ – инъекция.

Построим инъекцию ψ.

Для любого $f \in \bigcap\limits_{i=1}^{m} \widetilde{F}_{a_i}(S)$ положим

$$\psi(f) = (f_{\bmod a_1}, \ldots, f_{\bmod a_m}).$$

Так как

$$f \in \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \Leftrightarrow (\forall i = 1, \ldots, m)(f \in \widetilde{F}_{a_i}(S)) \Leftrightarrow$$

$$\Leftrightarrow (\forall i = 1, \ldots, m)(f_{\bmod a_i} \in \widehat{F}_{a_i}(S)) \Leftrightarrow$$

$$\Leftrightarrow (f_{\bmod a_1}, \ldots, f_{\bmod a_m}) \in \widehat{F}_{a_1}(S) \times \cdots \times \widehat{F}_{a_m}(S),$$

то отображение ψ является отображением вида (4.7).

Пусть $f \neq g$ $(f, g \in \bigcap\limits_{i=1}^{m} \widetilde{F}_{a_i}(S))$.

Тогда существует такой элемент $s \in S$, что $f(s) \neq g(s)$.

Это означает, что элементы $f(s)$ и $g(s)$ принадлежат разным блокам B' и B'' разбиения $\pi\left(K, \left(\prod\limits_{i=1}^{m} a_i\right)\right)$.

Так как (в силу следствия 4.1) блоки разбиения $\pi\left(K, \left(\prod\limits_{i=1}^{m} a_i\right)\right)$ являются пересечениями блоков разбиений

$$\pi(K, (a_1)), \ldots, \pi(K, (a_m)),$$

то

$$B' = \bigcap_{i=1}^{m} B'_i,$$

$$B'' = \bigcap_{i=1}^{m} B''_i,$$

где B'_i, B''_i $(i = 1, \ldots, m)$ – блоки разбиения $\pi(K, (a_i))$.

Следовательно, из того, что $B' \neq B''$ вытекает, что существует такое $j \in \{1, \ldots, m\}$, что $B'_i \neq B''_i$. Это означает, что $f_{\bmod a_j}(s)$ и $g_{\bmod a_j}(s)$ являются различными элементами множества $\mathrm{MOD}(a_j)$.

Поэтому

$$f_{\bmod a_j} \neq g_{\bmod a_j},$$

откуда вытекает, что

$$\psi(f) \neq \psi(g).$$

Так как

$$(\forall f, g \in \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S))(f \neq g \Rightarrow \psi(f) \neq \psi(g)),$$

то отображение ψ – инъекция.

□

Если $\widehat{F}_{a_i}(S)$ $(i = 1, \ldots, m)$ – конечные множества, то равенство (4.5) естественно записать в виде

$$\prod_{i=1}^{m} |\widehat{F}_{a_i}(S)| = \left| \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \right|. \tag{4.8}$$

4.1.3. Применение построенной схемы к решению алгебраических и теоретико-числовых задач.

Рассмотрим применение равенств (4.5) и (4.8) для решения модельных алгебраических и теоретико-числовых задач.

Пример 4.1. Пусть $a_1, \ldots, a_m$ $(m \in \mathbf{N})$ – попарно взаимно простые элементы дедекиндового кольца $\mathcal{K}$.

В [40] установлен изоморфизм фактор-колец, специальным случаем которого является изоморфизм

$$\mathcal{K}/_{\prod_{i=1}^{m}(a_i)} \leftrightarrow \prod_{i=1}^{m} \mathcal{K}/_{(a_i)}.$$

Пусть

$$|S| = 1.$$

Тогда множество $F_{a_i}(S)$ $(i = 1, \ldots, m)$ можно отождествить с множеством $\mathrm{MOD}(a_j)$.

Положив

$$\widehat{F}_{a_i}(S) = F_{a_i}(S) \ (i = 1, \ldots, m),$$

заключаем, что если $|S| = 1$, то равенство (4.5) устанавливает равномощность фактор-колец $\mathcal{K}/_{\prod\limits_{i=1}^{m}(a_i)}$ и $\prod\limits_{i=1}^{m}\mathcal{K}/_{(a_i)}$, а отображения φ и $\psi = \varphi^{-1}$, построенные при доказательстве теоремы 4.1, устанавливают изоморфизм этих фактор-колец.

Пример 4.2. Пусть $a_1, \ldots, a_m$ $(m \in \mathbf{N})$ – попарно взаимно простые элементы дедекиндового кольца $\mathcal{K}$, а $|S| = 1$.

Зафиксируем произвольные элементы $b_1, \ldots, b_m$ кольца $\mathcal{K}$ и положим

$$\widehat{F}_{a_i}(S) = \{f_i\} \ (i = 1, \ldots, m),$$

где

$$f_i(s) = b_i < \mathrm{mod}\ a_i > \ \ (i = 1, \ldots, m).$$

В рассматриваемом случае равенство (4.8) принимает вид

$$\left|\bigcap_{i=1}^{m}\widetilde{F}_{a_i}(S)\right| = 1.$$

При этом $f \in \bigcap\limits_{i=1}^{m}\widetilde{F}_{a_i}(S)$ представляет собой такое отображение, что $f(s)$ – это такой единственный элемент $c \in \mathrm{MOD}\left(\prod\limits_{i=1}^{m}a_i\right)$, что

$$c = b_i < \mathrm{mod}\ a_i >$$

для всех $i = 1, \ldots, m$.

Таким образом, показано, что система сравнений

$$x \equiv b_i \ (\mathrm{mod}\ (a_i)) \ (i = 1, \ldots, m)$$

имеет единственное решение, принадлежащее множеству $\mathrm{MOD}\left(\prod\limits_{i=1}^{m}a_i\right)$, т.е. доказан вариант китайской теоремы об остатках для дедекиндовых колец.

Пример 4.3. Обратимые матрицы над кольцом $\mathcal{Z}_n = (\mathbf{Z}_n\oplus, \circ)$ $(n \in \mathbf{N}\backslash\{1\})$ играют важную роль при поиске множеств решений некоторых систем (в том числе и нелинейных) уравнений. Кроме того, в [52] показано, что в терминах таких матриц могут быть охарактеризованы основные нетривиальные множества обратимых автоматов над кольцом $\mathcal{Z}_n$.

Из сказанного вытекает, что число обратимых матриц над кольцом $\mathcal{Z}_n$ используется при оценке мощности достаточно широкого класса множеств, определенных в терминах кольца $\mathcal{Z}_n$ ($n \in \mathbf{N}\backslash\{1\}$).

В [53] показано, что схема подсчета числа обратимых $l \times l$-матриц над кольцом $\mathcal{Z}_n$ ($n \in \mathbf{N}\backslash\{1\}$) может быть представлена в следующем виде.

Обозначим через $\mathsf{M}_l(p,k)$ (где p – простое число, а $k \in \mathbf{N}$) множество всех $l \times l$-матриц над кольцом $\mathcal{Z}_{p^k}$, а через $\mathsf{M}_l^{inv}(p,k)$ – множество всех обратимых матриц $A \in \mathsf{M}_l(p,k)$. Ясно, что

$$|\mathsf{M}_l(p,k)| = p^{kl^2}.$$

Пусть $k = 1$. Из непосредственного анализа для столбцов матрицы $A \in \mathsf{M}_l^{inv}(p,1)$ свойства «быть линейно независимыми» вытекает, что

$$|\mathsf{M}_l^{inv}(p,1)| = |\mathsf{M}_l(p,1)| \prod_{i=1}^{l}(1 - p^{-l}).$$

Пусть $k \geq 2$. Любая матрица $A \in \mathsf{M}_l^{inv}(p,k)$ единственным образом может быть представлена в виде

$$A = B \oplus C,$$

где $B \in \mathsf{M}_l^{inv}(p,1)$, а матрица C представляет собой $l \times l$-матрицу над кольцом $\mathcal{Z}_{p^k}$, у которой каждый элемент является необратимым элементом кольца $\mathcal{Z}_{p^k}$.

Следовательно,

$$|\mathsf{M}_l^{inv}(p,k)| = |\mathsf{M}_l(p,k)| \prod_{i=1}^{l}(1 - p^{-l}).$$

Для любого числа $n = p_1^{k_1} \ldots p_m^{k_m}$, где $m \geq 2$, а $p_1, \ldots, p_m$ – попарно-различные простые числа, мощность множества $\mathsf{M}_l^{inv}(n)$ всех обратимых $l \times l$-матриц над кольцом $\mathcal{Z}_n$ может быть вычислена следующим образом.

Пусть в качестве дедекиндового кольца $\mathcal{K}$ выбрано кольцо целых чисел $\mathcal{Z}$, а в качестве множества S – множество, состоящее из l^2 элементов.

В рассматриваемом случае множество отображений $F_{p_i^{k_i}}(S)$ ($i = 1, \ldots, m$) может быть отождествлено с множеством матриц $\mathsf{M}_l(p_i, k_i)$.

Пусть в качестве множества отображений $\widehat{F}_{p_i^{k_i}}(S)$ ($i = 1, \ldots, m$) выбрано множество матриц $\mathsf{M}_l^{inv}(p_i, k_i)$.

Тогда множество отображений $\widetilde{F}_{p_i^{k_i}}(S)$ ($i = 1, \ldots, m$) состоит из всех $l \times l$-матриц над кольцом $\mathcal{Z}_n$, определитель которых не сравним с нулем по модулю p_i.

Отсюда вытекает, что

$$\mathsf{M}_l^{inv}(n) = \bigcap_{i=1}^{m} \widetilde{F}_{p_i^{k_i}}(S).$$

Применив равенство (4.8), получим

$$|\mathsf{M}_l^{inv}(n)| = \left(\prod_{i=1}^{m} |\mathsf{M}_l(p_i, k_i)|\right) \prod_{j=1}^{m} \prod_{i=1}^{l} (1 - p_j^{-i}).$$

4.1.4. Ленточная модель.

Рассмотрим случай, когда в качестве дедекиндового кольца $\mathcal{K}$ выбрано кольцо целых чисел $\mathcal{Z}$, в качестве множества S – одноэлементное множество.

Зафиксируем попарно взаимно простые числа $a_1, \ldots, a_m \in \mathbf{N}\backslash\{1\}$ и, как это обычно делается, положим

$$\mathrm{MOD}(a_i) = \{0, 1, \ldots, a_i - 1\} \ (i = 1, \ldots, m).$$

Выберем любые такие неотрицательные целые числа $b_1, \ldots, b_m$, что $b_i \leq a_i$ для всех $i = 1, \ldots, m$.

В случае, когда

$$|\widehat{F}_{a_i}(S)| = b_i \ (i = 1, \ldots, m),$$

равенство (4.8) принимает следующий вид

$$\left| \bigcap_{i=1}^{m} \widetilde{F}_{a_i}(S) \right| = \prod_{i=1}^{m} b_i. \tag{4.9}$$

Равенство (4.9) имеет содержательную интерпретацию в терминах следующей геометрической модели, впервые исследованной в [54], которую назовем ленточной моделью.

Под *лентой* будем понимать одностороннюю бесконечную вправо ленту, разбитую на клетки, занумерованные неотрицательными целыми числами.

Расположив $m + 1$ лент одну над другой, занумеруем их сверху вниз неотрицательными целыми числами.

Ленты с номерами $1, \ldots, m$ назовем *рабочими*, а ленту с номером 0 – *результирующей.*

Осуществим разметку лент маркером в соответствии со следующими правилами.

Правило 4.1. Среди первых a_i $(i = 1, \ldots, m)$ клеток рабочей ленты с номером i отметим маркером те и только те b_i клеток, номера которых являются значениями отображений, принадлежащих множеству $\widehat{F}_{a_i}(S)$.

Правило 4.2. На рабочей ленте с номером i $(i = 1, \ldots, m)$ клетка с номером h $(h \geq a_i)$ отмечена маркером тогда и только тогда, когда маркером отмечена клетка с номером $h <\bmod a_i>$ этой ленты.

Правило 4.3. На результирующей ленте клетка с номером j $(j \in \mathbf{Z}_+)$ отмечена маркером тогда и только тогда, когда на каждой рабочей ленте клетка с номером j отмечена маркером.

Замечание 4.3. Из правил 4.1-4.3 вытекает, что все многообразие разметок лент определяется правилом 4.1, т.е. выбором семейства множеств отображений $\widehat{F}_{a_i}(S)$ $(i = 1, \ldots, m)$.

Обозначим через $\mathtt{L}_i$ $(i = 0, 1, \ldots, m)$ начальный отрезок ленты с номером i, состоящий из первых $\prod\limits_{i=1}^{m} a_i$ клеток.

Назовем *ленточной моделью* упорядоченный набор лент

$$(\mathtt{L}_0; \mathtt{L}_1, \ldots, \mathtt{L}_m). \tag{4.10}$$

В терминах ленточной модели формулировка равенства (4.9) имеет следующий вид.

Теорема 4.2. (*Ленточная теорема*). Для любых попарно взаимно простых чисел $a_1, \ldots, a_m \in \mathbf{N}\backslash\{1\}$ $(m \in \mathbf{N})$ при любых таких неотрицательных целых числах $b_1, \ldots, b_m$, что $b_i \leq a_i$ для всех $i = 1, \ldots, m$, в точности $\prod\limits_{i=1}^{m} b_i$ клеток результирующей ленты $\mathtt{L}_0$ отмечено маркером.

Замечание 4.4. В [54] ленточная модель исследована непосредственно, без использования разработанного выше математического аппарата.

Содержащееся в [54] доказательство теоремы 4.2 «в лоб» достаточно длинное и громоздкое, и основано на комбинации метода решета и индукции по числу рабочих лент.

Проиллюстрируем применение ленточной модели при решении модельных теоретико-числовых задач.

Пример 4.4. Пусть φ – функции Эйлера (т.е. $\varphi(1) = 1$ и $\varphi(n)$ $(n \in \mathbf{N}\backslash\{1\})$ – количество натуральных чисел, меньших числа n, и взаимно простых с числом n).

Докажем следующее свойство мультипликативности функции φ: для любых взаимно простых чисел $k_1, k_2 \in \mathbf{N}\backslash\{1\}$ истинно равенство

$$\varphi(k_1 k_2) = \varphi(k_1)\varphi(k_2).$$

Положив $m = 2$ в (4.10), построим такую ленточную модель

$$(\mathtt{L}_0; \mathtt{L}_1, \mathtt{L}_2),$$

что $a_i = k_i$ $(i = 1, 2)$, а множество $\widehat{F}_{a_i}(S)$ $(i = 1, 2)$ состоит из всех отображений $f \in F_{a_i}(S)$, значением которых является число, взаимно простое с числом a_i.

Для построенной модели

$$b_i = \varphi(a_i) \ (i = 1, 2),$$

а среди первых a_i $(i = 1, 2)$ клеток рабочей ленты $\mathtt{L}_i$ маркером отмечены те и только те b_i клеток, номерами которых являются числа, взаимно простые с числом a_i.

Так как числа a_1 и a_2 – взаимно простые, то число $a \in \mathbf{N}$ взаимно просто с произведением $a_1 a_2$ тогда и только тогда, когда оно взаимно просто с каждым из чисел a_1 и a_2.

Следовательно, клетка результирующей ленты $\mathtt{L}_0$ отмечена маркером тогда и только тогда, когда ее номером является число, взамно простое с произведением $a_1 a_2$.

Отсюда вытекает, что число клеток результирующей ленты $\mathtt{L}_0$, отмеченных маркером, равно $\varphi(a_1 a_2)$.

Применяя ленточную теорему, получим, что

$$\varphi(k_1 k_2) = \varphi(a_1 a_2) = b_1 b_2 = \varphi(k_1)\varphi(k_2),$$

что и требовалось доказать.

Пример 4.5. Пусть φ – функции Эйлера.

Докажем формулу Эйлера: если $n = p_1^{k_1} \dots p_m^{k_m}$ $(n \in \mathbf{N}\backslash\{1\})$ – каноническое разложение числа n, то

$$\varphi(n) = n \prod_{i=1}^{m} (1 - p_i^{-1}). \tag{4.11}$$

По условию, числа $p_1^{k_1}, \dots, p_m^{k_m}$ являютя взаимно простыми.

Построим такую ленточную модель (4.10), что

$$a_i = p_i^{k_i} \ (i = 1, \dots, m),$$

а множество $\widehat{F}_{a_i}(S)$ $(i = 1, \dots, m)$ состоит из всех отображений $f \in F_{a_i}(S)$, значением которых является число, взаимно простое с числом a_i.

Для построенной модели

$$b_i = \varphi(a_i) \ (i = 1, \dots, m),$$

а среди первых a_i $(i = 1, \dots, m)$ клеток рабочей ленты $\mathtt{L}_i$ маркером отмечены те и только те b_i клеток, номера которых – числа, взаимно простые с числом a_i.

Так как числа $a_1, \ldots, a_m$ – взаимно простые, то число $a \in \mathbf{N}$ взаимно просто с произведением $\prod\limits_{i=1}^{m} a_i$ тогда и только тогда, когда оно взаимно просто с каждым из чисел $a_1, \ldots, a_m$.

Следовательно, клетка результирующей ленты $\mathtt{L}_0$ отмечена маркером тогда и только тогда, когда ее номер – число, взамно простое с произведением $\prod\limits_{i=1}^{m} a_i$.

Отсюда вытекает, что число клеток результирующей ленты $\mathtt{L}_0$, отмеченных маркером, равно $\varphi(\prod\limits_{i=1}^{m} a_i)$.

Применяя ленточную теорему, получим, что

$$\varphi(n) = \varphi\left(\prod_{i=1}^{m} a_i\right) = \prod_{i=1}^{m} b_i = \prod_{i=1}^{m} \varphi(p_i^{k_i}). \tag{4.12}$$

Воспользовавшись в (4.12) равенствами

$$\varphi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i-1} \ \ (i = 1, \ldots, m),$$

получим

$$\varphi(n) = \prod_{i=1}^{m}(p_i^{k_i} - p_i^{k_i-1}) = \left(\prod_{i=1}^{m} p_i^{k_i}\right) \prod_{i=1}^{m}(1 - p_i^{-1}) = n \prod_{i=1}^{m}(1 - p_i^{-1}),$$

т.е. равенство (4.11) истинно.

Пример 4.6. Докажем следующий вариант китайской теоремы об остатках: если числа $k_1, \ldots k_m \in \mathbf{N}\backslash\{1\}$ являются попарно взаимно простыми числами, то для любых чисел $c_1, \ldots, c_m \in \mathbf{Z}$ система сравнений

$$x \equiv c_i \ (mod\ k_i) \ \ (i = 1, \ldots, m) \tag{4.13}$$

имеет единственное решение по модулю $\prod\limits_{i=1}^{m} k_i$.

Обозначив через r_i $(i = 1, \ldots, m)$ остаток от деления числа c_i на число k_i, перейдем от системы сравнений (4.13) к эквивалентной системе сравнений

$$x \equiv r_i \ (mod\ k_i) \ \ (i = 1, \ldots, m). \tag{4.14}$$

Построим такую ленточную модель (4.10), что

$$a_i = k_i \ \ (i = 1, \ldots, m),$$

а множество $\widehat{F}_{a_i}(S)$ $(i = 1, \ldots, m)$ состоит из единственного отображения $f \in F_{a_i}(S)$, значением которого является число r_i.

Для построенной модели

$$b_i = 1 \ \ (i = 1, \ldots, m),$$

а среди первых a_i $(i = 1, \dots, m)$ клеток рабочей ленты $\mathtt{L}_i$ маркером отмечена единственная клетка, номер которой равен r_i.

Следовательно, клетка с номером j $(j = 0, 1, \dots, \prod\limits_{i=1}^{m} a_i - 1)$ результирующей ленты $\mathtt{L}_0$ отмечена маркером тогда и только тогда, когда число j сравнимо с каждым из чисел r_i $(i = 1, \dots, m)$ по модулю a_i.

Отсюда вытекает, что число j является решением системы сравнений (4.14), т.е. решением системы сравнений (3.13).

Применяя ленточную теорему, получим, что число решений системы сравнений (4.13) по модулю $\prod\limits_{i=1}^{m} k_i$ равно

$$\prod_{i=1}^{m} b_i = \prod_{i=1}^{m} 1 = 1,$$

что и требовалось доказать.

Пример 4.7. В теореме 4.1 используется конечный набор попарно взаимно простых $a_1, \dots, a_m$ $(m \in \mathbf{N})$ дедекиндового кольца $\mathcal{K}$.

Ленточная модель дает возможность достаточно просто доказать, что теорема 4.1 не может быть непосредственно обобщена на бесконечный набор попарно взаимно простых элементов a_i $(i \in \mathbf{N})$ дедекиндового кольца $\mathcal{K}$, т.е. что ложно утверждение:

Утверждение 4.1. Для любого множества S и произвольного бесконечного набора попарно взаимно простых элементов a_i $(i \in \mathbf{N})$ дедекиндового кольца $\mathcal{K}$ истинно равенство

$$\left| \prod_{i=1}^{\infty} \widehat{F}_{a_i}(S) \right| = \left| \bigcap_{i=1}^{\infty} \widetilde{F}_{a_i}(S) \right|.$$

Для того, чтобы показать, что утверждение 4.1 не является истинным, достаточно доказать, что для обобщения ленточной модели на бесконечно число лент, т.е. для ленточной модели

$$(\mathtt{L}_0; \mathtt{L}_1, \dots, \mathtt{L}_m, \dots) \tag{4.15}$$

не является истинным следующее обобщение теоремы 4.2.

Утверждение 4.2. Для любой последовательности попарно взаимно простых чисел $a_i \in \mathbf{N}\backslash\{1\}$ $(i \in \mathbf{N})$ при любых таких неотрицательных числах b_i $(i \in \mathbf{N})$, что $b_i \leq a_i$ для всех $i \in \mathbf{N}$ в точности $\prod\limits_{r=1}^{\infty} b_r$ клеток результирующей ленты $\mathtt{L}_0$ отмечено маркером.

Построим следующую обобщенную ленточную модель (4.15).

Зафиксируем возрастающую последовательность попарно взаимно простых чисел $a_i \in \mathbf{N}\backslash\{1\}$ $(i \in \mathbf{N})$, а множества отображений $\widehat{F}_{a_i}(S)$ $(i \in \mathbf{N})$ выберем так, что:

1) множество $\widehat{F}_{a_1}(S)$ состоит из любого одного отображения $f \in F_{a_1}(S)$;

2) для каждого $i \geq 2$ множество $\widehat{F}_{a_i}(S)$ состоит из любого одного такого отображения $f \in F_{a_i}(S)$, что $a_{i-1} \leq f(s) < a_i$.

Так как $b_i = 1$ для всех $i \in \mathbf{N}$, то

$$\prod_{i=1}^{\infty} b_i = 1.$$

Покажем, что ни одна из клеток результирующей ленты $\mathtt{L}_0$ не отмечена маркером.

Предположим противное, т.е. что существует такое число $j \in \mathbf{Z}_+$, что клетка с номером j результирующей ленты отмечена маркером.

Так как $\{a_i\}_{i\in\mathbf{N}}$ – возрастающая последовательность натуральных чисел, то существует такое число $i_0 \in \mathbf{N}$, что $a_{i_0} > j$.

Так как клетка с номером j рабочей ленты $\mathtt{L}_{i_0+1}$ не отмечена маркером, то клетка с номером j результирующей ленты также отмечена маркером.

Получено противоречие.

Полученное противоречие показывает, что не является истинным предположение о том, что существует такое число $j \in \mathbf{Z}_+$, что клетка с номером j результирующей ленты отмечена маркером.

Следовательно, ни одна из клеток результирующей ленты не отмечена маркером, откуда вытекает,что утверждение 4.2 не является истинным, что и требовалось доказать.

4.2. Схема решения систем полиномиальных уравнений над конечным кольцом.

Решение систем линейных уравнений над полем $\mathcal{GF}(p^k)$ не вызывает особых затруднений. Однако ситуация в корне изменяется при решениии систем нелинейных уравнений над этим полем. Известно, что над полем $\mathcal{GF}(p^k)$ задача решения систем квадратных уравнений от многих переменных, даже в случае, когда $p = 2$, является NP-полной. Ситуация еще больше усложняется при решении систем полиномиальных уравнений с параметрами над кольцом $\mathcal{K}$, что обусловлено, прежде всего, наличием делителей нуля.

Поэтому разработка схем, предназначенных для эффективного решения узких классов систем полиномиальных уравнений с параметрами является достаточно актуальной.

4.2.1. Основные понятия.

Построим алгебраическую систему, предназначенную для упрощения процесса решения системы полиномиальных уравнений с параметрами

$$\begin{cases} f_1(u_1, \ldots, u_n, a_1, \ldots, a_h) = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f_l(u_1, \ldots, u_n, a_1, \ldots, a_h) = 0 \end{cases}, \qquad (4.16)$$

над кольцом $\mathcal{K} = (K, +, \cdot)$, где $u_1, \ldots, u_n$ – переменные, а $a_1, \ldots, a_h \in K$ – параметры.

Обозначим через $\mathtt{B}$ множество классов ассоциированных элементов кольца $\mathcal{K}$, через $< x >$ $(x \in K)$ – класс элементов кольца $\mathcal{K}$, ассоциированных с элементом x, а через $\mathcal{G} = (K^{inv}, \cdot)$ – мультипликативную группу кольца $\mathcal{K}$.

Тогда

$$\mathtt{B} = \{< 0 >, < 1 >, \mathtt{B}'\},$$

где $< 0 >= \{0\}$, $< 1 >= K^{inv}$, а множество

$$\mathtt{B}' = \{< x > | x \in (K \backslash \{0\}) \backslash K^{inv}\}$$

представляет собой множество классов, ассоциированных с необратимыми элементами кольца $\mathcal{K}$.

Далее будем считать, что $|K^{inv}| > 1$ и $|\mathtt{B}'| > 1$.

Определим на множестве $\mathtt{B}$ операцию умножения равенством

$$< x > \cdot < y >=< xy > \ \ (x, y \in K). \tag{4.17}$$

Такое определение корректно, так как

$$< x >= K^{inv} x \ (x \in K).$$

Отсюда вытекает, что $(\mathtt{B}, \cdot)$ – коммутативная полугруппа.

Положим

$$\mathtt{B}_0 = \{< x > | x \text{ неприводимый элемент кольца } \mathcal{K}\}.$$

В дальнейшем предполагается, что каждый элемент множества $\mathtt{B}'$ единственным образом (с точностью до ассоциированного разложения) может быть представлен в виде произведения элементов, принадлежащих множеству $\mathtt{B}_0$.

Замечание 4.5. Следует отметить, что это требование являтся более слабым, чем требование «$(\mathtt{B}, \cdot)$ – гауссова полугруппа», так как не требуется выполнения «закона сокращения», который не имеет места даже в случае кольца $\mathcal{Z}_{p^k}$ $(k \geq 3)$.

Определим сумму элементов множества $\mathtt{B}$ равенством

$$< x > + < y >=$$

$$= \{< z > \in \mathtt{B} | (\exists a \in < x >)(\exists b \in < y >)(a + b \in < z >)\}. \tag{4.18}$$

Замечание 4.6. Равенство (4.18) определяет во множестве $\mathtt{B}$ тернарное отношение, а не бинарную операцию (в алгебраическом смысле этого слова), что, в частности, истинно, даже если $\mathcal{K} = \mathcal{Z}_{p^k}$ $(k \geq 3)$.

Отметим, что из (4.18) вытекает, что

$$< x > + < y >=< y > + < x >,$$

для любых $x, y \in K$.

Таким образом, осуществлен переход от кольца $\mathcal{K} = (K, +, \cdot)$ к алгебраической системе

$$\mathcal{B} = (\mathtt{B}, \cdot, +).$$

Рассмотрим применение алгебраической системы $\mathcal{B}$ в процессе решения системы уравнений (4.16).

4.2.2. Общая схема.

Заменим в системе уравнений (4.16) элементы кольца $\mathcal{K}$ элементами множества $\mathtt{B}$, а операции в кольце $\mathcal{K}$ – действиями в алгебраической системе $\mathcal{B}$, определяемыми равенствами (4.17) и (4.18).

Получим систему уравнений над алгебраической системой $\mathcal{B}$

$$\begin{cases} f_1(< u_1 >, \ldots, < u_n >, < a_1 >, \ldots, < a_h >) = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_l(< u_1 >, \ldots, < u_n >, < a_1 >, \ldots, < a_h >) = 0 \end{cases} . \qquad (4.19)$$

Представим элементы $< a_1 >, \ldots, < a_h > \in \mathtt{B}$ в виде произведения элементов, принадлежаших множеству $\mathtt{B}_0$.

Найдем множество $\mathtt{S}$ решений системы уравнений (4.19), где для каждого решения

$$\mathtt{u} = (< u_1 >, \ldots, < u_n >) \in \mathtt{S} \qquad (4.20)$$

каждый элемент $< u_i > \in \mathtt{B}$ $(i = 1, \ldots, n)$ представлен в виде суммы произведений элементов, принадлежащих множеству $\mathtt{B}_0$.

Исходя из множества $\mathtt{S}$ построим множество S решений системы уравнений (4.16).

Для этого достаточно для каждого решения (4.20) построить множество

$$S_{\mathtt{u}} = \{(u_1^{(0)}, \ldots, u_n^{(0)}) | u_i^{(0)} \in < u_i^{(0)} > \ \ (i = 1, \ldots, n)\}$$

и выделить в нем (например, подстановкой в (4.16)) элементы, принадлежащие множеству S.

Ясно, что сложность предложенной схемы во многом определяется именно сложностью поиска, осуществляемого при построении множества S из множества $\mathtt{S}$.

Отсюда вытекает, что предложенная схема будет эффективной при построении множества решений системы уравнений (4.16), если указанный поиск отсутствует вообще, либо если его сложность невелика.

Отметим, что предложенная выше схема решения системы полиномиальных уравнений над кольцом $\mathcal{K}$ дает возможность осуществить качественный анализ структуры множества S решений системы уравнений уравнений (4.16), а именно: охарактеризовать множество S в терминах классов ассоциированных элементов кольца $\mathcal{K}$.

4.2.3. Классы ассоциированных элементов кольца $\mathcal{Z}_{p^k}$.

Рассмотрим кольцо $\mathcal{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$, где p – простое число, а $k \in \mathbf{N}$ $(k \geq 2)$.

В замечании 1.24 определен (см. формулу (1.1)) p-тип $\mathtt{t}_p(z)$ элемента $z \in \mathbf{Z}_{p^k}$ кольца $\mathcal{Z}_{p^k}$ и отмечено, что для того, чтобы задать класс C_r $(r = 0, 1, \ldots, k)$ ассоциированных элементов кольца $\mathcal{Z}_{p^k}$, достаточно зафиксировать p-тип $\mathtt{t}_p(z)$ элемента, принадлежащего этому классу.

При этом:

1) p-тип, равный 0, определяет класс C_0 ассоциированных элементов, состоящий из обратимых элементов кольца $\mathcal{Z}_{p^k}$, т.е.

$$C_0 = \mathbf{Z}_{p^k}^{inv};$$

2) p-тип, равный k, определяет одноэлементный класс ассоциированных элементов, состоящий из нуля 0 кольца $\mathcal{Z}_{p^k}$, т.е.

$$C_k = \{0\}.$$

Следующее утверждение характеризует класс C_r $(r = 1, \ldots, k-1)$ ассоциированных элементов кольца $\mathcal{Z}_{p^k}$, для которых p-тип равен r.

Утверждение 4.3. Для любого числа $r = 1, \ldots, k-1$ класс C_r ассоциированных элементов кольца $\mathcal{Z}_{p^k}$, для которых p-тип равен r, определяется равенством

$$C_r = \{\alpha \circ p^r | \alpha \in \mathbf{Z}_{p^{k-r}}^{inv}\} \ (r = 1, \ldots, k-1).$$

Доказательство. Разложив элемент $a \in \mathbf{Z}_{p^k}$ $(a \neq 0)$ по степеням числа p, получим

$$a = \sum_{i=0}^{k-1} \beta_i p^i, \tag{4.21}$$

где $\beta_i \in \mathbf{Z}_p$ $(i = 0, 1, \ldots, k-1)$.

Отметим, что так как $\beta_i \in \mathbf{Z}_p$ $(i = 0, 1, \ldots, k-1)$, то $\beta_i \in \mathbf{Z}_p^{inv}$ (а, следовательно, $\beta_i \in \mathbf{Z}_{p^k}^{inv}$) тогда и только тогда, когда $\beta_0 \neq 0$.

Из определения p-типа элемента кольца $\mathcal{Z}_{p^k}$ вытекает (формула (1.1)), что если элемент $a \in \mathbf{Z}_{p^k}$ представлен в виде (4.21), то

$$(\forall r = 1, \ldots, k-1)(\mathtt{t}_p(a) = r) \Leftrightarrow$$

$$\Leftrightarrow (\forall j = 0, 1, \ldots, r-1)(\beta_j = 0) \& (\beta_r \neq 0).$$

Следовательно, если элемент $a \in \mathbf{Z}_{p^k}$ представлен в виде (4.21), то

$$\mathtt{t}_p(a) = r \Leftrightarrow \left(a = \sum_{i=r}^{k-1} \beta_i p^i\right) \& (\beta_r \neq 0) \Leftrightarrow$$

$$\Leftrightarrow \left(a = p^r \circ \left(\sum_{i=0}^{k-r-1} \beta_{i+r} p^i\right)\right) \& (\beta_r \neq 0) \Leftrightarrow$$

$$\Leftrightarrow \left(a = p^r \circ \left(\sum_{i=0}^{k-r-1} \beta_{i+r} p^i\right)\right) \& \left(\left(\sum_{i=0}^{k-r-1} \beta_{i+r} p^i\right) \in \mathbf{Z}_{p^{k-r}}^{inv}\right).$$

□

Отметим, что для классов C_r $(r = 0, 1, \ldots, k)$ ассоциированных элементов кольца $\mathcal{Z}_{p^k}$ истинны следующие равенства, связанные с операцией умножения этих классов

$$C_r \circ C_0 = C_0 \circ C_r = C_r \ (r = 0, 1, \ldots, k), \tag{4.22}$$

$$C_r \circ C_k = C_k \circ C_r = C_k \ (r = 0, 1, \ldots, k), \tag{4.23}$$

$$C_{r_1} \circ C_{r_2} = \begin{cases} C_{r_1+r_2}, & \text{если } r_1 + r_2 < k \\ C_k, & \text{если } r_1 + r_2 \geq k \end{cases} \tag{4.24}$$

для любых чисел $r_1, r_2 = 1, \ldots, k-1$.

Кроме того, истинно равенство

$$C_{r_1} \circ p^{r_2} = p^{r_2} \circ C_{r_1} = \begin{cases} C_{r_1+r_2}, & \text{если } r_1 + r_2 \leq k \\ C_k, & \text{если } r_1 + r_2 > k \end{cases} \tag{4.25}$$

для любых чисел $r_1, r_2 = 1, \ldots, k$.

Для классов C_r $(r = 0, 1, \ldots, k)$ ассоциированных элементов кольца $\mathcal{Z}_{p^k}$ также истинны следующие равенства, связанные с суммой этих классов

$$C_r \oplus C_0 = C_0 \oplus C_r = C_0 \ (r = 1, \ldots, k), \tag{4.26}$$

$$C_r \oplus C_k = C_k \oplus C_r = C_r \ (r = 0, 1, \ldots, k) \tag{4.27}$$

и

$$C_{r_1} \oplus C_{r_2} = C_{r_2} \oplus C_{r_1} = \begin{cases} p^{r_1} \circ (C_0 \oplus C_{r_2-r_1}), & \text{если } r_1 \leq r_2 \\ p^{r_2} \circ (C_0 \oplus C_{r_1-r_2}), & \text{если } r_1 > r_2 \end{cases} \tag{4.28}$$

для любых чисел $r_1, r_2 = 1, \ldots, k-1$.

Отметим, что именно равенства (4.22)-(4.28) и дают возможность эффективно представлять множества решений систем полиномиальных уравнений с парачетрами над кольцом вычетов $\mathcal{Z}_{p^k}$.

4.3. Решение систем уравнений над кольцом $\mathcal{Z}_{p^k}$.

Проиллюстрируем применение предложенной в п.4.2 схемы решения систем полиномиальных уравнений с параметрами над конечным кольцом $\mathcal{K}$ в случае, когда $\mathcal{K} = \mathcal{Z}_{p^k}$.

4.3.1. Решение систем линейных уравнений.

Рассмотрим вначале линейное уравнение над кольцом $\mathcal{Z}_{p^k}$

$$a \circ x = b, \tag{4.29}$$

где $a, b \in \mathbf{Z}_{p^k}$ – параметры.

Переходя к уравнению в алгебраической системе $\mathcal{B}$, получим

$$C_{r_1} \circ C_{r_2} = C_{r_3}. \tag{4.30}$$

где $r_1, r_2, r_3 \in \{0, 1, \ldots, k\}$.

Из (4.22)-(4.24) вытекает, что:

1) если $r_3 < r_1$, то уравнение (4.30) (а, значит, и уравнение (4.29)) решений не имеет;

2) если $r_1 = 0$, то $r_2 = r_3$;

3) если $r_1 = k$, то $r_3 = k$, а r_2 может быть произвольным элементом множества $\{0, 1, \ldots, k\}$;

4) если $r_1, r_3 \in \{1, \ldots, k-1\}$, то $r_3 \geq r_1$ и $r_2 = r_3 - r_1$;

5) $r_1 \in \{1, \ldots, k-1\}$, а $r_3 = k$, то r_2 может быть произвольным элементом множества $\{k - r_1, \ldots, k\}$.

Из сказанного выше вытекает, что для поиска множества S решений уравнения (4.29) необходимо рассмотреть следующие ситуации.

1. Пусть $a \in \mathbf{Z}_{p^k}^{inv}$. Тогда уравнение (4.29) имеет единственное решение

$$x = a^{-1} \circ b,$$

т.е.

$$S = \{a^{-1} \circ b\}.$$

2. Пусть $a = 0$. Тогда при $b \neq 0$ уравнение (4.29) решений не имеет, а при $b = 0$ множеством решений уравнение (4.29) является любой элемент множества $\mathbf{Z}_{p^k}$, т.е.

$$S = \mathbf{Z}_{p^k}.$$

3. Пусть

$$a = \alpha \circ p^{r_1} \ (r_1 \in \{1, \ldots, k-1\},\ \alpha \in \mathbf{Z}^{inv}_{p^{k-r_1}})$$

и

$$b = \beta \circ p^{r_3} \ (r_3 \in \{r_1, \ldots, k-1\},\ \ \beta \in \mathbf{Z}^{inv}_{p^{k-r_3}}).$$

Тогда:

1) если $r_1 = r_3$, то

$$x = \gamma$$

или

$$x = \gamma \oplus \delta \circ p^{k-i} \ (i = k - r_1, \ldots, k-1),$$

где $\gamma \in \mathbf{Z}^{inv}_{p^k}$, а $\delta \in \mathbf{Z}^{inv}_{p^i}$;

2) если $r_1 < r_3$, то

$$x = \gamma \circ p^{r_3 - r_1}$$

или

$$x = \gamma \circ p^{r_3 - r_1} \oplus \delta \circ p^{k-i} \ (i = k - r_1, \ldots, k-1),$$

где $\gamma \in \mathbf{Z}^{inv}_{p^{k-r_3+r_1}}$, а $\delta \in \mathbf{Z}^{inv}_{p^i}$.

Подставив эти значения a, b и x в уравнение (4.29), получим, что

$$\alpha \circ \gamma \circ p^{r_3} = \beta \circ p^{r_3} \Leftrightarrow (\alpha \circ \gamma \ominus \beta) \circ p^{r_3} = 0$$

Следовательно, либо

$$\alpha \circ \gamma \ominus \beta = 0 \Leftrightarrow \gamma = \alpha^{-1} \circ \beta,$$

либо

$$\alpha \circ \gamma \ominus \beta = \varepsilon \circ p^j \Leftrightarrow \gamma = \alpha^{-1} \circ (\beta \oplus \varepsilon \circ p^j),$$

где $j = k - r_3, \ldots, k-1$, а $\varepsilon \in \mathbf{Z}^{inv}_{p^{k-j}}$.

Таким образом:

1) если $a = \alpha \circ p^{r_1}$ и $b = \beta \circ p^{r_1}$, где $r_1 \in \{1, \ldots, k-1\}$ и $\alpha, \beta \in \mathbf{Z}^{inv}_{p^{k-r_1}}$, то

$$S = S_1 \cup S_2 \cup S_3 \cup S_4,$$

где

$$S_1 = \{\alpha^{-1} \circ \beta\},$$

$$S_2 = \bigcup_{j=k-r_1}^{k-1} \{\alpha^{-1} \circ (\beta \oplus \varepsilon \circ p^j) | \varepsilon \in \mathbf{Z}_{p^{k-j}}^{inv}\},$$

$$S_3 = \bigcup_{i=k-r_1}^{k-1} \{\alpha^{-1} \circ \beta \oplus \delta \circ p^{k-i} | \delta \in \mathbf{Z}_{p^i}^{inv}\},$$

$$S_4 = \bigcup_{i=k-r_1}^{k-1} \bigcup_{j=k-r_1}^{k-1} \{\alpha^{-1} \circ (\beta \oplus \varepsilon \circ p^j) \oplus \delta \circ p^{k-i} | \delta \in \mathbf{Z}_{p^i}^{inv}, \varepsilon \in \mathbf{Z}_{p^{k-j}}^{inv}\};$$

2) если $a = \alpha \circ p^{r_1}$ и $b = \beta \circ p^{r_3}$, где $r_1, r_3 \in \{1, \ldots, k-1\}$ и $r_1 < r_3$, то

$$S = S_1 \cup S_2 \cup S_3 \cup S_4,$$

где

$$S_1 = \{\alpha^{-1} \circ \beta \circ p^{r_3 - r_1}\},$$

$$S_2 = \bigcup_{j=k-r_1}^{k-1} \{(\alpha^{-1} \circ (\beta \oplus \varepsilon \circ p^j) \circ p^{r_3 - r_1}) | \varepsilon \in \mathbf{Z}_{p^{k-j}}^{inv}\},$$

$$S_3 = \bigcup_{i=k-r_1}^{k-1} \{\alpha^{-1} \circ \beta \circ p^{r_3 - r_1} \oplus \delta \circ p^{k-i} | \delta \in \mathbf{Z}_{p^i}^{inv}\},$$

$$S_4 = \bigcup_{i=k-r_1}^{k-1} \bigcup_{j=k-r_1}^{k-1} \{(\alpha^{-1} \circ (\beta \oplus \varepsilon \circ p^j) \circ p^{r_3 - r_1}) \oplus \delta \circ p^{k-i} | \delta \in \mathbf{Z}_{p^i}^{inv}, \varepsilon \in \mathbf{Z}_{p^{k-j}}^{inv}\}.$$

4. Пусть

$$a = \alpha \circ p^{r_1},$$

где $r_1 \in \{1, \ldots, k-1\}$ и $\alpha \in \mathbf{Z}_{p^{k-r_1}}^{inv}$, а

$$b = 0.$$

Тогда либо $x = 0$, либо $x = \gamma \circ p^i$, где $i \in \{k-r_1, \ldots, k-1\}$ и $\gamma \in \mathbf{Z}_{p^{k-i}}^{inv}$. Следовательно,

$$S = \{0\} \cup \bigcup_{i=k-r_1}^{k-1} \{\gamma \circ p^i | \gamma \in \mathbf{Z}_{p^{k-i}}^{inv}\}.$$

Рассмотрим теперь систему n линейных уравнений с n неизвестными над кольцом $\mathcal{Z}_{p^k}$

$$\begin{cases} a_{11} \circ x_1 \oplus \cdots \oplus a_{1n} \circ x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1} \circ x_1 \oplus \cdots \oplus a_{nn} \circ x_n = b_n \end{cases}, \tag{4.31}$$

где $a_{ij}, b_i \in \mathbf{Z}_{p^k}$ $(i, j = 1, \ldots, n)$ – параметры.

Запишем систему (4.31) в матричном виде

$$A \circ \mathbf{x} = \mathbf{b}. \tag{4.32}$$

Известно (см., напр., [6]), что посредством элементарных преобразований и, возможно, изменения нумерации переменных (т.е. с помощью метода Гаусса) система уравнений (4.32) может быть преобразована в такую эквивалентную систему уравнений

$$D \circ \mathbf{x} = \mathbf{c}, \tag{4.33}$$

что $\mathbf{c} = (c_1, \ldots, c_n)^T$, где $c_1, \ldots, c_n \in \mathbf{Z}_{p^k}$ и

$$D = \begin{pmatrix} d_1 & \ldots & 0 \\ \vdots & \ldots & \vdots \\ 0 & \ldots & d_n \end{pmatrix},$$

где $d_1, \ldots, d_l \in \mathbf{Z}_{p^k}^{inv}$ $(0 \le l \le n)$ и $d_{l+1}, \ldots, d_n \in \mathbf{Z}_{p^k} \backslash \mathbf{Z}_{p^k}^{inv}$.

Записав систему (4.33) в явном виде, получим

$$\begin{cases} d_1 \circ x_1 = c_1 \\ \cdots\cdots\cdots \\ d_n \circ x_n = c_n \end{cases} . \tag{4.34}$$

Далее множество решений S_i $(i = 1, \ldots, n)$ i-го уравнения системы уравнений (3.34) может быть найдено рассмотренным выше методом решения линейного уравнения над кольцом $\mathcal{Z}_{p^k}$.

Множество

$$S = S_1 \times \cdots \times S_n$$

представляет собой множество решений системы уравнений (4.34) (а, следовательно, множество решений системы уравнений (4.31)).

Рассмотрим недоопределенную систему m линейных уравнений с n $(n > m)$ неизвестными над кольцом $\mathcal{Z}_{p^k}$

$$\begin{cases} a_{11} \circ x_1 \oplus \cdots \oplus a_{1n} \circ x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1} \circ x_1 \oplus \cdots \oplus a_{mn} \circ x_n = b_m \end{cases} , \tag{4.35}$$

где $a_{ij}, b_i \in \mathbf{Z}_{p^k}$ $(i = 1, \ldots, n;\ j = 1, \ldots, n)$ – параметры.

С помощью метода Гаусса (т.е. посредством элементарных преобразований и, возможно, перенумерации переменных) система уравнений (4.35) может быть приведена к виду

$$\begin{cases} d_1 \circ x_1 = c_{1,m+1} \circ x_{m+1} \oplus \cdots \oplus c_{1,n} \circ x_n \\ \cdots\cdots\cdots\cdots\cdots \\ d_m \circ x_m = c_{m,m+1} \circ x_{m+1} \oplus \cdots \oplus c_{m,n} \circ x_n \end{cases} , \tag{4.36}$$

где $d_i, c_{ij} \in \mathbf{Z}_{p^k}$ $(i = 1, \ldots, m;\ j = m+1, \ldots, n)$.

Далее множество решений $S^{(i)}_{x_{m+1},\ldots,x_n}$ $(i = 1, \ldots, m)$ i-го уравнения системы уравнений (3.36) может быть найдено рассмотренным выше методом решения линейного уравнения над кольцом $\mathcal{Z}_{p^k}$.

Множество

$$S = \bigcup_{(x_{m+1},\ldots,x_n)\in \mathbf{Z}_{p^k}^{n-m}} S^{(1)}_{x_{m+1},\ldots,x_n} \times \cdots \times S^{(m)}_{x_{m+1},\ldots,x_n} \times (x_{m+1},\ldots,x_n)$$

представляет собой множество решений системы уравнений (4.36) (а, следовательно, множество решений системы уравнений (4.35)).

Рассмотрим переопределенную систему m линейных уравнений с n $(n < m)$ неизвестными над кольцом $\mathcal{Z}_{p^k}$

$$\begin{cases} a_{11} \circ x_1 \oplus \cdots \oplus a_{1n} \circ x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1} \circ x_1 \oplus \cdots \oplus a_{mn} \circ x_n = b_m \end{cases}, \tag{4.37}$$

где $a_{ij}, b_i \in \mathbf{Z}_{p^k}$ $(i = 1,\ldots,n;\ j = 1,\ldots,n)$ – параметры.

Без ограничения общности можно считать, что ни одно из уравнений системы (4.37) не является линейной комбинацией остальных уравнений.

С помощью элементарных преобразований и, возможно, перенумерации переменных, представим систему линейных уравнений (4.37) в виде двух систем линейных уравнений над кольцом $\mathcal{Z}_{p^k}$

$$\begin{cases} d_1 \circ x_1 = c_1 \\ \cdots\cdots.. \\ d_n \circ x_n = c_n \end{cases} \tag{4.38}$$

и

$$\begin{cases} d_{n+1,1} \circ x_1 \oplus \cdots \oplus d_{n+1,n} \circ x_n = c_{n+1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ d_{m,1} \circ x_1 \oplus \cdots \oplus d_{m,n} \circ x_n = c_m \end{cases}. \tag{4.39}$$

Метод поиска множества решений S' системы линейный уравнений (3.38) над кольцом $\mathcal{Z}_{p^k}$ рассмотрен выше.

Далее из множества S' необходимо выделить множество S решений системы линейный уравнений (4.39) над кольцом $\mathcal{Z}_{p^k}$.

Множество S и представляет собой множество решений системы линейных уравнений (4.37) над кольцом $\mathcal{Z}_{p^k}$.

4.3.2. Решение систем нелинейных уравнений.

Проиллюстрируем применение предложенной в п.4.2 схемы решения систем полиномиальных уравнений с параметрами на примере следующей системы нелинейных уравнений над кольцом $\mathcal{Z}_{p^k}$

$$\begin{cases} a_1 \circ u_1 \circ u_2 \oplus a_2 \circ u_3 = 0 \\ a_2 \circ u_1 = 0 \end{cases}, \tag{4.40}$$

где $a_1, a_2 \in \mathbf{Z}_{p^k}$ – параметры.

Замечание 4.7. В [57] показано, что необходимость решения этой системы уравнений естественно возникает в процессе анализа структуры классов эквивалентных состояний класса автоматных моделей над кольцом, в рамки которого уклыдываются автоматы построенные на основе таких модельных хаотических динамических систем, как отображение Эно [38].

Переходя к уравнению в алгебраической системе $\mathcal{B}$, получим

$$\begin{cases} C_{r_1} \circ C_{r_2} \circ C_{r_3} \oplus C_{r_4} \circ C_{r_5} = C_k \\ C_{r_4} \circ C_{r_2} = C_k \end{cases}, \tag{4.41}$$

Из (4.22)-(4.28) вытекает, что:

1) если $r_1 = k$, то

$$\begin{cases} r_5 \geq k - r_4 \\ r_2 \geq k - r_4 \end{cases},$$

а r_3 может быть произвольным элементом множества $\{0, 1, \ldots, k\}$;

2) если $r_1 \neq k$ и $r_4 = 0$, то $r_2 = k$, $r_5 = k$, а r_3 может быть произвольным элементом множества $\{0, 1, \ldots, k\}$;

3) если $r_1 \neq k$ и $r_4 = k$, то $r_2 + r_3 \geq k - r_1$, а r_5 может быть произвольным элементом множества $\{0, 1, \ldots, k\}$;

4) если $r_1 \neq k$ и $r_4 \in \{1, \ldots, k-1\}$, то $r_2 \geq k - r_4$, а это означает, что:

а) если $r_2 = k$, то $r_5 \geq k - r_4$, а r_3 может быть произвольным элементом множества $\{0, 1, \ldots, k\}$;

б) если $k - r_4 \leq r_2 \leq k - 1$, то возможны два принципиально различные случая, а именно: когда $r_2 + r_3 \geq k - r_1$ и $r_5 \geq k - r_4$, а также когда $r_2 + r_3 < k - r_1$ и $r_2 + r_3 - r_5 = r_4 - r_1$.

В остальных случаях система уравнений (4.41) (а, следовательно, и система уравнений (4.40)) не имеет решений.

Из сказанного выше вытекает, что для поиска множества S решений системы уравнений (4.40) необходимо рассмотреть следующие ситуации.

1. Пусть $a_1 = 0$. Тогда система уравнений (4.40) принимает вид

$$\begin{cases} 0 \circ u_1 \circ u_2 \oplus a_2 \circ u_3 = 0 \\ a_2 \circ u_1 = 0 \end{cases}.$$

Следовательно:

1) если $a_2 \in \mathbf{Z}_{p^k}^{inv}$, то

$$S = \{(0, u_2, 0) | u_2 \in \mathbf{Z}_{p^k}\};$$

2) если $a_2 = \alpha_4 \circ p^{r_4}$ $(\alpha_4 \in \mathbf{Z}_{p^{k-r_4}}^{inv},\ r_4 \in \{1, \ldots, k-1\})$, то

$$S = S_1 \cup S_2 \cup C_3 \cup S_4,$$

где

$$S_1 = \{(0, u_2, 0) | u_2 \in \mathbf{Z}_{p^k}\},$$

$$S_2 = \bigcup_{r_5 = k - r_4}^{k-1} \{(0, u_2, \alpha_5 \circ p^{r_5}) | u_2 \in \mathbf{Z}_{p^k},\ \alpha_5 \in \mathbf{Z}_{p^{k-r_5}}^{inv}\},$$

$$S_3 = \bigcup_{r_2 = k - r_4}^{k-1} \{(\alpha_2 \circ p^{r_2}, u_2, 0) | u_2 \in \mathbf{Z}_{p^k},\ \alpha_2 \in \mathbf{Z}_{p^{k-r_2}}^{inv}\},$$

$$S_4 = \bigcup_{r_5 = k - r_4}^{k-1} \bigcup_{r_2 = k - r_4}^{k-1} S_{r_2, r_5}^{(1)},$$

а

$$S_{r_2, r_5}^{(1)} = \{(\alpha_2 \circ p^{r_2}, u_2, \alpha_5 \circ p^{r_5}) | u_2 \in \mathbf{Z}_{p^k},\ \alpha_i \in \mathbf{Z}_{p^{k-r_i}}^{inv}\ (i = 2, 5)\};$$

3) если $a_2 = 0$, то

$$S = \mathbf{Z}_{p^k}^3.$$

2. Пусть $a_1 \neq 0$ и $a_2 \in \mathbf{Z}_{p^k}^{inv}$. Тогда система уравнений (4.40) принимает вид

$$\begin{cases} a_2^{-1} \circ a_1 \circ u_1 \circ u_2 \oplus u_3 = 0 \\ u_1 = 0 \end{cases}.$$

Следовательно:

$$S = \{(0, u_2, 0) | u_2 \in \mathbf{Z}_{p^k}\}.$$

3. Пусть $a_1 \neq 0$ и $a_2 = 0$. Тогда система уравнений (4.40) принимает вид

$$\begin{cases} a_1 \circ u_1 \circ u_2 \oplus 0 \circ u_3 = 0 \\ 0 \circ u_1 = 0 \end{cases}.$$

Следовательно:

1) если $a_1 \in \mathbf{Z}_{p^k}^{inv}$, то

$$S = S_1 \cup S_2 \cup S_3,$$

где

$$S_1 = \{(u_1, 0, u_3) | u_1, u_3 \in \mathbf{Z}_{p^k}\},$$

$$S_2 = \{(0, u_2, u_3) | u_2 \in \mathbf{Z}_{p^k} \backslash \{0\}, u_3 \in \mathbf{Z}_{p^k}\},$$

$$S_3 = \bigcup_{r_3=1}^{k-1} \bigcup_{r_2=k-r_3}^{k-1} S_{r_2,r_3}^{(2)},$$

а

$$S_{r_2,r_3}^{(2)} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, u_3) | \alpha_i \in \mathbf{Z}_{p^{k-r_i}}^{inv} \ (i = 2, 3), u_3 \in \mathbf{Z}_{p^k}\};$$

2) если $a_1 = \alpha_1 \circ p^{r_1}$ ($\alpha_1 \in \mathbf{Z}_{p^{k-r_1}}^{inv}$; $r_1 \in \{1, \ldots, k-1\}$), то

$$S = \bigcup_{i=1}^{5} S_i,$$

где

$$S_1 = \{(u_1, 0, u_3) | u_1, u_3 \in \mathbf{Z}_{p^k}\},$$

$$S_2 = \{(0, u_2, u_3) | u_2 \in \mathbf{Z}_{p^k} \backslash \{0\}, u_3 \in \mathbf{Z}_{p^k}\},$$

$$S_3 = \bigcup_{r_2=k-r_1}^{k-1} \{(\alpha_2 \circ p^{r_2}, u_2, u_3) | \alpha_2 \in \mathbf{Z}_{p^{k-r_2}}^{inv}, u_2 \in \mathbf{Z}_{p^k}^{inv}, u_3 \in \mathbf{Z}_{p^k}\},$$

$$S_4 = \bigcup_{r_3=k-r_1}^{k-1} \{(u_1, \alpha_3 \circ p^{r_3}, u_3) | u_1 \in \mathbf{Z}_{p^k}^{inv}, \alpha_3 \in \mathbf{Z}_{p^{k-r_3}}^{inv}, u_3 \in \mathbf{Z}_{p^k}\},$$

$$S_5 = \bigcup_{r_2=1}^{k-1} \bigcup_{r_3=\max\{k-r_1-r_2,1\}}^{k-1} S_{r_2,r_3}^{(3)},$$

где

$$S_{r_2,r_3}^{(3)} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, u_3) | \alpha_i \in \mathbf{Z}_{p^{k-r_i}}^{inv} \ (i = 2, 3), u_3 \in \mathbf{Z}_{p^k}\}.$$

4. Пусть $a_1 \neq 0$ и $a_2 = \alpha_4 \circ p^{r_4}$ ($\alpha_4 \in \mathbf{Z}_{p^{k-r_4}}^{inv}$, $r_4 \in \{1, \ldots, k-1\}$).

1) если $a_1 \in \mathbf{Z}_{p^k}^{inv}$, то

$$S = \bigcup_{i=1}^{7} S_i,$$

где

$$S_1 = \{(0, u_2, 0) | u_2 \in \mathbf{Z}_{p^k}\},$$

$$S_2 = \bigcup_{r_5=k-r_4}^{k-1} \{(0, u_2, \alpha_5 \circ p^{r_5}) | u_2 \in \mathbf{Z}_{p^k}, \alpha_5 \in \mathbf{Z}_{p^{k-r_5}}^{inv}\},$$

$$S_3 = \bigcup_{r_2=k-r_4}^{k-1} \{(\alpha_2 \circ p^{r_2}, 0, 0) | \alpha_2 \in \mathbf{Z}_{p^{k-r_2}}^{inv}\},$$

$$S_4 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_5=k-r_4}^{k-1} S_{r_2,r_5}^{(4)},$$

а

$$S^{(4)}_{r_2,r_5} = \{(\alpha_2 \circ p^{r_2}, 0, \alpha_5 \circ p^{r_5}) | \alpha_i \in \mathbf{Z}^{inv}_{p^{k-r_i}} \ (i = 2, 5)\},$$

$$S_5 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_3=k-r_2}^{k-1} S^{(5)}_{r_2,r_3},$$

где

$$S^{(5)}_{r_2,r_3} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, 0) | \alpha_i \in \mathbf{Z}^{inv}_{p^{k-r_i}} \ (i = 2, 3)\},$$

$$S_6 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_3=k-r_2}^{k-1} \bigcup_{r_5=k-r_4}^{k-1} S^{(6)}_{r_2,r_3,r_5},$$

а

$$S^{(6)}_{r_2,r_3,r_5} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_5}) | \alpha_i \in \mathbf{Z}^{inv}_{p^{k-r_i}} \ (i = 2, 3, 5)\},$$

$$S_7 = \bigcup_{r_2=k-r_4}^{k-2} \bigcup_{r_3=1}^{k-1-r_2} \left(\widetilde{S}^{(7)}_{r_2,r_3} \cup \bigcup_{r_6=\max\{1,k-r_2-r_3\}}^{k-1} \widehat{S}^{(7)}_{r_2,r_3,r_6} \right),$$

где

$$\widetilde{S}^{(7)}_{r_2,r_3} = \emptyset,$$

если

$$r_2 + r_3 < r_4 + 1,$$

и

$$\widetilde{S}^{(7)}_{r_2,r_3} = \{\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_2+r_3-r_4} | \alpha_i \in \mathbf{Z}^{inv}_{p^{k-r_i}} \ (i = 2, 3),$$
$$\alpha_5 = (\ominus a_1 \circ {\alpha_4}^{-1} \circ \alpha_2 \circ \alpha_3) \ (mod\, p^{r_2+r_3-r_4})\},$$

если

$$r_2 + r_3 \geq r_4 + 1,$$

а

$$\widehat{S}^{(7)}_{r_2,r_3,r_6} = \emptyset,$$

если

$$r_2 + r_3 < r_4 + 1,$$

и

$$\widehat{S}^{(7)}_{r_2,r_3,r_6} = \{\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_2+r_3-r_4} | \alpha_i \in \mathbf{Z}^{inv}_{p^{k-r_i}} \ (i = 2, 3),$$
$$\alpha_5 = (a_1 \circ {\alpha_4}^{-1} \circ (\alpha_6 \circ p^{r_6} \ominus \alpha_2 \circ \alpha_3)) \ (mod\, p^{r_2+r_3-r_4}), \ \alpha_6 \in \mathbf{Z}^{inv}_{p^{k-r_6}}\};$$

если

$$r_2 + r_3 \geq r_4 + 1;$$

2) если $a_1 = \alpha_1 \circ p^{r_1}$ $(\alpha_1 \in \mathbf{Z}^{inv}_{p^{k-r_1}}, \ r_1 \in \{1, \ldots, k-1\})$, то

$$S = \bigcup_{i=1}^{11} S_i,$$

где

$$S_1 = \{(0, u_2, 0) | u_2 \in \mathbf{Z}_{p^k}\},$$

$$S_2 = \bigcup_{r_5=k-r_4}^{k-1} \{(0, u_2, \alpha_5 \circ p^{r_5}) | u_2 \in \mathbf{Z}_{p^k}, \alpha_5 \in \mathbf{Z}^{inv}_{p^{k-r_5}}\},$$

$$S_3 = \bigcup_{r_2=k-r_4}^{k-1} \{(\alpha_2 \circ p^{r_2}, 0, 0) | \alpha_2 \in \mathbf{Z}^{inv}_{p^{k-r_2}}\},$$

$$S_4 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_5=k-r_4}^{k-1} S^{(4)}_{r_2,r_5},$$

а

$$S^{(4)}_{r_2,r_5} = \{(\alpha_2 \circ p^{r_2}, 0, \alpha_5 \circ p^{r_5}) | \alpha_i \in \mathbf{Z}^{inv}_{p^{k-r_i}} \ (i = 2, 5)\},$$

$$S_5 = \bigcup_{r_2=\max\{k-r_1,k-r_4\}}^{k-1} \{\alpha_2 \circ p^{r_2}, u_2, 0) | \alpha_2 \in \mathbf{Z}^{inv}_{p^{k-r_2}}, \ u_2 \in \mathbf{Z}^{inv}_{p^k}\},$$

$$S_6 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_3=\max\{1,k-r_1-r_2\}}^{k-1} S^{(6)}_{r_2,r_3},$$

где

$$S^{(6)}_{r_2,r_3} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, 0) | \alpha_i \in \mathbf{Z}^{inv}_{p^{k-r_i}} \ (i = 2, 3)\},$$

$$S_7 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_3=\max\{1,k-r_1-r_2\}}^{k-1} \bigcup_{r_5=k-r_4}^{k-1} S^{(7)}_{r_2,r_3,r_5},$$

а

$$S^{(7)}_{r_2,r_3,r_5} = \{(\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_5}) | \alpha_i \in \mathbf{Z}^{inv}_{p^{k-r_i}} \ (i = 2, 3, 5)\},$$

$$S_8 = \bigcup_{r_2=k-r_4}^{k-1} \bigcup_{r_3=1}^{k-1-r_1-r_2} \left(\widetilde{S}^{(8)}_{r_2,r_3} \cup \bigcup_{r_6=\max\{1,k-r_1-r_2-r_3\}}^{k-1} \widehat{S}^{(8)}_{r_2,r_3,r_6} \right),$$

где

$$\widetilde{S}^{(8)}_{r_2,r_3} = \emptyset,$$

если

$$r_2 + r_3 < r_4 - r_1 + 1,$$

и

$$\widetilde{S}^{(8)}_{r_2,r_3} = \{\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_1+r_2+r_3-r_4} | \alpha_i \in \mathbf{Z}^{inv}_{p^{k-r_i}} \ (i = 2, 3),$$
$$\alpha_5 = (\ominus \alpha_1 \circ {\alpha_4}^{-1} \circ \alpha_2 \circ \alpha_3) \ (mod\, p^{r_1+r_2+r_3-r_4})\},$$

если

$$r_2 + r_3 \geq r_4 - r_1 + 1,$$

а

$$\widehat{S}^{(8)}_{r_2,r_3,r_6} = \emptyset,$$

если

$$r_2 + r_3 < r_4 - r_1 + 1,$$

и

$$\widehat{S}^{(8)}_{r_2,r_3,r_6} = \{\alpha_2 \circ p^{r_2}, \alpha_3 \circ p^{r_3}, \alpha_5 \circ p^{r_1+r_2+r_3-r_4} | \alpha_i \in \mathbf{Z}^{inv}_{p^{k-r_i}} \ (i = 2, 3),$$
$$\alpha_5 = (\alpha_1 \circ {\alpha_4}^{-1} \circ (\alpha_6 \circ p^{r_6} \ominus \alpha_2 \circ \alpha_3)) \ (mod\, p^{r_1+r_2+r_3-r_4}), \ \alpha_6 \in \mathbf{Z}^{inv}_{p^{k-r_6}}\},$$

если

$$r_2 + r_3 \geq r_4 - r_1 + 1.$$

Итак, показано, что предложенная схема решения систем полиномиальных уравнений с параметрами над кольцом вычетов $\mathcal{Z}_{p^k}$, основанная на понятии p-тип элемента, дает возможность эффективно находить множество решений этих систем.

Замечание 4.8. Полученные выше результаты показывают целесообразность обобщения предложенной схемы решения систем полиномиальных уравнений с параметрами на произвольное кольцо вычетов $\mathcal{Z}_n$, где $n = p_1^{\alpha_1} \dots p_l^{\alpha_l}$ $(l \geq 2)$.

Основная сложность здесь состоит в том, что при $n = p_1^{\alpha_1} \dots p_l^{\alpha_l}$ $(l \geq 2)$ типы элементов образуют частично упорядоченное (а не линейно упорядоченное) множество.

5. АВТОМАТЫ НАД КОНЕЧНЫМИ КОЛЬЦАМИ

Фрагментарное применение теории колец при построении современных шифров обосновывает актуальность исследования автоматных моделей, представленных системами уравнений над конечными кольцами. Анализ таких моделей представляет новое направление в теории автоматов. Более того, именно такие модели дают возможность установить глубокие внутренние связи между теорией систем, современной алгеброй, алгебраической геометрией, теорией автоматов и современной криптологией.

Цель настоящего раздела – систематическое исследование автоматов над конечным ассоциативно-коммутативным кольцом с единицей (в дальнейшем, для краткости, будем говорить просто «кольцо») $\mathcal{K} = (K, +, \cdot)$.

В п.5.1 представлены исследуемые модели. В п.5.2 рассмотрена схема анализа конечно-автоматных характеристик исследуемых моделей. В п.5.3 охарактеризованы классы эквивалентных состояний исследуемых автоматов. В п.5.4 для исследуемых автоматов решены задачи параметрической идентификации и идентификации начального состояния. В п.5.5 охарактеризованы неподвижные точки отображений, реализуемых исследуемыми автоматами. В п.5.6 исследуется вариация поведения автомата при вариации его параметров, либо его начального состояния. В п.5.7 рассмотрены линейные автоматы. В п.5.8 решена задача построения асимптотически точной имитационной модели для нелинейного одномерного автомата с лагом 2.

Материл, представленный в настоящем разделе, основан на результатах, полученных авторами в [34,35,52,55,61-63,67-69,74,76,77,116,117].

5.1. Исследуемые модели.

Определим основные классы автоматов Мили и Мура, исследованию которых посвящен настояший раздел.

5.1.1. Нелинейные автоматы общего вида.

Рассмотрим над кольцом $\mathcal{K} = (K, +, \cdot)$ множество $\mathcal{A}_{n,1}$ автоматов Мили

$$M_1 : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t) + \mathbf{f}_4(\mathbf{x}_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+) \tag{5.1}$$

и множество $\mathcal{A}_{n,2}$ автоматов Мура

$$M_2 : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.2}$$

где $\mathbf{f}_i : K^n \to K^n$ $(i = 1, \ldots, 4)$, причем $\mathbf{f}_2$ – нелинейное отображение, а $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in K^n$ – соответственно, состояние автомата, входной и выходной символ в момент $t \in \mathbf{Z}_+$.

Для криптографии представляют особый интерес подмножества $\mathcal{A}_{n,i}^{inv}$ $(i = 1, 2)$ таких автоматов $M_i \in \mathcal{A}_{n,i}$, что при каждом начальном состоянии $\mathbf{q}_0 \in K^n$ является биекцией автоматное отображение

$$\mathbf{F}_{(M,\mathbf{q}_0)} : (K^n)^+ \to (K^n)^+,$$

реализуемое инициальным автоматом $(M, \mathbf{q}_0)$. Такие автоматы определяют класс поточных шифров, для которых начальное состояние $\mathbf{q}_0 \in K^n$ – секретный сеансовый ключ.

Теорема 5.1. Для любых отображений $\mathbf{f}_i$ $(i = 1, 2, 3)$ истинно равенство

$$\mathcal{A}_{n,1}^{inv} = \{M_1 \in \mathcal{A}_{n,1} | \mathbf{f}_4 : K^n \to K^n \ - \text{ биекция } \}. \tag{5.3}$$

Доказательство. Предположим, что $M_1 \in \mathcal{A}_{n,1}$ – такой автомат, что $\mathbf{f}_4 : K^n \to K^n$ – биекция.

Из 2-го уравнения системы (5.1) находим

$$\mathbf{x}_{t+1} = \mathbf{f}_4^{-1}(\mathbf{y}_{t+1} - \mathbf{f}_2(\mathbf{q}_t)). \tag{5.4}$$

Подставив (5.4) в 1-е уравнение системы (5.1), получим

$$\mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{f}_4^{-1}(\mathbf{y}_{t+1} - \mathbf{f}_2(\mathbf{q}_t))). \tag{5.5}$$

Заменив в (5.4) и (5.5) $\mathbf{x}$ на $\mathbf{y}$ и $\mathbf{y}$ на $\mathbf{x}$, получим такой автомат

$$M_1^{-1} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{f}_4^{-1}(\mathbf{x}_{t+1} - \mathbf{f}_2(\mathbf{q}_t))) \\ \mathbf{y}_{t+1} = \mathbf{f}_4^{-1}(\mathbf{x}_{t+1} - \mathbf{f}_2(\mathbf{q}_t)) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.6}$$

что при каждом начальном состоянии $\mathbf{q}_0 \in K^n$ инициальный автомат $(M_1, \mathbf{q}_0)$ реализует отображение $\mathbf{F}_{(M_1,\mathbf{q}_0)}^{-1}$, т.е. при каждом начальном состоянии $\mathbf{q}_0 \in K^n$ отображение $\mathbf{F}_{(M_1,\mathbf{q}_0)}$ – биекция.

Следовательно, $M_1 \in \mathcal{A}_{n,1}^{inv}$.

Теперь предположим, что $M_1 \in \mathcal{A}_{n,1}$ – такой автомат, что отображение $\mathbf{f}_4 : K^n \to K^n$ не является биекцией.

Тогда существуют такие входные символы $\mathbf{x}_1, \widetilde{\mathbf{x}}_1 \in \ker \mathbf{f}_4$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$, что

$$\mathbf{f}_4(\mathbf{x}_1) = \mathbf{f}_4(\widetilde{\mathbf{x}}_1).$$

Отсюда вытекает, что

$$\mathbf{y}_1 = \mathbf{f}_2(\mathbf{q}_0) + \mathbf{f}_4(\mathbf{x}_1) = \mathbf{f}_2(\mathbf{q}_0) + \mathbf{f}_4(\widetilde{\mathbf{x}}_1) = \widetilde{\mathbf{y}_1}$$

для всех $\mathbf{q}_0 \in K^n$, т.е. при каждом начальном состоянии $\mathbf{q}_0 \in K^n$ отображение $\mathbf{F}_{(M_1,\mathbf{q}_0)}$ не является биекцией.

Следовательно, $M_1 \notin \mathcal{A}_{n,1}^{inv}$.

□

Теорема 5.2. Для любого отображения $\mathbf{f}_1$ истинно равенство

$$\mathcal{A}_{n,2}^{inv} = \{M_2 \in \mathcal{A}_{n,2} | \mathbf{f}_2 : K^n \to K^n \text{ и } \mathbf{f}_3 : K^n \to K^n \ - \text{ биекции } \}. \quad (5.7)$$

Доказательство. Пусть $M_2 \in \mathcal{A}_{n,2}$ – такой автомат, что отображения $\mathbf{f}_i$ $(i = 2, 3)$ – биекции.

Из (5.2) находим

$$\mathbf{x}_1 = \mathbf{f}_3^{-1}(\mathbf{q}_{t+1} - \mathbf{f}_1(\mathbf{q}_t)), \quad (5.8)$$

$$\mathbf{q}_{t+1} = \mathbf{f}_2^{-1}(\mathbf{y}_{t+1}). \quad (5.9)$$

Подставив (5.9) в (5.8), получим

$$\mathbf{x}_{t+1} = \mathbf{f}_3^{-1}(\mathbf{f}_2^{-1}(\mathbf{y}_{t+1}) - \mathbf{f}_1(\mathbf{q}_t)). \quad (5.10)$$

Заменив в (5.9) и (5.10) $\mathbf{x}$ на $\mathbf{y}$ и $\mathbf{y}$ на $\mathbf{x}$, получим такой автомат

$$M_2^{-1} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_2^{-1}(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_3^{-1}(\mathbf{f}_2^{-1}(\mathbf{x}_{t+1}) - \mathbf{f}_1(\mathbf{q}_t)) \end{cases} \quad (t \in \mathbf{Z}_+), \quad (5.11)$$

что при каждом начальном состоянии $\mathbf{q}_0 \in K^n$ инициальный автомат $(M_2, \mathbf{q}_0)$ реализует отображение $\mathbf{F}^{-1}_{(M_2,\mathbf{q}_0)}$, т.е. при каждом начальном состоянии $\mathbf{q}_0 \in K^n$ отображение $\mathbf{F}_{(M_2,\mathbf{q}_0)}$ – биекция.

Следовательно, $M_2 \in \mathcal{A}_{n,2}^{inv}$.

Пусть $M_2 \in \mathcal{A}_{n,2}$ – такой автомат, что хотя бы одно из отображений $\mathbf{f}_i : K^n \to K^n$ $(i = 2, 3)$ не является биекцией.

Если отображение $\mathbf{f}_3 : K^n \to K^n$ не является биекцией, то существуют такие $\mathbf{x}_1, \widetilde{\mathbf{x}}_1 \in \ker \mathbf{f}_3$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$, что

$$\mathbf{f}_3(\mathbf{x}_1) = \mathbf{f}_3(\widetilde{\mathbf{x}}_1).$$

Отсюда вытекает, что

$$\mathbf{y}_1 = \mathbf{f}_2(\mathbf{f}_1(\mathbf{q}_0) + \mathbf{f}_3(\mathbf{x}_1)) = \mathbf{f}_2(\mathbf{f}_1(\mathbf{q}_0) + \mathbf{f}_3(\widetilde{\mathbf{x}}_1)) = \widetilde{\mathbf{y}_1}$$

для всех $\mathbf{q}_0 \in K^n$, т.е. при каждом начальном состоянии $\mathbf{q}_0 \in K^n$ отображение $\mathbf{F}_{(M_1,\mathbf{q}_0)}$ не является биекцией.

Следовательно, $M_2 \notin \mathcal{A}_{n,2}^{inv}$.

Пусть $\mathbf{f}_3 : K^n \to K^n$ – биекция, а отображение $\mathbf{f}_2 : K^n \to K^n$ не является биекцией.

Так как отображение $\mathbf{f}_2 : K^n \to K^n$ не является биекцией, то существуют такие состояния $\mathbf{q}_1, \widetilde{\mathbf{q}}_1 \in \ker \mathbf{f}_2$, что $\mathbf{q}_1 \neq \widetilde{\mathbf{q}}_1$.

А так как отображение $\mathbf{f}_3 : K^n \to K^n$ – биекция, то для любого начального состояния $\mathbf{q}_0 \in K^n$ существуют такие входные символы $\mathbf{x}_1, \widetilde{\mathbf{x}}_1 \in K^n$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$, что

$$\mathbf{q}_1 = \mathbf{f}_1(\mathbf{q}_0) + \mathbf{f}_3(\mathbf{x}_1),$$

$$\widetilde{\mathbf{q}}_1 = \mathbf{f}_1(\mathbf{q}_0) + \mathbf{f}_3(\widetilde{\mathbf{x}}_1).$$

Следовательно, для каждого начального состояния $\mathbf{q}_0 \in K^n$ автомата $M_2 \in \mathcal{A}_{n,2}$ существуют такие входные символы $\mathbf{x}_1, \widetilde{\mathbf{x}}_1 \in K^n$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$, что

$$\mathbf{y}_1 = \mathbf{f}_2(\mathbf{q}_1) = \mathbf{f}_2(\widetilde{\mathbf{q}}_1) = \widetilde{\mathbf{y}}_1,$$

т.е. при каждом начальном состоянии $\mathbf{q}_0 \in K^n$ отображение $\mathbf{F}_{(M_2,\mathbf{q}_0)}$ не является биекцией.

Отсюда вытекает, что $M_2 \notin \mathcal{A}_{n,2}^{inv}$.

□

Из (5.6) и (5.11) вытекает, что для автомата $M \in \mathcal{A}_{n,1}^{inv} \cup \mathcal{A}_{n,2}^{inv}$ обратный автомат M^{-1} – автомат Мили.

Любая упорядоченная пара инициальных автоматов

$$((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0)) \ (M \in \mathcal{A}_{n,1}^{inv} \cup \mathcal{A}_{n,2}^{inv})$$

представляет собой симметричный поточный шифр гаммирования, построенный на основе нелинейного автоключа, для которого начальное состояние $\mathbf{q}_0 \in K^n$ – секретный сеансовый ключ.

Из теорем 5.1 и 4.5 вытекают следующие три следствия.

Следствие 5.1. Для любого поточного шифра

$$((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0)) \ (M \in \mathcal{A}_{n,1}^{inv} \cup \mathcal{A}_{n,2}^{inv})$$

в процессе «шифрование-расшифрование» автоматы M и M^{-1} движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

Следствие 5.2. Для любого автомата $M_1 \in \mathcal{A}_{n,1}^{inv}$ функции переходов и выходов автомата M_1^{-1} разделимы по переменным $\mathbf{q}$ и $\mathbf{x}$ тогда и только тогда, когда по этим переменным разделимы отображения

$$\mathbf{g}_1(\mathbf{q}, \mathbf{x}) = \mathbf{f}_3(\mathbf{f}_4^{-1}(\mathbf{x} - \mathbf{f}_2(\mathbf{q})))$$

и

$$\mathbf{g}_2(\mathbf{q}, \mathbf{x}) = \mathbf{f}_4^{-1}(\mathbf{x}_{t+1} - \mathbf{f}_2(\mathbf{q}_t)).$$

Следствие 5.3. Для любого автомата $M_2 \in \mathcal{A}_{n,2}^{inv}$ функция выходов автомата M_2^{-1} разделима по переменным $\mathbf{q}$ и $\mathbf{x}$ тогда и только тогда, когда по этим переменным разделимо отображение

$$\mathbf{g}_3(\mathbf{q}, \mathbf{x}) = \mathbf{f}_3^{-1}(\mathbf{f}_2^{-1}(\mathbf{x}) - \mathbf{f}_1(\mathbf{q})).$$

То обстоятельство, что в процессе «шифрование-расшифрование» автоматы M и M^{-1} движутся в пространстве состояний по одной и той же траектории в одном и том же направлении, дает возможность (за счет соответствующего дублирования информации) эффективно осуществлять контроль ошибок, возникающих при вычислениях, осуществляемых автоматами $(M, \mathbf{q}_0)$ и $(M^{-1}, \mathbf{q}_0)$ (но не контроль ошибок, возникающих в процессе передачи информации по каналу связи).

5.1.2. Автоматы с нелинейной функцией переходов.

В качестве модельных множеств автоматов, на которых будут детализироваться полученные результаты, будем использовать множества $\widetilde{\mathcal{A}}_{n,1}$ и $\widetilde{\mathcal{A}}_{n,2}$ автоматов, соответственно, вида

$$M_1 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + C\mathbf{q}_t + \mathbf{d} + E\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = G\mathbf{q}_t + F\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.12}$$

$$M_2 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + C\mathbf{q}_t + \mathbf{d} + E\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = G\mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.13}$$

где $\mathbf{q}_t = (q_t^{(1)}, \ldots, q_t^{(n)})^T$, $\mathbf{x}_t = (x_t^{(1)}, \ldots, x_t^{(n)})^T$ и $\mathbf{y}_t = (y_t^{(1)}, \ldots, y_t^{(n)})^T$ – соответственно, состояние автомата, входной и выходной символ в момент $t \in \mathbf{Z}_+$, $\mathbf{b}_t = (b^{(1)}, \ldots, b^{(n)})^T \in K^n$ и $\mathbf{d}_t = (d^{(1)}, \ldots, d^{(n)})^T \in K^n$ – фиксированные векторы, а A, C, E, G, F – фиксированные $n \times n$-матрицы над кольцом $\mathcal{K}$.

Обозначим через M_n множество всех $n \times n$-матриц над кольцом $\mathcal{K}$, через M_n^{inv} – множество всех обратимых матриц $X \in \mathsf{M}_n$ и положим $\mathsf{M}_n^{non-inv} = \mathsf{M}_n \backslash \mathsf{M}_n^{inv}$.

Из (5.5) и (5.6) вытекает, что:

1) $\widetilde{\mathcal{A}}_{n,1}^{inv}$ – множество всех таких автоматов $M_1 \in \widetilde{\mathcal{A}}_{n,1}$, что $F \in \mathsf{M}_n^{inv}$;

2) $\widetilde{\mathcal{A}}_{n.2}^{inv}$ – множество всех таких автоматов $M_2 \in \widetilde{\mathcal{A}}_{n,2}$, что $E, G \in \mathsf{M}_n^{inv}$.

Отметим, что в случае кольца $\mathcal{Z}_m = (\mathbf{Z}_m, \oplus, \circ)$

$$|\mathsf{M}_n| = n^{m^2}.$$

Кроме того (см., напр., [53]), если

$$m = \prod_{i=1}^{h} p_i^{k_i},$$

где p_i – попарно различные простые числа, то

$$|\mathsf{M}_n^{inv}| = |\mathsf{M}_n| \prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}),$$

а, следовательно,

$$|\mathsf{M}_n^{non-inv}| = |\mathsf{M}_n| \left(1 - \prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}) \right).$$

При построении шифров на основе аналогов над кольцом $\mathcal{K}$ хаотических динамических систем вместо автомата $M \in \widetilde{\mathcal{A}}_{n,1}^{inv} \cup \widetilde{\mathcal{A}}_{n,2}^{inv}$ часто более

удобно использовать автоматы Мили M_3 и Мура M_4, определяемые следующими четырьмя условиями.

Условие 5.1. Автоматы M_3 и M_4 определяются, соответственно, соотношениями (5.12) и (5.13).

Условие 5.2. Зафиксировано r $(1 \le r \le n)$ таких упорядоченных пар чисел (i_h, j_h) $(h = 1, \dots, r)$, что:

1) $i_h, j_h \in \mathbf{N}_n$ для всех $h = 1, \dots, r$;

2) если $h_1 \ne h_2$ $(h_1, h_2 = 1, \dots, r)$, то $i_{h_1} \ne i_{h_2}$ и $j_{h_1} \ne j_{h_2}$.

Условие 5.3. В клетках (i_h, j_h) $(h = 1, \dots, r)$ матриц E, F, G расположены обратимые элементы кольца $\mathcal{K}$, а во всех остальных клетках – нули.

Условие 5.4. Входной алфавит каждого из автоматов M_3 и M_4 – это множество всех всех таких $\mathbf{x} = (x^{(1)}, \dots, x^{(n)}) \in K^n$, что $x^{(j)} = 0$ для всех $j \in \mathbf{N}_n \backslash \{j_1, \dots, j_r\}$.

За счет изменения нумерации компонент векторов $\mathbf{q}, \mathbf{x}, \mathbf{y}, \mathbf{b}, \mathbf{d}$ представления (5.12) и (5.13) автоматов M_3 и M_4 могут быть приведены, соответственно, к виду

$$M_3 : \begin{cases} q_{t+1}^{(i)} = \mathbf{q}_t^T A_i \mathbf{q}_t + \mathbf{c}_i \mathbf{q}_t + d_i + \alpha_i e_i x_{t+1}^{(i)} \ (i \in \mathbf{N}_n) \\ y_{t+1}^{(i)} = g_i q_t^{(i)} + f_i x_{t+1}^{(i)} \ (i \in \mathbf{N}_r) \end{cases} \quad (t \in \mathbf{Z}_+), \quad (5.14)$$

где $\alpha_i = 1$, если $i \in \mathbf{N}_r$, и $\alpha_i = 0$, если $i \in \mathbf{N}_n \backslash \mathbf{N}_r$, $A_i \in \mathsf{M}_n$ $(i \in \mathbf{N}_n)$, $\mathbf{c}_i = (c_i^{(1)}, \dots, c_i^{(n)}) \in K^n$ $(i \in \mathbf{N}_n)$, $d_i \in K$ $(i \in \mathbf{N}_n)$, $e_i \in K$ $(i \in \mathbf{N}_r)$, $f_i \in K^{inv}$ $(i \in \mathbf{N}_r)$, где K^{inv} – множество всех обратимых элементов кольца $\mathcal{K}$ и

$$M_4 : \begin{cases} q_{t+1}^{(i)} = \mathbf{q}_t^T A_i \mathbf{q}_t + \mathbf{c}_i \mathbf{q}_t + d_i + \alpha_i e_i x_{t+1}^{(i)} \ (i \in \mathbf{N}_r) \\ y_{t+1}^{(i)} = g_i q_{t+1}^{(i)} \ (i \in \mathbf{N}_r) \end{cases} \quad (t \in \mathbf{Z}_+), \quad (5.15)$$

где $\alpha_i = 1$, если $i \in \mathbf{N}_r$, и $\alpha_i = 0$, если $i \in \mathbf{N}_n \backslash \mathbf{N}_r$, $A_i \in \mathsf{M}_n$ $(i \in \mathbf{N}_n)$, $\mathbf{c}_i = (c_i^{(1)}, \dots, c_i^{(n)}) \in K^n$ $(i \in \mathbf{N}_n)$, $d_i \in K$ $(\mathbf{N}_r)$, $e_i, d_i \in K^{inv}$ $(\mathbf{N}_r)$.

Обозначим через $\widetilde{\mathcal{A}}_{n,3}$ множество всех автоматов M_3, определяемых формулой (5.14), а через $\widetilde{\mathcal{A}}_{n,4}$ – множество всех автоматов M_4, определяемых формулой (5.15).

Любой автомат $M \in \widetilde{\mathcal{A}}_{n,3} \cup \widetilde{\mathcal{A}}_{n,4}$ – обратимый, причем включения $\widetilde{\mathcal{A}}_{n,3} \subseteq \widetilde{\mathcal{A}}^{inv}_{n,1}$ и $\widetilde{\mathcal{A}}_{n,4} \subseteq \widetilde{\mathcal{A}}^{inv}_{n,2}$ истинны тогда и только тогда, когда $r = n$.

Пример 5.1. Построим автомат $M \in \widetilde{\mathcal{A}}_{n,4}$ для некоторых модельных хаотических динамических систем [38].

В случаях 1-3 осуществляется дискретизация с шагом h.

Информационная переменная вводится в 1-е уравнение и осуществляется переход к вычислениям в кольце $\mathcal{K}$.

1. Для системы Рёсслера

$$\begin{cases} \dot{x} = -y - x \\ \dot{y} = x + ay \\ \dot{z} = b + (x - r)z \end{cases}$$

получаем автомат ($a, b, r \in K$, а $d, h \in K^{inv}$)

$$M_R : \begin{cases} q^{(1)}_{t+1} = q^{(1)}_t - h \circ q^{(2)}_t - h \circ q^{(3)}_t - hdx_{t+1} \\ q^{(2)}_{t+1} = hq^{(1)}_t + (ah + 1)q^{(2)}_t \\ q^{(3)}_{t+1} = hb + (1 - hr)q^{(3)}_t + hq^{(1)}_t q^{(3)}_t \\ y_{t+1} = q^{(1)}_{t+1} \end{cases} \qquad (t \in \mathbf{Z}_+). \tag{5.16}$$

2. Для 1-й системы Спротта

$$\begin{cases} \dot{x} = y \\ \dot{y} = -x + yz \\ \dot{z} = 1 - y^2 \end{cases}$$

получаем автомат ($a, h \in K^{inv}$)

$$M_S : \begin{cases} q^{(1)}_{t+1} = q^{(1)}_t + hq^{(2)}_t - hax_{t+1} \\ q^{(2)}_{t+1} = q^{(2)}_t - hq^{(1)}_t + hq^{(2)}_t q^{(3)}_t \\ q^{(3)}_{t+1} = h + q^{(3)}_{t+1} - h(q^{(2)}_t)^2 \\ y_{t+1} = q^{(1)}_{t+1} \end{cases} \qquad (t \in \mathbf{Z}_+). \tag{5.17}$$

3. Для системы Лоренца

$$\begin{cases} \dot{x} = a_1(y - z) \\ \dot{y} = x(a_2 - z) - y \\ \dot{z} = xy - a_3 z \end{cases}$$

получаем автомат ($a_1, a_2, a_3 \in K$, а $a, h \in K^{inv}$)

$$M_L : \begin{cases} q_{t+1}^{(1)} = (1 - ha_1)q_t^{(1)} + ha_1 q_t^{(1)} \\ q_{t+1}^{(2)} = (1 - h)q_t^{(2)} + hq_t^{(1)}(a_2 - q_t^{(3)}) - hax_{t+1} \\ q_{t+1}^{(3)} = (1 - ha_3)q_t^{(3)} + hq_t^{(1)}q_t^{(2)} \\ y_{t+1} = q_{t+1}^{(2)} \end{cases} \quad (t \in \mathbf{Z}_+). \tag{5.18}$$

4. Для отображения Эно

$$\begin{cases} x_{n+1} = 1 - ax_n^2 - by_n \\ y_{n+1} = x_n \end{cases} \quad (n \in \mathbf{Z}_+)$$

получаем автомат ($a, b \in K$, а $c \in K^{inv}$)

$$M_H : \begin{cases} q_{t+2} = 1 - aq_{t+1}^2 - bq_t + cx_{t+1} \\ y_{t+1} = q_{t+2} \end{cases} \quad (t \in \mathbf{Z}_+). \tag{5.19}$$

5.2. Характеристики исследуемых моделей.

Одной из основных задач анализа конечных автоматов является поиск условий их принадлежности нетривиальным подмножествам автоматов, имеющим многочисленные приложения.

Такие условия дают также возможность осуществить метрический анализ, т.е. оценить мощности соответствующих подмножеств автоматов. Как следствие, может быть оценена вероятность того, что случайно выбранный автомат принадлежит тому или иному подмножеству автоматов.

Именно решение этих задач для исследуемых моделей и рассматривается ниже.

5.2.1. Схема анализа конечно-автоматных характеристик.

Пусть множество автоматов $\mathcal{A}$ над кольцом $\mathcal{K}$ определяется конечным множеством параметров S, причем выбор каждого параметра осуществляется независимо из конечного множества параметров Ω возможных значений. Тогда

$$|\mathcal{A}| = |\Omega|^{|S|}. \tag{5.20}$$

Анализ принадлежности автоматов нетривиальным подмножествам множества $\mathcal{A}$, характеризуемым в терминах теории автоматов («быть

перестановочным автоматом», «быть приведенным автоматом», «иметь данную степень различимости состояний», «иметь данный диаметр графа переходов», «быть обратимым автоматом» и т.д.), укладывается в рамки следующей схемы.

Схема 5.1. Фиксируются непустые попарно непересекающиеся подмножества Ω_i $(i = 1, \ldots, l)$ множества Ω, а также непустые попарно непересекающиеся подмножества S_i $(i = 1, \ldots, l)$ множества S.

Далее доказывается одно из следующих трех утверждений.

Утверждение 5.1. (Достаточное условие). Если параметры, принадлежащие подмножеству S_i $(i = 1, \ldots, l)$, принимают значения, принадлежащие множеству Ω_i, то автомат $M \in \mathcal{A}$ принадлежит подмножеству $\mathcal{A}_1$ множества $\mathcal{A}$.

Утверждение 5.2. (Необходимое условие). Для любого автомата $M \in \mathcal{A}_1$ параметры, принадлежащие подмножеству S_i $(i = 1, \ldots, l)$, принимают значения из множества Ω_i.

Утверждение 5.3. (Критерий). Автомат $M \in \mathcal{A}$ принадлежит подмножеству $\mathcal{A}_1$ множества $\mathcal{A}$ тогда и только тогда, когда параметры, принадлежащие подмножеству S_i $(i = 1, \ldots, l)$, принимают значения из множества Ω_i.

Из схемы 5.1 вытекает следующая характеристика множества $\mathcal{A}_1$.

Теорема 5.3. Если истинно утверждение $5.i$ $(i = 1, 2, 3)$, то истинна оценка

$$|\mathcal{A}_1| \Diamond |\mathcal{A}| \prod_{i=1}^{l} \left(\frac{|\Omega_i|}{|\Omega|} \right)^{|S_i|}, \tag{5.21}$$

где

$$\Diamond = \begin{cases} \geq, & \text{если истинно утверждение 5.1} \\ \leq, & \text{если истинно утверждение 5.2} \\ =, & \text{если истинно утверждение 5.3} \end{cases}. \tag{5.22}$$

Доказательство. Из формулировки утверждений 5.1-5.3, а также определения множества автоматов $\mathcal{A}$ вытекает, что при построении автомата $M \in \mathcal{A}_1$ осуществляется независимый выбор из множеств Ω_i

$(i = 1, \ldots, l)$ значений параметров, принадлежащих подмножеству S_i, а также независимый выбор из множества Ω значений параметров, принадлежащих множеству $S \setminus \left(\bigcup_{i=1}^{l} S_i \right)$.

Так как S_i $(i = 1, \ldots, l)$ – попарно непересекающиеся множества, то

$$|\mathcal{A}_1| \lozenge \prod_{i=1}^{l} |\Omega_i|^{|S_i|} |\Omega|^{|S| - \sum_{i=1}^{l} |S_i|} = |\Omega|^{|S|} \prod_{i=1}^{l} \left(\frac{|\Omega_i|}{|\Omega|} \right)^{|S_i|}, \tag{5.23}$$

где $\lozenge$ определяется формулой (5.22).

Воспользовавшись в (5.23) формулой (5.20), получим (5.21).

□

Следствие 5.4. Если на множестве Ω задано равномерное распределение, а $\mathsf{P}_{\mathcal{A}_1}$ – вероятность того, что случайно выбранный автомат $M \in \mathcal{A}$ принадлежит множеству $\mathcal{A}_1$, то

$$\mathsf{P}_{\mathcal{A}_1} \lozenge \prod_{i=1}^{l} \left(\frac{|\Omega_i|}{|\Omega|} \right)^{|S_i|}, \tag{5.24}$$

где $\lozenge$ определяется формулой (5.22).

Доказательство. Так как выбор значения каждого параметра, принадлежащего множеству S осуществляется независимо из конечного множества Ω, на котором задано равномерное распределение, то на множестве $\mathcal{A}$ также задано равномерное распределение.

Следовательно,

$$\mathsf{P}_{\mathcal{A}_1} = \frac{|\mathcal{A}_1|}{|\mathcal{A}|}. \tag{5.25}$$

Подставив (5.20) и (5.21) в (5.25), получим (5.24)

□

Под «временной сложностью» будем понимать «временную сложность в худшем случае», т.е. наибольшее время, необходимое алгоритму для

анализа объекта, если объект принадлежит заданному конечному множеству объектов.

Обозначим T_{S_i} $(i = 1, \ldots, l)$ временную сложность проверки принадлежности параметра $s \in S$ множеству S_i (т.е. временную сложность проверки того, что значение параметра $s \in S$ принадлежит множеству Ω_i), а $T_{\mathcal{A}_1}$ – временную сложность проверки принадлежности автомата $M \in \mathcal{A}$ множеству $\mathcal{A}_1$.

Из формулировки утверждений 5.2 и 5.3 вытекает

$$T_{\mathcal{A}_1} \begin{cases} \geq \sum\limits_{i=1}^{l} |S_i| T_{S_i}, & \text{если истинно утверждение 5.2} \\ = \sum\limits_{i=1}^{l} |S_i| T_{S_i}, & \text{если истинно утверждение 5.3} \end{cases}. \tag{5.26}$$

Выделим два специальных случая рассмотренной схемы.

Случай 5.1. Пусть $l = 1$. Тогда формулы (5.21), (5.24) и (5.26) принимают, соответственно, вид

$$|\mathcal{A}_1| \Diamond |\mathcal{A}| \left(\frac{|\Omega_1|}{|\Omega|} \right)^{|S_1|}, \tag{5.27}$$

$$\mathsf{P}_{\mathcal{A}_1} \Diamond \left(\frac{|\Omega_1|}{|\Omega|} \right)^{|S_1|}, \tag{5.28}$$

$$T_{\mathcal{A}_1} \begin{cases} \geq |S_1| T_{S_1}, & \text{если истинно утверждение 5.2} \\ = |S_1| T_{S_1}, & \text{если истинно утверждение 5.3} \end{cases}. \tag{5.29}$$

Случай 5.2. Пусть $l = 1$ и $\Omega_1 \cup \Omega_2 = \Omega$. Тогда формулы (5.21), (5.24) и (5.26) принимают, соответственно, вид

$$|\mathcal{A}_1| \Diamond |\mathcal{A}| \left(\frac{|\Omega_1|}{|\Omega|} \right)^{|S_1|} \left(1 - \frac{|\Omega_1|}{|\Omega|} \right)^{|S_1|}, \tag{5.30}$$

$$\mathsf{P}_{\mathcal{A}_1} \Diamond \left(\frac{|\Omega_1|}{|\Omega|} \right)^{|S_1|} \left(1 - \frac{|\Omega_1|}{|\Omega|} \right)^{|S_1|}, \tag{5.31}$$

$$T_{\mathcal{A}_1} \begin{cases} \geq (|S_1| + |S_2|) \min\{T_{S_1}, T_{S_2}\}, & \text{если истинно} \\ & \text{утверждение 4.2} \\ = (|S_1| + |S_2|) \min\{T_{S_1}, T_{S_2}\}, & \text{если истинно} \\ & \text{утверждение 4.3} \end{cases} . \qquad (5.32)$$

5.2.2. Характеристики нетривиальных подмножеств нелинейных автоматов общего вида.

Установим условия принадлежности автоматов, рассмотренных в п.5.1.1, нетривиальным подмножествам автоматов.

Утверждение 5.4. Автомат $M \in \mathcal{A}_{n,1} \cup \mathcal{A}_{n,2}$ над кольцом $\mathcal{K}$ – сильно связный автомат тогда и только тогда, когда $\mathbf{f}_3 : K^n \to K^n$ – биекция.

Доказательство. Отображение $\mathbf{f}_3 : K^n \to K^n$ – биекция тогда и только тогда, когда

$$|\{\mathbf{f}_1(\mathbf{q}) + \mathbf{f}_3(\mathbf{x}) | \mathbf{x} \in K^n\}| = |K^n|$$

для всех $\mathbf{q} \in K^n$, т.е. когда для любых состояний $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ автомата $M \in \mathcal{A}_{n,1} \cup \mathcal{A}_{n,2}$ существует такой входной символ $\mathbf{x} \in K^n$, что

$$\widetilde{\mathbf{q}} = \mathbf{f}_1(\mathbf{q}) + \mathbf{f}_3(\mathbf{x}).$$

Последнее эквивалентно тому, что $M \in \mathcal{A}_{n,1} \cup \mathcal{A}_{n,2}$ – сильно связный автомат над кольцом $\mathcal{K}$.

□

Из утверждения 5.4 вытекает, что истинны следующие два следствия.

Следствие 5.5. Автомат $M \in \mathcal{A}_{n,1} \cup \mathcal{A}_{n,2}$ над кольцом $\mathcal{K}$ – перестановочный автомат тогда и только тогда, когда $\mathbf{f}_3 : K^n \to K^n$ – биекция.

Следствие 5.6. Если отображение $\mathbf{f}_2 : K^n \to K^n$ не является биекцией, то диаметр графа переходов автомата $M \in \mathcal{A}_{n,1} \cup \mathcal{A}_{n,2}$ над кольцом $\mathcal{K}$ больше, чем 1.

Утверждение 5.5. В кольце $\mathcal{K}$, если $\mathbf{f}_3 : K^n \to K^n$ – биекция, то $M \in \mathcal{A}_{n,1}$ – приведенный автомат, любые два состояния которого различимы любым входным символом.

Доказательство. Если $\mathbf{f}_2 : K^n \to K^n$ – биекция, то

$$\mathbf{f}_2(\mathbf{q}) \neq \mathbf{f}_2(\widetilde{\mathbf{q}})$$

для любых $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$.

Следовательно,

$$\mathbf{y} = \mathbf{f}_2(\mathbf{q}) + \mathbf{f}_4(\mathbf{x}) \neq \mathbf{f}_2(\widetilde{\mathbf{q}}) + \mathbf{f}_4(\mathbf{x}) = \widetilde{\mathbf{y}}$$

для любых состояний $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ автомата $M \in \mathcal{A}_{n,1}$ и входного символа $\mathbf{x} \in K^n$.

□

Утверждение 5.6. В кольце $\mathcal{K}$, если $\mathbf{f}_1 : K^n \to K^n$ и $\mathbf{f}_2 : K^n \to K^n$ – биекции, то $M \in \mathcal{A}_{n,2}$ – приведенный автомат, любые два состояния которого различимы любым входным символом.

Доказательство. Если $\mathbf{f}_1 : K^n \to K^n$ – биекция, то

$$\mathbf{f}_1(\mathbf{q}) \neq \mathbf{f}_1(\widetilde{\mathbf{q}})$$

для любых $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$.

Следовательно,

$$\mathbf{f}_1(\mathbf{q}) + \mathbf{f}_3(\mathbf{x}) \neq \mathbf{f}_1(\widetilde{\mathbf{q}}) + \mathbf{f}_3(\mathbf{x})$$

для любых $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ и $\mathbf{x} \in K^n$.

Если же, кроме того, $\mathbf{f}_2 : K^n \to K^n$ – биекция, то

$$\mathbf{y} = \mathbf{f}_2(\mathbf{f}_1(\mathbf{q}) + \mathbf{f}_3(\mathbf{x})) \neq \mathbf{f}_2(\mathbf{f}_1(\widetilde{\mathbf{q}}) + \mathbf{f}_3(\mathbf{x})) = \widetilde{\mathbf{y}}$$

для любых состояний $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ автомата $M \in \mathcal{A}_{n,2}$ и входного символа $\mathbf{x} \in K^n$.

□

Два состояния автомата называются близнецами, если по любому входному символу они переходят в одно и то же состояние, а выдаваемые автоматом выходные символы совпадают.

Утверждение 5.7. В кольце $\mathcal{K}$ состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ автомата $M \in \mathcal{A}_{n,1} \cup \mathcal{A}_{n,2}$ являются близнецами тогда и только тогда, когда они принадлежат одному и тому же классу разбиения K^n/ε, где

$$\varepsilon = \ker \mathbf{f}_1 \cap \ker \mathbf{f}_2,$$

если $M \in \mathcal{A}_{n,1}$ и

$$\varepsilon = \ker \mathbf{f}_1,$$

если $M \in \mathcal{A}_{n,2}$.

Доказательство. Состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ автомата $M \in \mathcal{A}_{n,1}$ – близнецы тогда и только тогда, когда $\mathbf{f}_1(\mathbf{q}) = \mathbf{f}_1(\widetilde{\mathbf{q}})$ и $\mathbf{f}_2(\mathbf{q}) = \mathbf{f}_2(\widetilde{\mathbf{q}})$

Следовательно,

$$\mathbf{q} \equiv \widetilde{\mathbf{q}} \, (\ker \mathbf{f}_1 \cap \ker \mathbf{f}_2),$$

т.е. состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ принадлежат одному и тому классу разбиения $K^n/(\ker \mathbf{f}_1 \cap \ker \mathbf{f}_2)$.

Состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ автомата $M \in \mathcal{A}_{n,2}$ – близнецы тогда и только тогда, когда

$$\mathbf{f}_1(\mathbf{q}) = \mathbf{f}_1(\widetilde{\mathbf{q}}).$$

Последнее означает, что состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ принадлежат одному и тому классу разбиения $K^n/\ker \mathbf{f}_1$.

□

5.2.3. Характеристики нетривиальных подмножеств нелинейных автоматов над кольцом $\mathcal{Z}_m$.

Проиллюстрируем применение рассмотренной выше схемы анализа автоматов при установлении характеристк нетривиальных подмножеств автоматов над кольцом $\mathcal{Z}_m$.

Пример 5.2. Над кольцом $\mathcal{Z}_m$ мощности множеств $\widetilde{\mathcal{A}}_{n,i}, \widetilde{\mathcal{A}}^{inv}_{n,i}$ $(i = 1, 2)$ вычисляются по формулам

$$|\widetilde{\mathcal{A}}_{n,1}| = |\mathsf{M}_n|^5 m^{2n}, \tag{5.33}$$

$$|\widetilde{\mathcal{A}}_{n,2}| = |\mathsf{M}_n|^4 m^{2n}, \tag{5.34}$$

$$|\widetilde{\mathcal{A}}^{inv}_{n,1}| = |\mathsf{M}_n|^5 m^{2n} \prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}), \tag{5.35}$$

$$|\widetilde{\mathcal{A}}_{n,2}^{inv}| = |\mathsf{M}_n|^4 m^{2n} \left(\prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}) \right)^2. \tag{5.36}$$

Из (5.33)-(5.36) вытекает, что вероятность $\mathsf{P}_{\widetilde{\mathcal{A}}_{n,i}^{inv}}$ $(i = 1, 2)$ того, что случайно выбранный автомат $M \in \widetilde{\mathcal{A}}_{n,i}$ принадлежит множеству $\widetilde{\mathcal{A}}_{n,i}^{inv}$ вычисляется по формулам

$$\mathsf{P}_{\widetilde{\mathcal{A}}_{n,1}^{inv}} = \prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}),$$

$$\mathsf{P}_{\widetilde{\mathcal{A}}_{n,2}^{inv}} = \left(\prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}) \right)^2.$$

Из утверждения 5.4, следствия 5.5 и утверждения 5.6 вытекает, что:

1) автомат $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$ – сильно связный автомат, диаметр графа переходов которого равен 1 тогда и только тогда, когда $E \in \mathsf{M}_n^{inv}$;

2) автомат $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$ – перестановочный автомат тогда и только тогда, когда $E \in \mathsf{M}_n^{inv}$;

3) если $G, F \in \mathsf{M}_n^{inv}$, то $M \in \widetilde{\mathcal{A}}_{n,1}^{inv}$ – приведенный автомат, любые два состояния которого различимы любым входным символом.

Пусть $\widetilde{\mathcal{A}}_{n,i}^{sc}$ $(i = 1, 2)$ и $\widetilde{\mathcal{A}}_{n,i}^{prm}$ $(i = 1, 2)$ – множество всех, соответственно, сильно связных и перестановочных автоматов $M_i \in \widetilde{\mathcal{A}}_{n,i}$, а $\widetilde{\mathcal{A}}_{n,1}^{inv-rd}$ – множество всех приведенных автоматов $M_1 \in \widetilde{\mathcal{A}}_{n,2}^{inv}$. Тогда

$$|\widetilde{\mathcal{A}}_{n,1}^{sc}| \geq |\mathsf{M}_n|^5 m^{2n} \prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}), \tag{5.37}$$

$$|\widetilde{\mathcal{A}}_{n,2}^{sc}| \geq |\mathsf{M}_n|^4 m^{2n} \left(\prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}) \right)^2. \tag{5.38}$$

$$|\widetilde{\mathcal{A}}_{n,1}^{sc}| = |\mathsf{M}_n|^5 m^{2n} \prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}), \tag{5.39}$$

$$|\widetilde{\mathcal{A}}_{n,2}^{sc}| = |\mathsf{M}_n|^4 m^{2n} \left(\prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}) \right)^2. \tag{5.40}$$

$$|\widetilde{\mathcal{A}}_{n,1}^{inv-rd}| \geq |\mathsf{M}_n|^5 m^{2n} \left(\prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}) \right)^2. \tag{5.41}$$

Из (5.33), (5.34) и (5.37)-(5.41) вытекает, что вероятности выбора автомата с рассматриваемыми свойствами из множества всех автоматов данного типа вычисляются по формулам

$$\mathsf{P}_{\widetilde{\mathcal{A}}_{n,1}^{sc}} \geq \prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}),$$

$$\mathsf{P}_{\widetilde{\mathcal{A}}_{n,2}^{sc}} \geq \left(\prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}) \right)^2,$$

$$\mathsf{P}_{\widetilde{\mathcal{A}}_{n,1}^{sc}} = \prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}),$$

$$\mathsf{P}_{\widetilde{\mathcal{A}}_{n,2}^{sc}} = \left(\prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}) \right)^2,$$

$$\mathsf{P}_{\widetilde{\mathcal{A}}_{n,1}^{inv-rd}} \geq \left(\prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}) \right)^2.$$

5.3. Эквивалентность состояний исследуемых моделей.

Охарактеризуем классы эквивалентных состояний рассматриваемых автоматов.

Актуальность этой задачи с прикладной точки зрения обосновывается следующим обстоятельством.

Переход к приведенному автомату может существенно сократить поиск в пространстве состояний.

В то же время, переход к приведенному автомату может существенно усложнить систему уравнений, представляющую этот автомат. Как следствие, существенно возрастает сложность анализа системы уравнений, представляющей автомат, а работа с такой системой уравнений становится малоэффективной.

Сложность системы уравнений, представляющей приведенный автомат, во многом определяется сложностью структуры классов эквивалентных состояний.

Ниже показано, что для исследуемых автоматов классы эквивалентных состояний имеют достаточно сложную структуру. Отсюда вытекает, что при использовании таких автоматов в процессе решения прикладных задач переход к приведенному автомату нецелесообразен, прежде всего, с вычислительной точки зрения.

Кроме того, полученные ниже результаты показывают, что при использовании таких обратимых автоматов при построении поточных шифров, переход к приведенному автомату не облегчает работу криптоаналитика.

5.3.1. Эквивалентность состояний автомата $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$.

Если $G \in \mathsf{M}_n^{inv}$, то $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ – приведенный автомат, т.е. у автомата M_1 нет эквивалентных состояний.

Теорема 5.4. Если $G \in \mathsf{M}_n^{non-inv}$, то состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ эквивалентны тогда и только тогда, когда

$$G(\mathbf{q}_0^{(2)} - \mathbf{q}_0^{(1)}) = 0 \tag{5.42}$$

и

$$G(\mathbf{q}_t^{(2)} - \mathbf{q}_t^{(1)}) = 0 \ (t = 1, \ldots, |K^n| - 2). \tag{5.43}$$

для всех входных слов $\mathbf{x}_1 \ldots \mathbf{x}_t \in (K^n)^t$.

Доказательство. Известно (см., напр., [24]), что любые два неэквивалентных состояния автомата $M = (Q, X, Y, \delta, \lambda)$ являются $(|Q| - 1)$-различимыми состояниями.

Число состояний автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ равно K^n.

Следовательно, состояния $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(2)}$ автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ эквивалентны тогда и только тогда, когда

$$\mathbf{y}_1^{(2)} \cdots \mathbf{y}_{|K^n|-1}^{(2)} = \mathbf{y}_1^{(1)} \cdots \mathbf{y}_{|K^n|-1}^{(1)} \tag{5.44}$$

для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_{|K^n|-1} \in (K^n)^{|K^n|-1}$.

Из 2-го уравнения системы (5.12) вытекает, что равенство (5.44) истинно тогда и только тогда, когда

$$\mathbf{y}_1^{(2)} = \mathbf{y}_1^{(1)} \Leftrightarrow G(\mathbf{q}_0^{(2)} - \mathbf{q}_0^{(1)}) = 0$$

и

$$(\forall i = 2, \dots |K^n| - 1)(\mathbf{y}_i^{(2)} = \mathbf{y}_i^{(2)}) \Leftrightarrow$$

$$\Leftrightarrow (\forall i = 2, \dots |K^n| - 1)(G(\mathbf{q}_{i-1}^{(2)} - \mathbf{q}_{i-1}^{(1)}) = 0),$$

т.е. когда истинны равенства (5.42) и (5.43).

□

Теорема 5.5. Два различных состояния $\mathbf{q}_0^{(1)}, \mathbf{q}_0^{(2)} \in K^n$ автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}^{inv}$ эквивалентны тогда и только тогда, когда они являются близнецами.

Доказательство. Пусть состояния $\mathbf{q}_0^{(1)}, \mathbf{q}_0^{(2)} \in K^n$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}^{inv}$ являются близнецами. Тогда $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(1)}$ – эквивалентные состояния автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}^{inv}$.

Пусть $\mathbf{q}_0^{(1)}, \mathbf{q}_0^{(2)} \in K^n$ $(\mathbf{q}_0^{(1)} \neq \mathbf{q}_0^{(2)})$ – эквивалентные состояния автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}^{inv}$.

Подставив $\mathbf{q}_0^{(1)}$ и $\mathbf{q}_0^{(1)}$ во 2-е уравнение системы (4.13), получим, что

$$\mathbf{y}_1^{(i)} = G\mathbf{q}_1^{(i)} \ (i = 1, 2)$$

для всех $\mathbf{x}_1 \in K^n$.

Так как $\mathbf{q}_0^{(2)}$ и $\mathbf{q}_0^{(1)}$ – эквивалентные состояния автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}^{inv}$, то $\mathbf{y}_1^{(2)} = \mathbf{y}_1^{(1)}$ для всех $\mathbf{x}_1 \in K^n$.

Следовательно,

$$G(\mathbf{q}_0^{(2)} - \mathbf{q}_0^{(1)}) = 0.$$

А так как $G \in \mathsf{M}_n^{inv}$, то из последнего равенства вытекает, что

$$\mathbf{q}_0^{(2)} - \mathbf{q}_0^{(1)} = 0 \Leftrightarrow \mathbf{q}_0^{(2)} = \mathbf{q}_0^{(1)}$$

для всех $\mathbf{x}_1 \in K^n$, т.е. состояния $\mathbf{q}_0^{(2)}$ и $\mathbf{q}_0^{(1)}$ автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}^{inv}$ являются близнецами.

□

Из теоремы 5.5 вытекает, что истинно следующее следствие.

Следствие 5.7. Для любого состояния $\mathbf{q}_0 \in K^n$ автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}^{inv}$ множество всех состояний $\widetilde{\mathbf{q}}$, эквивалентных состоянию $\mathbf{q}_0$, совпадает с множеством решений уравнения

$$A(\widetilde{\mathbf{q}}\widetilde{\mathbf{q}}^T - \mathbf{q}_0\mathbf{q}_0^T)\mathbf{b} + C(\widetilde{\mathbf{q}} - \mathbf{q}_0) = 0 \tag{5.45}$$

5.3.2. Эквивалентность состояний автомата $M \in \widetilde{\mathcal{A}}_{n,3} \cup \widetilde{\mathcal{A}}_{n,4}$.

Для автомата $M \in \widetilde{\mathcal{A}}_{n,3}$ истинна следующая теорема.

Теорема 5.6. Состояния $\mathbf{q}_0 = (q_0^{(1)}, \ldots, q_0^{(n)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \ldots, \widetilde{q}_0^{(n)})^T$ автомата $M_3 \in \widetilde{\mathcal{A}}_{n,3}$ эквивалентны тогда и только тогда, когда

$$\widetilde{q}_0^{(i)} - q_0^{(i)} = 0 \ (i = 1, \ldots, r) \tag{5.46}$$

и

$$\widetilde{q}_t^{(i)} - q_t^{(i)} = 0 \ (i = 1, \ldots, r;\ t = 1, \ldots, |K^n| - 2) \tag{5.47}$$

для всех входных слов

$$(x_1^{(1)}, \ldots, x_1^{(r)}, \underbrace{0, \ldots, 0}_{n-r})^T \ldots (x_t^{(1)}, \ldots, x_t^{(r)}, \underbrace{0, \ldots, 0}_{n-r})^T \in (K^n)^t.$$

Доказательство теоремы 5.6 аналогично доказательству теоремы 4.4.
Из теоремы 5.6 вытекает, что истинно следующее следствие.

Следствие 5.8. Если $r = n$, то $M_3 \in \widetilde{\mathcal{A}}_{n,3}$ – приведенный автомат.

Для автомата $M \in \widetilde{\mathcal{A}}_{n,4}$ истинна следующая теорема.

Теорема 5.7. Состояния $\mathbf{q}_0 = (q_0^{(1)}, \ldots, q_0^{(n)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \ldots, \widetilde{q}_0^{(n)})^T$ автомата $M_4 \in \widetilde{\mathcal{A}}_{n,4}$ эквивалентны тогда и только тогда, когда

$$\widetilde{q}_t^{(i)} - q_t^{(i)} = 0 \ (i = 1, \ldots, r;\ t = 1, \ldots, |K^n| - 1) \tag{5.48}$$

для всех входных слов

$$(x_1^{(1)}, \ldots, x_1^{(r)}, \underbrace{0, \ldots, 0}_{n-r})^T \ldots (x_t^{(1)}, \ldots, x_t^{(r)}, \underbrace{0, \ldots, 0}_{n-r})^T \in (K^n)^t.$$

Доказательство теоремы 5.7 аналогично доказательству теоремы 5.4.
Из теоремы 5.7 вытекает, что истинно следующее следствие.

Следствие 5.9. Если $M_4 \in \widetilde{\mathcal{A}}_{n,4}$ – такой автомат, что $r = n$, то его состояния $\mathbf{q}_0 = (q_0^{(1)}, \ldots, q_0^{(n)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \ldots, \widetilde{q}_0^{(n)})^T$ эквивалентны тогда и только тогда, когда они являются близнецами.

Пример 5.3. Охарактеризуем классы эквивалентных состояний для автоматов, построенных в примере 5.1.

1. Рассмотрим автомат $M_R \in \widetilde{\mathcal{A}}_{3,4}$.

Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата M_R эквивалентны тогда и только тогда, когда

$$\begin{cases} \widetilde{q}_0^{(1)} = q_0^{(1)} - (a + h^{-1})\Delta \\ \widetilde{q}_0^{(2)} = q_0^{(2)} + \Delta \\ \widetilde{q}_0^{(3)} = q_0^{(3)} - (ah^{-1} + h^{-2} + 1)\Delta \end{cases}, \tag{5.49}$$

где Δ – решение уравнения

$$(ah + 1)(ah^{-1} + h^{-2} + 1)\Delta^2 - (q_0^{(3)}(ah + 1) + q_0^{(1)}(a + h^{-1} + h) +$$

$$+(1 - hr)(ah^{-1} + h^{-2} + 1))\Delta = 0. \tag{5.50}$$

Из (5.49) и (5.50) вытекает, что:

1) если у двух различных состояний $\mathbf{q}_0$ и $\widetilde{\mathbf{q}}_0$ автомата M_R совпадают вторые компоненты, то состояния $\mathbf{q}_0$ и $\widetilde{\mathbf{q}}_0$ – неэквивалентные состояния автомата M_R;

2) любые два различные эквивалентные состояния $\mathbf{q}_0$ и $\widetilde{\mathbf{q}}_0$ автомата M_R являются близнецами.

2. Рассмотрим автомат $M_S \in \widetilde{\mathcal{A}}_{3,4}$.

Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата M_S эквивалентны тогда и только тогда, когда

$$\begin{cases} \widetilde{q}_0^{(1)} - q_0^{(1)} + h(\widetilde{q}_0^{(2)} - q_0^{(2)}) = 0 \\ \widetilde{q}_0^{(2)} - q_0^{(2)} - h(\widetilde{q}_0^{(1)} - q_0^{(1)}) + h(\widetilde{q}_0^{(2)}\widetilde{q}_0^{(3)} - q_0^{(2)}q_0^{(3)}) = 0 \\ \widetilde{q}_t^{(2)}\widetilde{q}_t^{(3)} - q_t^{(2)}q_t^{(3)} = 0 \ \ (t = 1, \ldots, |K^3| - 3) \end{cases} \tag{5.51}$$

для всех $x_1 \ldots x_t \in (K^n)^t$.

Из (5.51) вытекает, что различные эквивалентные состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата M_S являются близнецами тогда и только тогда, когда

$$\begin{cases} \widetilde{q}_0^{(1)} = q_0^{(1)} - h\Delta \\ \widetilde{q}_0^{(2)} = q_0^{(2)} + \Delta \\ \widetilde{q}_0^{(3)} = q_0^{(3)} + 2hq_0^{(2)}\Delta + h\Delta^2 \end{cases} \tag{5.52}$$

где Δ – решение уравнения

$$\Delta^3 + 3q_0^{(2)}\Delta^2 + (2(q_0^{(2)})^2 + h^{-1}q_0^{(3)} + 1 + h^{-2})\Delta = 0. \tag{5.53}$$

3. Рассмотрим автомат $M_L \in \widetilde{\mathcal{A}}_{3,4}$.

Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата M_L эквивалентны тогда и только тогда, когда

$$\begin{cases} a_2(\widetilde{q}_0^{(1)} - q_0^{(1)}) + (h^{-1} - 1)(\widetilde{q}_0^{(2)} - q_0^{(2)}) - \widetilde{q}_t^{(1)}\widetilde{q}_t^{(3)} + q_t^{(1)}q_t^{(3)} = 0 \\ a_2(\widetilde{q}_t^{(1)} - q_t^{(1)}) - \widetilde{q}_t^{(1)}\widetilde{q}_t^{(3)} + q_t^{(1)}q_t^{(3)} = 0 \ (t = 1, \ldots, |K^3| - 2) \end{cases} \tag{5.54}$$

Из (5.54) вытекает, что различные эквивалентные состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата M_L являются близнецами тогда и только тогда, когда

$$\begin{cases} \widetilde{q}_0^{(1)} = q_0^{(1)} + \Delta_1 \\ \widetilde{q}_0^{(2)} = q_0^{(2)} + \Delta_2 \\ \widetilde{q}_0^{(3)} = q_0^{(3)} + \Delta_3 \end{cases} \tag{5.55}$$

где $(\Delta_1, \Delta_2, \Delta_3)$ – решение системы уравнений

$$\begin{cases} (h^{-1} - a_1)\Delta_1 + a_1\Delta_2 = 0 \\ (a_2 - q_0^{(3)})\Delta_1 + (h^{-1} - 1)\Delta_2 - q_0^{(1)}\Delta_3 - \Delta_1\Delta_3 = 0 \\ q_0^{(2)}\Delta_1 + q_0^{(1)}\Delta_2 + (h^{-1} - a_3)\Delta_3 + \Delta_1\Delta_2 \end{cases} . \tag{5.56}$$

4. Рассмотрим автомат $M_H \in \widetilde{\mathcal{A}}_{2,4}$.

Если $a = b = 0$, то M_H – автомат без памяти, т.е. автомат, реализующий отображение $f : K \to K$.

Если $a = 0$ и $b \neq 0$, то M_H – линейный автомат над кольцом $\mathcal{K}$.

В этом случае состояния $\mathbf{q}_0 = (q_1, q_0)^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_1, \widetilde{q}_0)^T$ автомата M_H эквивалентны тогда и только тогда, когда

$$b(\widetilde{q}_1 - q_1) = 0.$$

Пусть $a \neq 0$ и $b \neq 0$.

Выходной последовательностью, генерируемой автоматом M_H на любую входную последовательность $x_1 \ldots x_t \in K^t$ является последовательность $q_2 \ldots x_{t+1} \in K^t$.

Следовательно, состояния $\mathbf{q}_0 = (q_1, q_0)^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_1, \widetilde{q}_0)^T$ автомата M_H эквивалентны тогда и только тогда, когда

$$\begin{cases} a(\widetilde{q}_1^2 - q_0^2) - b(\widetilde{q}_1 - q_0) = 0 \\ b(\widetilde{q}_1 - q_1) = 0 \end{cases} . \tag{5.57}$$

Из (5.57) вытекает, что:

1) если $b \in K^{inv}$, то M_H – приведенный автомат;

2) два различных состояния $\mathbf{q}_0 = (q_1, q_0)^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_1, \widetilde{q}_0)^T$ автомата M_H являются близнецами тогда и только тогда, когда

$$\widetilde{q}_1 = q_1$$

и

$$b(\widetilde{q}_0 - q_0) = 0.$$

5.4. Задачи идентификации автомата $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$.

Исследование сложности решения задач идентификации начального состояния и параметрической идентификации автомата $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$ представляют интерес как с теоретической, так и прикладной точки зрения.

С теоретической точки зрения эти задачи являются модельными задачами теории систем.

С прикладной точки зрения, при использовании обратимого автомата в качестве математической модели поточного шифра, сложность решения этих задач является теоретическим обоснованием сложности атаки криптоаналитика, соответственно, на секретный сеансовый ключ и на секретный ключ средней длительности.

Поэтому с прикладной точки зрения особый интерес представляет исследование того, как свойство «быть обратимым автоматом» влияет на сложность решения этих задач.

5.4.1. Идентификация начального состояния.

Рассмотрим задачу идентификации начального состояния $\mathbf{q}_0 \in K^n$ автомата $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$ в предположении, что экспериментатор может проводить с автоматом M эксперимент любой кратности, т.е. экспериментатор полностью управляет входом автомата, а также полностью наблюдает выход автомата.

С прикладной точки зрения такое предположение соответствует одной из наиболее сильных атак криптоаналитика.

Отметим, что любой эксперимент с автоматом $M_i \in \widetilde{\mathcal{A}}_{n,i}$ $(i = 1, 2)$, не использующий контрольные точки, обеспечивающие дополнительную информацию о вычислениях функций переходов и выходов автомата, не

дает возможность восстановить начальное состояние с точностью, превосходящей множество $S_{\mathbf{q}_0}(M_i)$ состояний, эквивалентных состоянию $\mathbf{q}_0$.

Отсюда вытекает, что решение задачи идентификации начального состояния $\mathbf{q}_0 \in K^n$ автомата $M_i \in \widetilde{\mathcal{A}}_{n,i}$ $(i = 1, 2)$ сводится к поиску такого множества W $(\emptyset \neq W \subseteq K^n)$, что истинно включение

$$W \subseteq S_{\mathbf{q}_0}(M_i).$$

Рассмотрим вначале автомат $M_1 \in \widetilde{\mathcal{A}}_{n,1}$.

Перепишем 2-е уравнение системы уравнений (5.12) в виде

$$G\mathbf{q}_t = \mathbf{y}_{t+1} - F\mathbf{x}_{t+1} \ (t \in \mathbf{Z}_+). \tag{5.58}$$

Пусть $G \in \mathsf{M}_n^{inv}$.

Положив $t = 0$ в (5.58), получим, что

$$\mathbf{q}_0 = G^{-1}(\mathbf{y}_1 - F\mathbf{x}_1)$$

для любого входного символа $\mathbf{x}_1 \in K^n$, т.е. начальное состояние автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ однозначно определяется в результате любого простого эксперимента длины 1.

Отсюда, в частности вытекает,что если $G \in \mathsf{M}_n^{inv}$, то $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ – приведенный автомат.

Пусть $G \notin \mathsf{M}_n^{inv}$.

Из 1-го уравнения системы уравнений (5.12) вытекает, что для любого входного слова $\mathbf{x}_1 \dots \mathbf{x}_i \in (K^n)^i$ в системе уравнений

$$\begin{cases} G\mathbf{q}_0 = \mathbf{y}_1 - F\mathbf{x}_1 \\ \dots\dots\dots\dots\dots\dots \\ G\mathbf{q}_{i-1} = \mathbf{y}_i - F\mathbf{x}_i \end{cases} \tag{5.59}$$

каждое состояние $\mathbf{q}_1, \dots, \mathbf{q}_{i-1} \in K^n$ может быть выражено через начальное состояние $\mathbf{q}_0 \in K^n$ автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$.

Следовательно, (5.59) – это система (нелинейных, если $i \geq 1$) уравнений над кольцом $\mathcal{K}$ в которой неизвестным является начальное состояние $\mathbf{q}_0 \in K^n$ автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$.

Пусть $U(\mathbf{x}_1 \dots \mathbf{x}_i)$ – множество решений системы уравнений (5.59).

Тогда решение задачи идентификации начального состояния $\mathbf{q}_0 \in K^n$ автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ имеет следующий вид:

1. В случае простого эксперимента с автоматом $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ осуществляется поиск такого входного слова $\mathbf{x}_1 \dots \mathbf{x}_t \in (K^n)^t$ заранее неизвестной минимальной длины t, если такое слово вообще существует, что

$$U(\mathbf{x}_1 \dots \mathbf{x}_t) \subseteq S_{\mathbf{q}_0}(M_1)$$

и

$$U(\mathbf{x}_1 \dots \mathbf{x}_i) \not\subseteq S_{\mathbf{q}_0}(M_1)$$

для всех $i = 1, \dots, t-1$.

Множество $U(\mathbf{x}_1 \dots \mathbf{x}_t)$ и представляет собой решение задачи идентификации начального состояния $\mathbf{q}_0 \in K^n$ автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$.

2. В случае l-кратного ($l \geq 2$) эксперимента с автоматом $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ осуществляется поиск такого множества входных слов

$$\mathbf{x}_1^{(i)} \dots \mathbf{x}_{t_i}^{(i)} \in (K^n)^{t_i} \ (i = 1, \dots, l),$$

что

$$\bigcap_{i=1}^{l} U(\mathbf{x}_1^{(i)} \dots \mathbf{x}_{t_i}^{(i)}) \subseteq S_{\mathbf{q}_0}(M_1)$$

и

$$\bigcap_{i=1}^{l} U(\mathbf{x}_1^{(i)} \dots \mathbf{x}_{t_i - j_i}^{(i)}) \not\subseteq S_{\mathbf{q}_0}(M_1)$$

для любых таких чисел j_i ($0 \leq j_i < t_i$), что $\sum\limits_{i=1}^{l} j_i \geq 1$.

Множество $\bigcap\limits_{i=1}^{l} U(\mathbf{x}_1^{(i)} \dots \mathbf{x}_{t_i}^{(i)})$ и представляет собой решение задачи идентификации начального состояния $\mathbf{q}_0 \in K^n$ автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$.

Рассмотрим теперь автомат $M_2 \in \widetilde{\mathcal{A}}_{n,2}$.

Из системы уравнений (5.13) вытекает, что для для любого входного слова $\mathbf{x}_1 \dots \mathbf{x}_i \in (K^n)^i$ в системе уравнений

$$\begin{cases} G(A\mathbf{q}_0\mathbf{q}_0^T\mathbf{b} + C\mathbf{q}_0) = \mathbf{y}_1 - G(E\mathbf{x}_1 + \mathbf{d}) \\ G(A\mathbf{q}_1\mathbf{q}_1^T\mathbf{b} + C\mathbf{q}_1) = \mathbf{y}_2 - G(E\mathbf{x}_2 + \mathbf{d}) \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ G(A\mathbf{q}_{i-1}\mathbf{q}_{i-1}^T\mathbf{b} + C\mathbf{q}_{i-1}) = \mathbf{y}_i - G(E\mathbf{x}_i + \mathbf{d}) \end{cases} \tag{5.60}$$

каждое состояние $\mathbf{q}_1, \ldots, \mathbf{q}_{i-1} \in K^n$ может быть выражено через начальное состояние $\mathbf{q}_0 \in K^n$ автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}$.

Следовательно, (5.60) – это система нелинейных уравнений над кольцом $\mathcal{K}$ в которой неизвестным является начальное состояние $\mathbf{q}_0 \in K^n$ автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}$.

Пусть $V(\mathbf{x}_1 \ldots \mathbf{x}_i)$ – множество решений системы уравнений (5.60).

Тогда решение задачи идентификации начального состояния $\mathbf{q}_0 \in K^n$ автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}$ имеет следующий вид:

1. В случае простого эксперимента с автоматом $M_2 \in \widetilde{\mathcal{A}}_{n,2}$ осуществляется поиск такого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in (K^n)^t$ заранее неизвестной минимальной длины t, если такое слово вообще существует, что

$$V(\mathbf{x}_1 \ldots \mathbf{x}_t) \subseteq S_{\mathbf{q}_0}(M_2)$$

и

$$V(\mathbf{x}_1 \ldots \mathbf{x}_i) \not\subseteq S_{\mathbf{q}_0}(M_2)$$

для всех $i = 1, \ldots, t-1$.

Множество $V(\mathbf{x}_1 \ldots \mathbf{x}_t)$ – решение задачи идентификации начального состояния $\mathbf{q}_0 \in K^n$ автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}$.

2. В случае l-кратного ($l \geq 2$) эксперимента с автоматом $M_2 \in \widetilde{\mathcal{A}}_{n,2}$ осуществляется поиск такого множества входных слов

$$\mathbf{x}_1^{(i)} \ldots \mathbf{x}_{t_i}^{(i)} \in (K^n)^{t_i} \ (i = 1, \ldots, l),$$

что

$$\bigcap_{i=1}^{l} V(\mathbf{x}_1^{(i)} \ldots \mathbf{x}_{t_i}^{(i)}) \subseteq S_{\mathbf{q}_0}(M_2)$$

и

$$\bigcap_{i=1}^{l} V(\mathbf{x}_1^{(i)} \ldots \mathbf{x}_{t_i - j_i}^{(i)}) \not\subseteq S_{\mathbf{q}_0}(M_2)$$

для любых таких чисел j_i $(0 \leq j_i < t_i)$, что $\sum\limits_{i=1}^{l} j_i \geq 1$.

Множество $\bigcap\limits_{i=1}^{l} V(\mathbf{x}_1^{(i)} \ldots \mathbf{x}_{t_i}^{(i)})$ – решение задачи идентификации начального состояния $\mathbf{q}_0 \in K^n$ автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}$.

Полученные результаты показывают, что задача идентификации начального состояния $\mathbf{q}_0 \in K^n$ автомата $M \in \widetilde{\mathcal{A}}_{n,1}$ – тривиальная задача, если $G \in \mathsf{M}_n^{inv}$.

Во всех остальных случаях задача идентификации начального состояния $\mathbf{q}_0 \in K^n$ автомата $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$ – трудная задача. Высокая сложность ее решения обусловлена следующими обстоятельствами.

Во-первых, это сложность поиска по множеству входных слов.

Во-вторых, это сложность поиска решений систем уравнений над кольцом $\mathcal{A}$ (даже над полями Галуа $GF(2^k)$ решение системы уравнений 2-й степени от многих переменных – NP-полная задача).

В-третьих, это сложность проверки свойства «быть подмножеством множества эквивалентных состояний автомата».

Кроме того, условие $M \in \widetilde{\mathcal{A}}^{inv}_{n,1} \cup \widetilde{\mathcal{A}}^{inv}_{n,2}$ не упрощает решение задачи идентификации начального состояния исследуемых моделей, что обосновывает целесообразность выбора начального состояния автомата $M \in \widetilde{\mathcal{A}}^{inv}_{n,1} \cup \widetilde{\mathcal{A}}^{inv}_{n,2}$ в качестве секретного сеансового ключа для соответствующего поточного шифра.

5.4.2. Параметрическая идентификация.

Задачу параметрической идентификации автомата $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$ рассмотрим в предположении, что экспериментатор полностью управляет входом автомата и его инициализацией, а также полностью наблюдает выход автомата.

Рассмотрим автомат $M_1 \in \widetilde{\mathcal{A}}_{n,1}$.

Положив

$$\mathbf{q}_0 = \mathbf{0},$$

из 2-го уравнения системы уравнений (5.12) получим, что

$$F\mathbf{x}_1 = \mathbf{y}_1. \tag{5.61}$$

Из (5.61) вытекает, что если

$$\mathbf{x}_1 = (\underbrace{0,\ldots,0}_{i-1},1,\underbrace{0,\ldots,0}_{n-i})^T \ (i = 1,\ldots,n),$$

то $\mathbf{y}_1$ - i-й столбец матрицы F.

Следовательно, идентификация матрицы F осуществляется в результате n-кратного эксперимента высоты 1.

Положив

$$\mathbf{x}_1 = \mathbf{0},$$

из 2-го уравнения системы уравнений (5.12) получим, что

$$G\mathbf{q}_0 = \mathbf{y}_1. \tag{5.62}$$

Из (5.62) вытекает, что если

$$\mathbf{q}_0 = (\underbrace{0,\ldots,0}_{i-1},1,\underbrace{0,\ldots,0}_{n-i})^T \ (i=1,\ldots,n),$$

то $\mathbf{y}_1$ - i-й столбец матрицы G.

Следовательно, идентификация матрицы G осуществляется в результате n-кратного эксперимента высоты 1.

В дальнейшем считаем, что матрицы G и F известны.

Из системы уравнений (5.12) вытекает, что

$$G(A\mathbf{q}_0\mathbf{q}_0^T\mathbf{b} + C\mathbf{q}_0 + \mathbf{d} + E\mathbf{x}_1) = \mathbf{y}_2 - F\mathbf{x}_2. \tag{5.63}$$

Положив

$$\mathbf{q}_0 = \mathbf{0}$$

и

$$\mathbf{x}_1 = \mathbf{0}$$

в (5.63), получим

$$G\mathbf{d} = \mathbf{y}_2 - F\mathbf{x}_2. \tag{5.64}$$

Из (5.64) вытекает, что если $G \in \mathsf{M}_n^{inv}$, то при известных матрицах G и F идентификация вектора $\mathbf{d}$ осуществляется в результате простого эксперимента длины 2.

Если же $G \in \mathsf{M}_n^{non-inv}$, то множество S_1 решений уравнения (4.64) определяет возможные значения вектора $\mathbf{d}$.

Дальнейшие вычисления необходимо осуществлять для каждого значения $\mathbf{d} \in S_1$.

В дальнейшем считаем, что вектор $\mathbf{d}$ известен.

Преобразуем уравнение (5.63) к виду

$$G(A\mathbf{q}_0\mathbf{q}_0^T\mathbf{b} + C\mathbf{q}_0 + E\mathbf{x}_1) = \mathbf{y}_2 - F\mathbf{x}_2 - G\mathbf{d}. \tag{5.65}$$

Положив

$$\mathbf{q}_0 = \mathbf{0}$$

в (5.65), получим

$$GE\mathbf{x}_1 = \mathbf{y}_2 - F\mathbf{x}_2 - G\mathbf{d}. \tag{5.66}$$

Если $G \in \mathsf{M}_n^{non-inv}$, то уравнение (5.66) преобразуется в эквивалентное уравнение

$$E\mathbf{x}_1 = G^{-1}(\mathbf{y}_2 - F\mathbf{x}_2 - G\mathbf{d}). \tag{5.67}$$

Из (5.67) вытекает, что если

$$\mathbf{x}_1 = (\underbrace{0,\ldots,0}_{i-1},1,\underbrace{0,\ldots,0}_{n-i})^T \ (i = 1,\ldots,n),$$

то при известных матрицах G, F и векторе $\mathbf{d}$ идентификация матрицы E осуществляется в результате n-кратного эксперимента высоты 2.

Если же $G \in \mathsf{M}_n^{non-inv}$, то множество S_2 решений уравнения (5.67) определяет возможные значения матрицы E.

Дальнейшие вычисления необходимо осуществлять для каждого значения $E \in S_2$.

В дальнейшем считаем, что матрица E известна.

Преобразуем уравнение (5.65) к виду

$$G(A\mathbf{q}_0\mathbf{q}_0^T\mathbf{b} + C\mathbf{q}_0) = \mathbf{y}_2 - F\mathbf{x}_2 - GE\mathbf{x}_1 - G\mathbf{d}. \tag{5.68}$$

Обозначим $S_3(\mathbf{q}_0)$ множество решений уравнения (5.68).

Если

$$\Big|\bigcap_{\mathbf{q}_0 \in K^n} S_3(\mathbf{q}_0)\Big| = 1,$$

то матрицы A, C и вектор $\mathbf{b}$ идентифицируются единственным образом в результате некоторого l-кратного ($l \le |K|^n$) эксперимента высоты 1.

В противном случае осуществляется поиск входных слов заранее неизвестной длины и соответствующих начальных состояний с целью формирования системы уравнений вида

$$G(A\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + C\mathbf{q}_t) = \mathbf{y}_{t+2} - F\mathbf{x}_{t+2} - GE\mathbf{x}_{t+1} - G\mathbf{d} \ (t = 0,1,\ldots,l). \tag{5.69}$$

В системе уравнений (5.69) каждое состояние $\mathbf{q}_t$ $(t = 1, \ldots, l)$ с помощью 1-го уравнения системы уравнений (5.12) выражается через $A, \mathbf{b}, C, \mathbf{d}, E, \mathbf{q}_0, \mathbf{x}_1, \ldots, \mathbf{x}_t$.

Решения полученной таким образом системы нелинейных уравнений – возможные значения матриц A, C и вектора $\mathbf{b}$.

Рассмотрим автомат $M_2 \in \widetilde{\mathcal{A}}_{n,2}$.

Из системы уравнений (5.13) вытекает, что

$$(GA)\mathbf{q}_0\mathbf{q}_0^T\mathbf{b} + (GC)\mathbf{q}_0) + G\mathbf{d} + (GE)\mathbf{x}_1 = \mathbf{y}_1. \tag{5.70}$$

Положив

$$\mathbf{q}_0 = \mathbf{0}$$

и

$$\mathbf{x}_1 = \mathbf{0}$$

в (5.70), получим

$$G\mathbf{d} = \mathbf{y}_1,$$

т.е. идентификация вектора $G\mathbf{d}$ осуществляется в результате простого эксперимента длины 1.

В дальнейшем считаем, что вектор $G\mathbf{d}$ известен.

Преобразуем уравнение (5.70) к виду

$$(GA)\mathbf{q}_0\mathbf{q}_0^T\mathbf{b} + (GC)\mathbf{q}_0) + (GE)\mathbf{x}_1 = \mathbf{y}_1 - G\mathbf{d}. \tag{5.71}$$

Положив

$$\mathbf{q}_0 = \mathbf{0}$$

в (5.71), получим

$$(GE)\mathbf{x}_1 = \mathbf{y}_1 - G\mathbf{d}. \tag{5.72}$$

Из (5.72) вытекает, что если

$$\mathbf{x}_1 = (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i})^T,$$

то $\mathbf{y}_1 - G\mathbf{d}$ – i-й столбец матрицы матрицы GE.

Следовательно, при известном векторе $G\mathbf{d}$ идентификация матрицы GE осуществляется в результате n-кратного эксперимента высоты 1.

В дальнейшем считаем, что матрица GE известна.

Преобразуем уравнение (5.71) к виду

$$(GA)\mathbf{q}_0\mathbf{q}_0^T\mathbf{b} + (GC)\mathbf{q}_0) = \mathbf{y}_1 - G\mathbf{d}(GE)\mathbf{x}_1. \tag{5.73}$$

Обозначим $S_4(\mathbf{q}_0)$ множество решений уравнения (5.73).

Если

$$\left| \bigcap_{\mathbf{q}_0 \in K^n} S_4(\mathbf{q}_0) \right| = 1,$$

то каждая из матриц GA и GC, а также вектор $\mathbf{b}$ идентифицируются единственным образом в результате некоторого l-кратного ($l \leq |K|^n$) эксперимента высоты 1.

В противном случае осуществляется поиск входных слов заранее неизвестной длины и соответствующих начальных состояний с целью формирования системы уравнений вида

$$(GA)\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + (GC)\mathbf{q}_t) = \mathbf{y}_{t+2} - (GE)\mathbf{x}_{t+1} - G\mathbf{d} \ (t = 0, 1, \ldots, l). \tag{5.74}$$

Дальнейшие действия с системой уравнений (5.74) такие же, как и с системой уравнений (5.69).

Полученные результаты показывают, что для автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ идентификация матриц G и F осуществляется достаточно легко.

Сложность идентификации вектора $\mathbf{d}$ и матрицы E существенно зависит от того, является ли матрица G обратимой матрицей.

При положительном ответе идентификация вектора $\mathbf{d}$ и матрицы E также осуществляется достаточно легко.

Однако, если матрица G не является обратимой матрицей, то приходится осуществлять перебор по множествам решений уравнений (5.64) и (5.66).

Трудной задачей является идентификация матриц A, C и вектора $\mathbf{b}$, так как приходится формировать и решать системы нелинейных уравнений над кольцом $\mathcal{K}$.

Кроме того, условие $M \in \widetilde{\mathcal{A}}_{n,1}^{inv} \cup \widetilde{\mathcal{A}}_{n,2}^{inv}$ не упрощает решение задачи параметрической идентификации исследуемых моделей.

Поэтому при использовании автомата $M \in \widetilde{\mathcal{A}}_{n,1}^{inv} \cup \widetilde{\mathcal{A}}_{n,2}^{inv}$ в качестве поточного шифра (в этом случае параметры играют роль секретного ключа средней или большой длительности) следует уделить особое внимание обеспечению секретности параметров A, C и $\mathbf{b}$.

Пример 5.4. Решим задачу параметрической идентификации для автоматов, построенных в примере 5.1.

1. Рассмотрим автомат $M_R \in \widetilde{\mathcal{A}}_{3,4}$.
Положив $\mathbf{q}_0 = (0,1,0)^T$ и $x_1 = 0$, получим

$$h = -y_1.$$

Положив $\mathbf{q}_0 = (0,0,0)^T$ и $x_1 = 0$, получим

$$d = -h^{-1}y_1.$$

Положив $\mathbf{q}_0 = (0,0,0)^T$ и $x_1x_2 = 00$, получим

$$b = -h^{-2}y_2.$$

Положив $\mathbf{q}_0 = (0,0,1)^T$ и $x_1x_2 = 00$, получим

$$r = -h^{-2}y_2 + 2h^{-1} - b$$

Положив $\mathbf{q}_0 = (0,1,0)^T$ и $x_1x_2 = 00$, получим

$$a = -2h^{-1} - b - h^{-2}y_2.$$

2. Рассмотрим автомат $M_S \in \widetilde{\mathcal{A}}_{3,4}$.
Положив $\mathbf{q}_0 = (0,1,0)^T$ и $x_1 = 0$, получим

$$h = y_1.$$

Положив $\mathbf{q}_0 = (0,0,0)^T$ и $x_1 = 1$, получим

$$a = -h^{-1}y_1.$$

3. Рассмотрим автомат $M_L \in \widetilde{\mathcal{A}}_{3,4}$.
Положив $\mathbf{q}_0 = (0,1,0)^T$ и $x_1 = 0$, получим

$$h = 1 - y_1.$$

Положив $\mathbf{q}_0 = (0,0,0)^T$ и $x_1 = 1$, получим

$$a = -h^{-1}y_1.$$

Положив $\mathbf{q}_0 = (1,0,0)^T$ и $x_1x_2 = 00$, получим

$$a_2 = h^{-1}y_1$$

и

$$y_2 = ha_2(2 - h - ha_1). \tag{5.75}$$

Из уравнения (5.75) находим множество допустимых значений параметра a_1.
Положив $\mathbf{q}_0 = (1, 0, 1)^T$ и $x_1x_2 = 00$, получим

$$y_2 = (1 - h)h(a_2 - 1) + h(1 - ha_1)(a_2 + ha_3 - 1). \tag{5.76}$$

Из уравнения (5.76) находим множество допустимых значений параметра a_3.

4. Рассмотрим автомат $M_H \in \widetilde{\mathcal{A}}_{2,4}$.
Положив $\mathbf{q}_0 = (0, 0)^T$ и $x_1 = 1$, получим

$$c = y_1 - 1.$$

Положив $\mathbf{q}_0 = (0, 1)^T$ и $x_1 = 0$, получим

$$a = y_1 - 1.$$

Положив $\mathbf{q}_0 = (1, 0)^T$ и $x_1 = 0$, получим

$$a = y_1 - 1.$$

5.5. Неподвижные точки автоматных отображений.

Для автомата, у которого входной алфавит совпадает с выходным алфавитом, отображение входной полугруппы в себя, реализуемое инициальным автоматом, может отображать некоторые входные слова на себя. Такие входные слова называются неподвижными точками соответствующего автоматного отображения.

В том случае, когда обратимый автомат используется в качестве математической модели поточного шифра, множество неподвижных точек является множеством тех сообщений, которые для данного шифра остаются незашифрованными. Поэтому исследование множеств неподвижных точек аывтоматных отображений имеет не только теоретическое, но и прикладное значение.

Охарактеризуем множества неподвижных точек для исследуемых моделей.

5.5.1. Основные понятия.

Множество $S_{fxd}(M, \mathbf{q}_0)$ всех неподвижных точек отображения

$$f_{(M,\mathbf{q}_0)} : (K^n)^+ \to (K^n)^+,$$

реализуемого инициальным автоматом $(M, \mathbf{q}_0)$, определяется равенством

$$S_{fxd}(M, \mathbf{q}_0) = \{\mathbf{u} \in (K^n)^+ | f_{(M,\mathbf{q}_0)}(\mathbf{u}) = \mathbf{u}\}.$$

Положим

$$S^{(i)}_{fxd}(M, \mathbf{q}_0) = S_{fxd}(M, \mathbf{q}_0) \cap (K^n)^i \ (i \in \mathbf{N}).$$

Тогда:

1) истинно равенство

$$S_{fxd}(M, \mathbf{q}_0) = \bigcup_{i=1}^{\infty} S^{(i)}_{fxd}(M, \mathbf{q}_0);$$

2) для любых таких $i_1, i_2 \in \mathbf{N}$, что $(i_1 \neq i_2)$ истинно равенство

$$S^{(i_1)}_{fxd}(M, \mathbf{q}_0) \cap S^{(i_2)}_{fxd}(M, \mathbf{q}_0) = \emptyset;$$

3)для каждого $i \in \mathbf{N}$ истинно включение

$$S^{(i+1)}_{fxd}(M, \mathbf{q}_0) \subseteq \{\mathbf{ux} | \mathbf{u} \in S^{(i)}_{fxd}(M, \mathbf{q}_0), \mathbf{x} \in K^n\};$$

4) если

$$S^{(i)}_{fxd}(M, \mathbf{q}_0) = \emptyset,$$

то

$$S^{(i+k)}_{fxd}(M, \mathbf{q}_0) = \emptyset \ (k \in \mathbf{N});$$

5) $S_{fxd}(M, \mathbf{q}_0)$ – конечное множество тогда и только тогда, когда существует такое $i \in \mathbf{N}$, что

$$S^{(i)}_{fxd}(M, \mathbf{q}_0) = \emptyset.$$

Из установленных свойств вытекает, что достаточно исследовать множества $S^{(1)}_{fxd}(M, \mathbf{q}_0)$ $(\mathbf{q}_0 \in K^n)$.

5.5.2. Неподвижные точки для автомата $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$.

Пусть $I \in \mathsf{M}^{inv}_n$ – единичная матрица.

Из 2-го уравнения системы уравнений (5.12) вытекает, что истинно следующее утверждение.

Утверждение 5.8. Для любого автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ и любого начального состояния $\mathbf{q}_0 \in K^n$ множество $S^{(1)}_{fxd}(M_1, \mathbf{q}_0)$ непусто тогда и только тогда, когда имеет решения уравнение

$$(I - F)\mathbf{x} = G\mathbf{q}_0. \tag{5.77}$$

Из утверждения 5.8 вытекает, что истинны следующие два следствия.

Следствие 5.10. Если $I - F \in \mathsf{M}_n^{inv}$, то для автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ при любом начальном состоянии $\mathbf{q}_0 \in K^n$:

1) $|S^{(i)}_{fxd}(M_1, \mathbf{q}_0)| = 1$ $(i \in \mathbf{N})$;

2) $S_{fxd}(M_1, \mathbf{q}_0)$ – бесконечное множество.

Следствие 5.11. Если $F = I$, то $S^{(1)}_{fxd}(M_1, \mathbf{q}_0) = K^n$ для автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ при любом таком начальном состоянии $\mathbf{q}_0 \in K^n$, что

$$G\mathbf{q}_0 = \mathbf{0}.$$

Из системы уравнений (5.13) вытекает, что истинно утверждение.

Утверждение 5.9. Для любого автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}$ и любого начального состояния $\mathbf{q}_0 \in K^n$ множество $S^{(1)}_{fxd}(M_2, \mathbf{q}_0)$ непусто тогда и только тогда, когда имеет решения уравнение

$$(G^{-1} - E)\mathbf{x} = A\mathbf{q}_0\mathbf{q}_0^T B + C\mathbf{q}_0 + \mathbf{d}. \tag{5.78}$$

Из утверждения 5.9 вытекает, что истинны следующие два следствия.

Следствие 5.12. Если $G^{-1} - E \in \mathsf{M}_n^{inv}$, то для автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}$ при любом начальном состоянии $\mathbf{q}_0 \in K^n$:

1) $|S^{(i)}_{fxd}(M_2, \mathbf{q}_0)| = 1$ $(i \in \mathbf{N})$;

2) $S_{fxd}(M_2, \mathbf{q}_0)$ – бесконечное множество.

Следствие 5.13. Если $E = G^{-1}$, то для автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}$

$$S^{(1)}_{fxd}(M_2, \mathbf{q}_0) = K^n$$

при любом таком начальном состоянии $\mathbf{q}_0 \in K^n$, что

$$A\mathbf{q}_0\mathbf{q}_0^T B + C\mathbf{q}_0 + \mathbf{d} = \mathbf{0}.$$

Из полученных результатов вытекает, что при использовании автомата $M \in \widetilde{\mathcal{A}}_{n,1}^{inv} \cup \widetilde{\mathcal{A}}_{n,2}^{inv}$. в качестве математической модели поточного шифра:

1) для автомата $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ матрицу $F \in \mathsf{M}_n^{inv} \backslash \{I\}$ целесообразно выбирать так, что либо

$$I - F \in \mathsf{M}_n^{inv},$$

либо

$$I - F \in \mathsf{M}_n^{non-inv} \backslash \mathcal{M}_n^{inv},$$

но мощность множества решений уравнения

$$(I - F)\mathbf{x} = \mathbf{0}$$

достаточно мала по сравнению с числом $|K^n|$.

2) для автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}$ матрицы $G, E \in \mathsf{M}_n^{inv}$ целесообразно выбирать так, что

$$E \neq G^{-1}$$

и, кроме того, либо

$$G^{-1} - E \in \mathsf{M}_n^{inv},$$

либо

$$G^{-1} - E \in \mathsf{M}_n^{non-inv},$$

но мощность множества решений уравнения

$$(G^{-1} - E)\mathbf{x} = \mathbf{0}$$

достаточно мала по сравнению с числом $|K^n|$.

Множества неподвижных точек автомата $M \in \widetilde{\mathcal{A}}_{n,3} \cup \widetilde{\mathcal{A}}_{n,4}$ исследуются аналогичным образом.

5.6. Вариация поведения исследуемых автоматов.

Анализ вариации автоматных отображений при вариации начального состояния и/или параметров, с теоретической точки зрения характеризует соответствующую вариацию поведения автомата.

С прикладной точки зрения значение этой задачи состоит в следующем.

При использовании обратимого автомата в качестве математической модели поточного шифра указанная вариация дает возможность охарактеризовать, какую дополнительную информацию о секретном ключе может получить криптоаналитиком, осуществляя «небольшую» вариацию начального состояния и/или параметров.

Таким образом, решение рассматриваемой задачи представляет собой разработку основ аналога дифференциального анализа для поточных шифров.

5.6.1. Вариация поведения автомата $M \in \widetilde{\mathcal{A}}_{n,1} \cup \widetilde{\mathcal{A}}_{n,2}$.

Охарактеризуем вариацию автоматного отображения, реализуемого автоматом $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ при переходе от начального состояния $\mathbf{q}_0 \in K^n$ к начальному состоянию $\widetilde{\mathbf{q}_0} \in K^n$.

Подставив $\widetilde{\mathbf{q}_0}$ в (5.12), получим

$$\begin{cases} \widetilde{\mathbf{q}}_{t+1} = A\widetilde{\mathbf{q}_t}\widetilde{\mathbf{q}_{tt}}^T\mathbf{b} + C\widetilde{\mathbf{q}_t} + \mathbf{d} + E\mathbf{x}_{t+1} \\ \widetilde{\mathbf{y}}_{t+1} = G\widetilde{\mathbf{q}_t} + F\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+). \tag{5.79}$$

Вычитая из уравнений системы (5.79) соответствующие уравнения системы (5.12), получим

$$\begin{cases} \Delta\mathbf{q}_{t+1} = A(\mathbf{q}_t(\Delta\mathbf{q}_t)^T + (\Delta\mathbf{q}_t)\mathbf{q}_t^T + (\Delta\mathbf{q}_t)(\Delta\mathbf{q}_t)^T)\mathbf{b} + C\Delta\mathbf{q}_t \\ \Delta\mathbf{y}_{t+1} = G\Delta\mathbf{q}_t \end{cases}, \tag{5.80}$$

где

$$\Delta\mathbf{q}_t = \widetilde{\mathbf{q}_t} - \mathbf{q}_t$$

и

$$\Delta\mathbf{y}_{t+1} = \widetilde{\mathbf{y}}_{t+1} - \mathbf{y}_{t+1}$$

для всех $t \in \mathbf{Z}_+$.

Ясно, что образом отображения (5.80) является множество

$$\{\mathbf{0}^k | k \in \mathbf{N}\}$$

тогда и только тогда, когда $\widetilde{\mathbf{q}_0} \in S_{\mathbf{q}_0}(M_1)$.

Обозначим через $\mathbf{U}_{M_1,\mathbf{q}_0,\widetilde{\mathbf{q}_0}}(k)$ $(k \in \mathbf{N})$ множество всех входных слов $\mathbf{u} \in (K^n)^k$, которые отображением (5.80) переводятся в слова, не принадлежащие множеству $\{\mathbf{0}^k | k \in \mathbf{N}\}$. Тогда

$$\mu_{M_1,\mathbf{q}_0,\widetilde{\mathbf{q}_0}}(k) = \frac{|\mathbf{U}_{M_1,\mathbf{q}_0,\widetilde{\mathbf{q}_0}}(k)|}{|K^n|^k} \tag{5.81}$$

характеризует различимость отображений, реализуемых инициальными автоматами $(M_1, \mathbf{q}_0)$ и $(M_1, \widetilde{\mathbf{q}_0})$, на входных словах длины k.

Охарактеризуем вариацию автоматного отображения, реализуемого инициальным автоматом $(M_1, \mathbf{q}_0)$ $(M_1 \in \widetilde{\mathcal{A}}_{n,1}, \mathbf{q}_0 \in K^n)$ при переходе от параметров $A, \mathbf{b}, C, \mathbf{d}, E, F, G$ к параметрам $\widetilde{A}, \widetilde{\mathbf{b}}, \widetilde{C}, \widetilde{\mathbf{d}}, \widetilde{E}, \widetilde{F}, \widetilde{G}$.

Подставив эти значения параметров в уравнения системы (5.12), получим

$$\begin{cases} \widetilde{\mathbf{q}}_{t+1} = \widetilde{A}\widetilde{\mathbf{q}}_t\widetilde{\mathbf{q}}_t^T\widetilde{\mathbf{b}} + \widetilde{C}\widetilde{\mathbf{q}}_t + \widetilde{\mathbf{d}} + \widetilde{E}\mathbf{x}_{t+1} \\ \widetilde{\mathbf{y}}_{t+1} = \widetilde{G}\widetilde{\mathbf{q}}_t + \widetilde{F}\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+). \tag{5.82}$$

Вычитая из уравнений системы (5.82) соответствующие уравнения системы (5.12), получим, что

$$\begin{cases} \Delta\mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^T\Delta\mathbf{b} + A\mathbf{q}_t(\Delta\mathbf{q}_t)^T\mathbf{b} + \\ \quad + A\mathbf{q}_t(\Delta\mathbf{q}_t)^T\Delta\mathbf{b} + A(\Delta\mathbf{q}_t)\mathbf{q}_t^T\mathbf{b} + \\ \quad + A(\Delta\mathbf{q}_t)\mathbf{q}_t^T\Delta\mathbf{b} + A(\Delta\mathbf{q}_t)(\Delta\mathbf{q}_t)^T\mathbf{b} + \\ \quad + A(\Delta\mathbf{q}_t)(\Delta\mathbf{q}_t)^T\Delta\mathbf{b} + (\Delta A)\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + \\ \quad + (\Delta A)\mathbf{q}_t\mathbf{q}_t^T\Delta\mathbf{b} + (\Delta A)\mathbf{q}_t(\Delta\mathbf{q}_t)^T\mathbf{b} + \\ \quad + (\Delta A)\mathbf{q}_t(\Delta\mathbf{q}_t)^T\Delta\mathbf{b} + (\Delta A)(\Delta\mathbf{q}_t)\mathbf{q}_t^T\mathbf{b} + \\ \quad + (\Delta A)(\Delta\mathbf{q}_t)\mathbf{q}_t^T\Delta\mathbf{b} + (\Delta A)(\Delta\mathbf{q}_t)(\Delta\mathbf{q}_t)^T\mathbf{b} + \\ \quad + (\Delta A)(\Delta\mathbf{q}_t)(\Delta\mathbf{q}_t)^T\Delta\mathbf{b} + C\Delta\mathbf{q}_t + (\Delta C)\mathbf{q}_t + \\ \quad + (\Delta C)\Delta\mathbf{q}_t + \Delta\mathbf{d} + (\Delta E)\mathbf{x}_{t+1} \\ \Delta\mathbf{y}_{t+1} = G\Delta\mathbf{q}_t + (\Delta G)\mathbf{q}_t + (\Delta G)\Delta\mathbf{q}_t + (\Delta F)\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{N}), \tag{5.83}$$

где

$$\Delta\mathbf{q}_t = \widetilde{\mathbf{q}}_t - \mathbf{q}_t \ (t \in \mathbf{N}),$$

$$\Delta u = \widetilde{u} - u \ (u \in \{A, \mathbf{b}, C, \mathbf{d}, E, F, G\}).$$

На основе анализа (5.83) по аналогии с (5.81) может быть определена мера, характеризующая различимость автоматных отображений при вариации параметров $A, \mathbf{b}, C, \mathbf{d}, E, F, G$.

Осуществляя аналогичные построения, заключаем, что вариация автоматного отображения, реализуемого автоматом $M_2 \in \widetilde{\mathcal{A}}_{n,2}$ при переходе от начального состояния $\mathbf{q}_0 \in K^n$ к начальному состоянию $\widetilde{\mathbf{q}}_0 \in K^n$ характеризуется уравнениями

$$\begin{cases} \Delta\mathbf{q}_{t+1} = A(\mathbf{q}_t(\Delta\mathbf{q}_t)^T + (\Delta\mathbf{q}_t)\mathbf{q}_t^T + (\Delta\mathbf{q}_t)(\Delta\mathbf{q}_t)^T)\mathbf{b} + C\Delta\mathbf{q}_t \\ \Delta\mathbf{y}_{t+1} = G\Delta\mathbf{q}_{t+1} \end{cases}, \quad (5.84)$$

где

$$\Delta\mathbf{q}_t = \widetilde{\mathbf{q}}_t - \mathbf{q}_t,$$

$$\Delta\mathbf{y}_{t+1} = \widetilde{\mathbf{y}}_{t+1} - \mathbf{y}_{t+1}$$

для всех $t \in \mathbf{Z}_+$, а вариация автоматного отображения, реализуемого инициальным автоматом $(M_2, \mathbf{q}_0)$ $(M_2 \in \widetilde{\mathcal{A}}_{n,2}, \mathbf{q}_0 \in K^n)$ при переходе от параметров $A, \mathbf{b}, C, \mathbf{d}, E, G$ к параметрам $\widetilde{A}, \widetilde{\mathbf{b}}, \widetilde{C}, \widetilde{\mathbf{d}}, \widetilde{E}, \widetilde{G}$ характеризуется уравнениями

$$\begin{cases} \Delta\mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^T\Delta\mathbf{b} + A\mathbf{q}_t(\Delta\mathbf{q}_t)^T\mathbf{b} + \\ \quad + A\mathbf{q}_t(\Delta\mathbf{q}_t)^T\Delta\mathbf{b} + A(\Delta\mathbf{q}_t)\mathbf{q}_t^T\mathbf{b} + \\ \quad + A(\Delta\mathbf{q}_t)\mathbf{q}_t^T\Delta\mathbf{b} + A(\Delta\mathbf{q}_t)(\Delta\mathbf{q}_t)^T\mathbf{b} + \\ \quad + A(\Delta\mathbf{q}_t)(\Delta\mathbf{q}_t)^T\Delta\mathbf{b} + (\Delta A)\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + \\ \quad + (\Delta A)\mathbf{q}_t\mathbf{q}_t^T\Delta\mathbf{b} + (\Delta A)\mathbf{q}_t(\Delta\mathbf{q}_t)^T\mathbf{b} + \\ \quad + (\Delta A)\mathbf{q}_t(\Delta\mathbf{q}_t)^T\Delta\mathbf{b} + (\Delta A)(\Delta\mathbf{q}_t)\mathbf{q}_t^T\mathbf{b} + \\ \quad + (\Delta A)(\Delta\mathbf{q}_t)\mathbf{q}_t^T\Delta\mathbf{b} + (\Delta A)(\Delta\mathbf{q}_t)(\Delta\mathbf{q}_t)^T\mathbf{b} + \\ \quad + (\Delta A)(\Delta\mathbf{q}_t)(\Delta\mathbf{q}_t)^T\Delta\mathbf{b} + C\Delta\mathbf{q}_t + (\Delta C)\mathbf{q}_t + \\ \quad + (\Delta C)\Delta\mathbf{q}_t + \Delta\mathbf{d} + (\Delta E)\mathbf{x}_{t+1} \\ \Delta\mathbf{y}_{t+1} = G\Delta\mathbf{q}_{t+1} + (\Delta G)\mathbf{q}_{t+1} + (\Delta G)\Delta\mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \quad (5.85)$$

где

$$\Delta\mathbf{q}_t = \widetilde{\mathbf{q}}_t - \mathbf{q}_t \ (t \in \mathbf{Z}_+),$$

$$\Delta u = \widetilde{u} - u \ (u \in \{A, \mathbf{b}, C, \mathbf{d}, E, G\}).$$

На основе анализа (5.84) и (5.85) может быть определена мера, характеризующая различимость автоматных отображений при вариации, соответственно, начального состояния или параметров автомата $M_2 \in \widetilde{\mathcal{A}}_{n,2}$.

5.6.2. Вариация поведения автомата $M \in \widetilde{\mathcal{A}}_{n,3} \cup \widetilde{\mathcal{A}}_{n,4}$.

Охарактеризуем вариацию автоматного отображения, реализуемого автоматом $M_3 \in \widetilde{\mathcal{A}}_{n,3}$ при переходе от начального состояния $\mathbf{q}_0 \in K^n$ к начальному состоянию $\widetilde{\mathbf{q}}_0 \in K^n$.

Подставив $\widetilde{\mathbf{q}}_0$ в (5.14), получим

$$\begin{cases} \widetilde{q}_{t+1}^{(i)} = \widetilde{\mathbf{q}}_t^T A_i \widetilde{\mathbf{q}}_t + \mathbf{c}_i \widetilde{\mathbf{q}}_t + d_i + \alpha_i e_i x_{t+1}^{(i)} \ (i \in \mathbf{N}_n) \\ \widetilde{y}_{t+1}^{(i)} = g_i \widetilde{q}_t^{(i)} + f_i x_{t+1}^{(i)} \ (i \in \mathbf{N}_r) \end{cases} \quad (t \in \mathbf{Z}_+), \qquad (5.86)$$

где

$$\alpha_i = \begin{cases} 1, & \text{если } i \in \mathbf{N}_r \\ 0, & \text{если } i \in \mathbf{N}_n \backslash \mathbf{N}_r \end{cases}.$$

Вычитая из уравнений системы (5.86) соответствующие уравнения системы (5.14), получим, что

$$\begin{cases} \Delta q_{t+1}^{(i)} = (\mathbf{q}_t)^T A_i \Delta \mathbf{q}_t + (\Delta \mathbf{q}_t)^T A_i \mathbf{q}_t + \\ \qquad + (\Delta \mathbf{q}_t)^T A_i \Delta \mathbf{q}_t + \mathbf{c}_i \Delta \mathbf{q}_t \ (i \in \mathbf{N}_n) \\ \Delta y_{t+1}^{(i)} = g_i \Delta q_t^{(i)} \ (i \in \mathbf{N}_r) \end{cases} \quad (t \in \mathbf{Z}_+), \qquad (5.87)$$

где

$$\Delta \mathbf{q}_t = \widetilde{\mathbf{q}}_t - \mathbf{q}_t,$$

$$\Delta q_t^{(i)} = \widetilde{q}_t^{(i)} - q_t^{(i)} \ (i \in \mathbf{N}_n)$$

и

$$\Delta y_t^{(i)} = \widetilde{y}_t^{(i)} - y_t^{(i)} \ (i \in \mathbf{N}_r)$$

для всех $t \in \mathbf{Z}_+$.

Охарактеризуем вариацию автоматного отображения, реализуемого автоматом $M_3 \in \widetilde{\mathcal{A}}_{n,3}$ при переходе от параметров $A_i, \mathbf{c}_i, d_i, e_i$ $(i \in \mathbf{N}_n)$ и g_i, f_i $(i \in \mathbf{N}_r)$ к параметрам $\widetilde{A}_i, \widetilde{\mathbf{c}}_i, \widetilde{d}_i, \widetilde{e}_i$ $(i \in \mathbf{N}_n)$ и $\widetilde{g}_i, \widetilde{f}_i$ $(i \in \mathbf{N}_r)$.

Подставив эти значения параметров в уравнения системы (5.14), получим

$$\begin{cases} \widetilde{q}_1^{(i)} = \mathbf{q}_0^T \widetilde{A}_i \mathbf{q}_0 + \widetilde{\mathbf{c}}_i \mathbf{q}_0 + \widetilde{d}_i + \alpha_i \widetilde{e}_i x_{t+1}^{(i)} \ (i \in \mathbf{N}_n) \\ \widetilde{y}_{t+1}^{(i)} = \widetilde{g}_i q_t^{(i)} + \widetilde{f}_i x_{t+1}^{(i)} \ (i \in \mathbf{N}_r) \end{cases}. \qquad (5.88)$$

Вычитая из уравнений системы (5.88) соответствующие уравнения системы (5.14), получим, что

$$\begin{cases} \Delta q_{t+1}^{(i)} = \mathbf{q}_t^T A_i \Delta\mathbf{q}_t + \mathbf{q}_t^T(\Delta A_i)\mathbf{q}_t + \\ \quad +\mathbf{q}_t^T(\Delta A_i)\Delta\mathbf{q}_t + (\Delta\mathbf{q}_t)^T A_i\mathbf{q}_t + \\ \quad +(\Delta\mathbf{q}_t)^T A_i\Delta\mathbf{q}_t + (\Delta\mathbf{q}_t)^T(\Delta A_i)\mathbf{q}_t + \\ \quad +(\Delta\mathbf{q}_t)^T(\Delta A_i)\Delta\mathbf{q}_t + \mathbf{c}_i\Delta\mathbf{q}_t + (\Delta\mathbf{c}_i)\mathbf{q}_t + \qquad (t \in \mathbf{N}), \\ \quad +(\Delta\mathbf{c}_i)\Delta\mathbf{q}_t + \Delta d_i + \alpha_i(\Delta e_i)x_{t+1}^{(i)} \ (i \in \mathbf{N}_n) \\ \Delta y_{t+1}^{(i)} = g_i\Delta q_t^{(i)} + (\Delta g_i)q_t^{(i)} + \\ \quad +(\Delta g_i)\Delta q_t^{(i)} + (\Delta f_i)x_{t+1}^{(i)} \ (i \in \mathbf{N}_r) \end{cases} \tag{5.89}$$

где

$$\alpha_i = \begin{cases} 1, & \text{если } i \in \mathbf{N}_r \\ 0, & \text{если } i \in \mathbf{N}_n \backslash \mathbf{N}_r \end{cases},$$

$$\Delta\mathbf{q}_t = \widetilde{\mathbf{q}}_t - \mathbf{q}_t \ t \in \mathbf{Z}_+,$$

$$\Delta q_t^{(i)} = \widetilde{q}_t^{(i)} - q_t^{(i)} \ (i \in \mathbf{N}_n, t \in \mathbf{Z}_+),$$

$$\Delta y_t^{(i)} = \widetilde{y}_t^{(i)} - y_t^{(i)} \ (i \in \mathbf{N}_r, t \in \mathbf{Z}_+)$$

$$\Delta u = \widetilde{u} - u \ (u \in \{A_i, \mathbf{c}_i, d_i, e_i | i \in \mathbf{N}_n\} \cup \{g_i, f_i | i \in \mathbf{N}_r\}),$$

На основе анализа (5.87) и (5.89) может быть определена мера, характеризующая различимость автоматных отображений при вариации, соответственно, начального состояния или параметров автомата $M_3 \in \widetilde{\mathcal{A}}_{n,3}$.

Осуществляя аналогичные построения, заключаем, что вариация автоматного отображения, реализуемого автоматом $M_4 \in \widetilde{\mathcal{A}}_{n,4}$ при переходе от начального состояния $\mathbf{q}_0 \in K^n$ к начальному состоянию $\widetilde{\mathbf{q}}_0 \in K^n$ характеризуется уравнениями

$$\begin{cases} \Delta q_{t+1}^{(i)} = (\mathbf{q}_t)^T A_i\Delta\mathbf{q}_t + (\Delta\mathbf{q}_t)^T A_i\mathbf{q}_t + \\ \qquad +(\Delta\mathbf{q}_t)^T A_i\Delta\mathbf{q}_t + \mathbf{c}_i\Delta\mathbf{q}_t \ (i \in \mathbf{N}_n) \quad (t \in \mathbf{Z}_+), \\ \Delta y_{t+1}^{(i)} = g_i\Delta q_{t+1}^{(i)} \ (i \in \mathbf{N}_r) \end{cases} \tag{5.90}$$

где

$$\Delta\mathbf{q}_t = \widetilde{\mathbf{q}}_t - \mathbf{q}_t \ (t \in \mathbf{Z}_+),$$

$$\Delta q_t^{(i)} = \widetilde{q}_t^{(i)} - q_t^{(i)} \ (i \in \mathbf{N}_n, t \in \mathbf{Z}_+),$$

$$\Delta y_t^{(i)} = \widetilde{y}_t^{(i)} - y_t^{(i)} \ (i \in \mathbf{N}_r, t \in \mathbf{Z}_+),$$

а вариация автоматного отображения, реализуемого инициальным автоматом $(M_4, \mathbf{q}_0)$ $(M_4 \in \widetilde{\mathcal{A}}_{n,2}, \mathbf{q}_0 \in K^n)$ при переходе от параметров $A_i, \mathbf{c}_i, d_i, e_i$ $(i \in \mathbf{N}_n)$ и g_i $(i \in \mathbf{N}_r)$ к параметрам $\widetilde{A}_i, \widetilde{\mathbf{c}}_i, \widetilde{d}_i, \widetilde{e}_i$ $(i \in \mathbf{N}_n)$ и $\widetilde{g}_i$ $(i \in \mathbf{N}_r)$ характеризуется уравнениями

$$\begin{cases} \Delta q_{t+1}^{(i)} = \mathbf{q}_t^T A_i \Delta\mathbf{q}_t + \mathbf{q}_t^T (\Delta A_i)\mathbf{q}_t + \\ \quad + \mathbf{q}_t^T (\Delta A_i)\Delta\mathbf{q}_t + (\Delta\mathbf{q}_t)^T A_i \mathbf{q}_t + \\ \quad + (\Delta\mathbf{q}_t)^T A_i \Delta\mathbf{q}_t + (\Delta\mathbf{q}_t)^T (\Delta A_i)\mathbf{q}_t + \\ \quad + (\Delta\mathbf{q}_t)^T (\Delta A_i)\Delta\mathbf{q}_t + \mathbf{c}_i \Delta\mathbf{q}_t + (\Delta\mathbf{c}_i)\mathbf{q}_t + \\ \quad + (\Delta\mathbf{c}_i)\Delta\mathbf{q}_t + \Delta d_i + \alpha_i (\Delta e_i) x_{t+1}^{(i)} \ (i \in \mathbf{N}_n) \\ \Delta y_{t+1}^{(i)} = g_i \Delta q_{t+1}^{(i)} + (\Delta g_i) q_{t+1}^{(i)} + (\Delta g_i)\Delta q_{t+1}^{(i)} \ (i \in \mathbf{N}_r) \end{cases} \quad (t \in \mathbf{N}), \quad (5.91)$$

где

$$\alpha_i = \begin{cases} 1, & \text{если } i \in \mathbf{N}_r \\ 0, & \text{если } i \in \mathbf{N}_n \backslash \mathbf{N}_r \end{cases},$$

$$\Delta\mathbf{q}_t = \widetilde{\mathbf{q}}_t - \mathbf{q}_t \ (t \in \mathbf{Z}_+),$$

$$\Delta q_t^{(i)} = \widetilde{q}_t^{(i)} - q_t^{(i)} \ (i \in \mathbf{N}_n, t \in \mathbf{Z}_+),$$

$$\Delta y_t^{(i)} = \widetilde{y}_t^{(i)} - y_t^{(i)} \ (i \in \mathbf{N}_r, t \in \mathbf{Z}_+),$$

$$\Delta u = \widetilde{u} - u \ (u \in \{A_i, \mathbf{c}_i, d_i, e_i | i \in \mathbf{N}_n\} \cup \{g_i | i \in \mathbf{N}_r\}).$$

На основе анализа (5.90) и (5.91) может быть определена мера, характеризующая различимость автоматных отображений при вариации, соответственно, начального состояния или параметров автомата $M_4 \in \widetilde{\mathcal{A}}_{n,4}$.

Пример 5.5. Рассмотрим автоматы, построенные в примере 5.1.

1. Для автомата $M_R \in \widetilde{\mathcal{A}}_{3,4}$ вариация отображения при переходе от начального состояния $\mathbf{q}_0 \in K^3$ к начальному состоянию $\widetilde{\mathbf{q}}_0 \in K^3$ характеризуется уравнениями

$$\begin{cases} \Delta q_{t+1}^{(1)} = \Delta q_t^{(1)} - h\Delta q_t^{(2)} - h\Delta q_t^{(3)} \\ \Delta q_{t+1}^{(2)} = h\Delta q_t^{(1)} + (ah+1)\Delta q_t^{(2)} \\ \Delta q_{t+1}^{(3)} = (1 + h(q_t^{(1)} - r))\Delta q_t^{(3)} + h(q_t^{(3)} + \Delta q_t^{(3)})\Delta q_t^{(1)} \\ \Delta y_{t+1} = \Delta q_{t+1}^{(1)} \end{cases} \qquad (t \in \mathbf{Z}_+).$$

2. Для автомата $M_S \in \widetilde{\mathcal{A}}_{3,4}$ вариация отображения при переходе от начального состояния $\mathbf{q}_0 \in K^3$ к начальному состоянию $\widetilde{\mathbf{q}}_0 \in K^3$ характеризуется уравнениями

$$\begin{cases} \Delta q_{t+1}^{(1)} = \Delta q_t^{(1)} + h\Delta q_t^{(2)} \\ \Delta q_{t+1}^{(2)} = (1 + hq_t^{(3)})\Delta q_t^{(2)} + h(q_t^{(2)} + \Delta q_t^{(2)})\Delta q_t^{(3)} - h\Delta q_t^{(1)} \\ \Delta q_{t+1}^{(3)} = \Delta q_t^{(3)} - h(2 + \Delta q_t^{(2)})\Delta q_t^{(2)} \\ \Delta y_{t+1} = \Delta q_{t+1}^{(1)} \end{cases} \qquad (t \in \mathbf{Z}_+).$$

3. Для автомата $M_L \in \widetilde{\mathcal{A}}_{3,4}$ вариация отображения при переходе от начального состояния $\mathbf{q}_0 \in K^3$ к начальному состоянию $\widetilde{\mathbf{q}}_0 \in K^3$ характеризуется уравнениями

$$\begin{cases} \Delta q_{t+1}^{(1)} = (1 - ha_1)\Delta q_t^{(1)} + ha_1\Delta q_t^{(2)} \\ \Delta q_{t+1}^{(2)} = (1-h)\Delta q_t^{(2)} + h(a_2 - q_t^{(3)})\Delta q_t^{(1)} - \\ \qquad -h(q_t^{(1)} + \Delta q_t^{(1)})\Delta q_t^{(3)} \\ \Delta q_{t+1}^{(3)} = (1 - ha_3)\Delta q_t^{(3)} + h((q_t^{(1)} + \Delta q_t^{(1)})\Delta q_t^{(2)} + q_t^{(2)}\Delta q_t^{(1)}) \\ \Delta y_{t+1} = \Delta q_{t+1}^{(2)} \end{cases} \qquad (t \in \mathbf{Z}_+).$$

4. Для автомата $M_H \in \widetilde{\mathcal{A}}_{2,4}$ вариация отображения при переходе от параметров a, b, c к параметрам $\widetilde{a}, \widetilde{b}, \widetilde{c}$ характеризуется уравнениями

$$\begin{cases} \Delta q_{t+2} = (b + \Delta b)\Delta q_t + q_t\Delta b - a(2q_{t+1} + \Delta q_{t+1})\Delta q_{t+1} - \\ \qquad -\Delta a(q_{t+1}^2 + (2q_{t+1} + \Delta q_{t+1})\Delta q_{t+1}) + \Delta c x_{t+1} \\ \Delta y_{t+1} = \Delta q_{t+2} \end{cases} \qquad (t \in \mathbf{Z}_+).$$

5.7. Анализ линейных автоматов.

Известно, что исследование линейных моделей дает возможность охарактеризовать нижнюю границу сложности решения задач анализа и синтеза. Кроме того, для линейных моделей могут быть получены результаты, являющиеся более сильными, чем аналогичные результаты для нелинейных моделей.

Охарактеризуем кратко линейные автоматы над кольцом $\mathcal{K} = (K, +, \cdot)$.

5.7.1. Линейные автоматы с лагом 1.

Обозначим через $\widetilde{\mathcal{A}}_{n,5}$ множество автоматов Мили

$$M_5 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t + B\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C\mathbf{q}_t + D\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.92}$$

а через $\widetilde{\mathcal{A}}_{n,6}$ – множество автоматов Мура

$$M_6 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t + B\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C\mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.93}$$

где $A, B, C, D \in \mathsf{M}_n$ $(n \in \mathbf{N})$, а $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in (\mathbf{Z}_m)^n$ – вектор-столбцы, представляющие, соответственно, состояние автомата, входной и выходной символ в момент t.

Замечание 5.1. Так как $\widetilde{\mathcal{A}}_{n,5} \subset \widetilde{\mathcal{A}}_{n,1}$ и $\widetilde{\mathcal{A}}_{n,6} \subset \widetilde{\mathcal{A}}_{n,2}$, то результаты, установленные в пп.5.1-5.6 для автоматов, принадлежащих множествам $\widetilde{\mathcal{A}}_{n,1}$ и $\widetilde{\mathcal{A}}_{n,2}$, автоматически переносятся на рассматриваемый случай, в предположении, что все объекты, не входящие в (5.92) и (5.93) – нулевые.

Это дополнительное условие дает возможность усилить ряд установленных в пп.5.1-5.6 результатов для автоматов, принадлежащих множествам $\widetilde{\mathcal{A}}_{n,5}$ и $\widetilde{\mathcal{A}}_{n,6}$.

Из теорем 5.1 и 5.2 и формул (5.6) и (5.11) вытекает, что истинны следующие два утверждения.

Утверждение 5.10. Автомат $M_5 \in \widetilde{\mathcal{A}}_{n,5}$ является обратимым автоматом тогда и только тогда, когда $D \in \mathsf{M}_n^{inv}$. При этом обратный автомат имеет вид

$$M_5^{-1}:\begin{cases}\mathbf{q}_{t+1}=A_1\mathbf{q}_t+B_1\mathbf{x}_{t+1}\\ \mathbf{y}_{t+1}=C_1\mathbf{q}_t+D_1\mathbf{x}_{t+1}\end{cases}\quad(t\in\mathbf{Z}_+),\tag{5.94}$$

где

$$\begin{cases}A_1=A-BD^{-1}C\\ B_1=BD^{-1}\\ C_1=-D^{-1}C\\ D_1=D^{-1}\end{cases}.$$

Утверждение 5.11. Автомат $M_6\in\widetilde{\mathcal{A}}_{n,6}$ является обратимым автоматом тогда и только тогда, когда $B,C\in\mathsf{M}_n^{inv}$. При этом обратный автомат имеет вид

$$M_6^{-1}:\begin{cases}\mathbf{q}_{t+1}=B_1\mathbf{x}_{t+1}\\ \mathbf{y}_{t+1}=C_1\mathbf{q}_t+D_1+\mathbf{x}_{t+1}\end{cases}\quad(t\in\mathbf{Z}_+),\tag{5.95}$$

где

$$\begin{cases}B_1=C^{-1}\\ C_1=-A\\ D_1=B^{-1}C^{-1}\end{cases}.$$

Обозначим через $\widetilde{\mathcal{A}}_{n,i}^{inv}$ $(i=5,6)$ множество всех обратимых автоматов $M_i\in\widetilde{\mathcal{A}}_{n,i}$.

Из утверждений 5.10 и 5.11, а также из формул (5.20), (5.21) и (5.24) вытекает, что если $\mathcal{K}=\mathcal{Z}_m$ ($m=\prod\limits_{i=1}^{h}p_i^{k_i}$, где p_i – попарно различные простые числа), то

$$|\widetilde{\mathcal{A}}_{n,i}|=|\mathsf{M}_n|^{9-i}\ (i=5,6),\tag{5.96}$$

$$|\widetilde{\mathcal{A}}_{n,r}^{inv}|=|\widetilde{\mathcal{A}}_{n,r}|\left(\prod_{i=1}^{h}\prod_{j=1}^{n}(1-p_i^{-j})\right)^{r-4}\quad(r=5,6),\tag{5.97}$$

$$\mathsf{P}_{\widetilde{\mathcal{A}}_{n,r}^{inv}} = \left(\prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}) \right)^{r-4} \quad (r = 5, 6). \tag{5.98}$$

Следующие утверждения характеризуют нетривиальные подмножества множеств $\widetilde{\mathcal{A}}_{n,i}^{inv}$ $(i = 5, 6)$.

Утверждение 5.12. Граф переходов автомата $M_i \in \widetilde{\mathcal{A}}_{n,i}$ $(i = 5, 6)$ – полный граф с петлями тогда и только тогда, когда $B \in \mathsf{M}_n^{inv}$.

Утверждение 5.13. Автомат $M_i \in \widetilde{\mathcal{A}}_{n,i}$ $(i = 5, 6)$ – перестановочный автомат тогда и только тогда, когда $A \in \mathsf{M}_n^{inv}$.

Утверждение 5.14. Если $C \in \mathsf{M}_n^{inv}$, то $M_5 \in \widetilde{\mathcal{A}}_{n,5}$ – приведенный автомат, степень различимости которого равна 1.

Утверждение 5.15. Если $A, C \in \mathsf{M}_n^{inv}$, то $M_6 \in \widetilde{\mathcal{A}}_{n,6}$ – приведенный автомат, степень различимости которого равна 1.

Утверждение 5.16. Если $A, C \in \mathsf{M}_n^{non-inv}$, и система уравнений

$$\begin{cases} A\mathbf{u} = \mathbf{0} \\ C\mathbf{u} = \mathbf{0} \end{cases}$$

имеет ненулевое решение, то в автомате $M_5 \in \widetilde{\mathcal{A}}_{n,5}$ существуют состояния-близнецы.

Утверждение 5.17. Если $A \in \mathsf{M}_n^{non-inv}$, то в автомате $M_6 \in \widetilde{\mathcal{A}}_{n,6}$ существуют состояния-близнецы.

Доказательство утверждений 5.12-5.19 аналогично доказательству соответствующих утверждений из [52].

Исходя из утверждений 5.10-5.19, с использованием схемы 5.1, могут быть получены метрические соотношения, характеризующие соответствующие подмножества линейных автоматов.

Можно показать, что эквивалентность автоматов, принадлежащих множеству $\widetilde{\mathcal{A}}_{n,i}$ $(i = 5, 6)$ характеризуется следующим образом.

Теорема 5.8. Автоматы $M_5, M_5' \in \widetilde{\mathcal{A}}_{n,5}$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

1) $D = D'$;

2) для любого состояния $\mathbf{q}_0 \in (\mathbf{Z}_m)^n$ автомата M_5 существует такое состояние $\mathbf{q}_0^{'} \in (\mathbf{Z}_m)^n$ автомата $M_5^{'}$ и, наоборот, для любого состояния $\mathbf{q}_0^{'} \in (\mathbf{Z}_m)^n$ автомата $M_5^{'}$ существует такое состояние $\mathbf{q}_0 \in (\mathbf{Z}_m)^n$ автомата M_5, что:

а) $C'\mathbf{q}_0^{'} - C\mathbf{q}_0 = \mathbf{0}$;

б) $C'(A')^j\mathbf{q}_0^{'} - CA^j\mathbf{q}_0 = \mathbf{0}$ $(j = 1, \ldots, 2m^n - 2)$;

3) $C'(A')^jB' - CA^jB = O$ $(j = 1, \ldots, 2m^n - 3)$, где $O \in \mathsf{M}_n$ – нулевая матрица;

4) $C'B' - CB = O$.

Теорема 5.9. Автоматы $M_6, M_6^{'} \in \widetilde{\mathcal{A}}_{n,6}$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

1) $C'B' - CB = O$;

2) для любого состояния $\mathbf{q}_0 \in (\mathbf{Z}_m)^n$ автомата M_6 существует такое состояние $\mathbf{q}_0^{'} \in (\mathbf{Z}_m)^n$ автомата $M_6^{'}$ и, наоборот, для любого состояния $\mathbf{q}_0^{'} \in (\mathbf{Z}_m)^n$ автомата $M_6^{'}$ существует такое состояние $\mathbf{q}_0 \in (\mathbf{Z}_m)^n$ автомата M_5, что

$$C'(A')^j\mathbf{q}_0^{'} - CA^j\mathbf{q}_0 = \mathbf{0} \ (j = 1, \ldots, 2m^n - 1);$$

3) $C'(A')^jB' - CA^jB = O$ $(j = 1, \ldots, 2m^n - 2)$.

Доказательство теорем 5.8 и 5.9 аналогично доказательству соответствующих теорем из [52].

Из теорем 5.8 и 5.9 непосредственно вытекает, что истинны следующие два следствия

Следствие 5.14. Состояния $\mathbf{q}_0, \mathbf{q}_0^{'} \in (\mathbf{Z}_m)^n$ автомата $M_5 \in \widetilde{\mathcal{A}}_{n,5}$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

1) $C(\mathbf{q}_0^{'} - \mathbf{q}_0) = \mathbf{0}$;

2) $C(A)^j(\mathbf{q}_0^{'} - \mathbf{q}_0) = \mathbf{0}$ для всех $j = 1, \ldots, m^n - 2$.

Следствие 5.15. Состояния $\mathbf{q}_0, \mathbf{q}_0^{'} \in (\mathbf{Z}_m)^n$ автомата $M_6 \in \widetilde{\mathcal{A}}_{n,6}$ эквивалентны тогда и только тогда, когда

$$C(A)^j(\mathbf{q}_0^{'} - \mathbf{q}_0) = \mathbf{0}$$

для всех $j = 1, \ldots, m^n - 2$.

Для автомата $M_i \in \widetilde{\mathcal{A}}_{n,i}$ $(i = 5, 6)$ сложность решения задач идентификации характеризуется следующим образом.

Теорема 5.10. Пусть экспериментатор полностью управляет входом и инициализацией автомата $M_5 \in \widetilde{\mathcal{A}}_{n,i}$, а также полностью наблюдает выход автомата M_5. Тогда:

1) каждая из матриц C и D идентифицируется единственным образом посредством n-кратного эксперимента высоты 1;

2) если $C \in \mathsf{M}_n^{inv}$, то идентификация каждой из матриц A и B сводится к решению n систем линейных уравнений над кольцом $\mathcal{K}$, построенных в результате n-кратного эксперимента высоты 2.

Доказательство этой теоремы аналогично доказательству теремы 5.11 из [52].

Сложность решения задачи параметрической идентификации автомата $M_5 \in \widetilde{\mathcal{A}}_{n,5}$ существенно возрастает, если $C \in \mathsf{M}_n^{non-inv}$. Это обусловлено тем, что идентификация матриц A и B сводится к решению при известных матрицах C и D системы нелинейных уравнений

$$C\left(A^i\mathbf{q}_0 + \sum_{j=1}^{i-1} A^{i-j}B\mathbf{x}_j + B\mathbf{x}_i\right) = \mathbf{y}_{i+1} - D\mathbf{x}_{i+1}, \tag{5.99}$$

где $\mathbf{q}_0 \in K^n$ и $\mathbf{x}_1 \ldots \mathbf{x}_{i+1} \in |K|^{n(i+1)}$ $(i = 1, \ldots, |K|^n - 1)$.

Для автомата $M_6 \in \widetilde{\mathcal{A}}_{n,6}$ решение задачи параметрической идентификации всегда сводится к решению относительно матриц A, B и C системы нелинейных уравнений

$$C\left(A^{i+1}\mathbf{q}_0 + \sum_{j=0}^{i-1} A^{i-j}B\mathbf{x}_{j+1} + B\mathbf{x}_{i+1}\right) = \mathbf{y}_{i+1}, \tag{5.100}$$

где $\mathbf{q}_0 \in K^n$ и $\mathbf{x}_1 \ldots \mathbf{x}_{i+1} \in |K|^{n(i+1)}$ $(i = 1, \ldots, |K|^n - 1)$.

Рассмотрим решение задачи идентификации начального состояния автомата $M_i \in \widetilde{\mathcal{A}}_{n,i}$ $(i = 5, 6)$ в предположении, что экспериментатору известны параметры модели, но он не может управлять этими параметрами.

Положив $t = 0$ во 2-м уравнении системы (5.92), получим

$$C\mathbf{q}_0 = \mathbf{y}_1 - D\mathbf{x}_1. \tag{5.101}$$

Если $C \in \mathsf{M}_n^{inv}$, то из (5.101) вытекает, что

$$\mathbf{q}_0 = C^{-1}(\mathbf{y}_1 - D\mathbf{x}_1),$$

т.е. идентификация начального состояния автомата $M_5 \in \widetilde{\mathcal{A}}_{n,5}$ сводится к решению системы линейных уравнений, полученной в результате любого простого эксперимента длины 1.

Если же $C \in \mathsf{M}_n^{non-inv}$, то решение системы линейных уравнений (5.101) дает возможность найти только множество возможных кандидатов на начальное состояние (которое может быть значительно шире класса эквивалентных состояний). Поэтому в этом случае решение задачи идентификации начального состояния автомата $M_5 \in \widetilde{\mathcal{A}}_{n,5}$ сводится к решению при известных матрицах A, B, C, D системы линейных уравнений (5.99).

Положив $t = 0$ во 2-м уравнении системы (5.93), получим

$$C\mathbf{q}_0 = \mathbf{y}_1 - D\mathbf{x}_1. \tag{5.102}$$

Если $A, C \in \mathsf{M}_n^{inv}$, то из (5.102) вытекает, что

$$\mathbf{q}_0 = A^{-1}C^{-1}(\mathbf{y}_1 - CB\mathbf{x}_1),$$

т.е. идентификация начального состояния автомата $M_6 \in \widetilde{\mathcal{A}}_{n,6}$ сводится к решению системы линейных уравнений, полученной в результате любого простого эксперимента длины 1.

Если же $A \in \mathsf{M}_n^{non-inv}$ или $C \in \mathsf{M}_n^{non-inv}$, то решение системы линейных уравнений (5.101) дает возможность найти только множество возможных кандидатов на начальное состояние (которое может быть значительно шире класса эквивалентных состояний).

Поэтому в этом случае решение задачи идентификации начального состояния автомата $M_6 \in \widetilde{\mathcal{A}}_{n,6}$ сводится к решению при известных матрицах A, B, C системы линейных уравнений (5.100).

Множество неподвижных точек, автоматных отображений, реализуемых автоматом $M_i \in \widetilde{\mathcal{A}}_{n,i}$ $(i = 5, 6)$ характеризуется следующим образом.

Теорема 5.11. Для любого автомата $M \in \widetilde{\mathcal{A}}_{n,5} \cup \widetilde{\mathcal{A}}_{n,6}$ множество $S_{fxd}^{(t+1)}(M, \mathbf{q}_0)$ $(\mathbf{q}_0 \in K^n, t \in \mathbf{Z}_+)$ состоит из всех таких входных слов $\mathbf{x}_1 \dots \mathbf{x}_{t+1} \in K^{n(t+1)}$, что:

1) если $M \in \widetilde{\mathcal{A}}_{n,5}$, то $(\mathbf{x}_1, \ldots, \mathbf{x}_{t+1})$ – решение системы уравнений

$$\begin{cases} (I-D)\mathbf{x}_1 = C\mathbf{q}_0 \\ (I-D)\mathbf{x}_{i+1} = C\left(A^i\mathbf{q}_0 + \sum\limits_{j=1}^{i-1} A^{i-j}B\mathbf{x}_j + B\mathbf{x}_i\right) \end{cases} \quad (i = 1, \ldots, t);$$

2) если $M \in \widetilde{\mathcal{A}}_{n,6}$, то $(\mathbf{x}_1, \ldots, \mathbf{x}_{t+1})$ – решение системы уравнений

$$\begin{cases} (I-CB)\mathbf{x}_1 = CA\mathbf{q}_0 \\ (I-CB)\mathbf{x}_{i+1} = CA\left(A^i\mathbf{q}_0 + \sum\limits_{j=1}^{i-1} A^{i-j}B\mathbf{x}_j + B\mathbf{x}_i\right) \end{cases} \quad (i = 1, \ldots, t).$$

Доказательство этой теоремы аналогично доказательству теремы 5.12 из [52].

Из теоремы 5.11 вытекает, что истинны следующие четыре следствия.

Следствие 5.16. Если $I - D \in \mathsf{M}_n^{inv}$ для автомата $M_5 \in \widetilde{\mathcal{A}}_{n,5}$, то для любого начального состояния $\mathbf{q}_0 \in K^n$ множество $S_{fxd}(M_5, \mathbf{q}_0)$ является бесконечным, причем $S_{fxd}^{(t+1)}(M_5, \mathbf{q}_0)$ $(t \in \mathbf{Z}_+)$ – одноэлементное множество, содержащее такое входное слово $\mathbf{x}_1 \ldots \mathbf{x}_{t+1} \in K^{n(t+1)}$, что

$$\begin{cases} \mathbf{x}_1 = (I-D)^{-1}C\mathbf{q}_0 \\ \mathbf{x}_{i+1} = (I-D)^{-1}C\left(A^i\mathbf{q}_0 + \sum\limits_{j=1}^{i-1} A^{i-j}B\mathbf{x}_j + B\mathbf{x}_i\right) \end{cases} \quad (i = 1, \ldots, t);$$

Следствие 5.17. Если $I - CB \in \mathsf{M}_n^{inv}$ для автомата $M_6 \in \widetilde{\mathcal{A}}_{n,6}$, то для любого начального состояния $\mathbf{q}_0 \in K^n$ множество $S_{fxd}(M_6, \mathbf{q}_0)$ является бесконечным, причем $S_{fxd}^{(t+1)}(M_6, \mathbf{q}_0)$ $(t \in \mathbf{Z}_+)$ – одноэлементное множество, содержащее такое входное слово $\mathbf{x}_1 \ldots \mathbf{x}_{t+1} \in K^{n(t+1)}$, что

$$\begin{cases} \mathbf{x}_1 = (I-CB)^{-1}CA\mathbf{q}_0 \\ \mathbf{x}_{i+1} = (I-CB)^{-1}CA\left(A^i\mathbf{q}_0 + \sum\limits_{j=1}^{i-1} A^{i-j}B\mathbf{x}_j + B\mathbf{x}_i\right) \end{cases} \quad (i = 1, \ldots, t).$$

Следствие 5.18. Для любого автомата $M \in \widetilde{\mathcal{A}}_{n,5} \cup \widetilde{\mathcal{A}}_{n,6}$ и любых начальных состояний $\mathbf{q}_0, \widetilde{\mathbf{q}}_0 \in K^n$, если $\mathbf{x} \in S^{(1)}_{fxd}(M, \mathbf{q}_0)$ и $\widetilde{\mathbf{x}} \in S^{(1)}_{fxd}(M, \widetilde{\mathbf{q}}_0)$, то $\mathbf{x} - \widetilde{\mathbf{x}} \in S^{(1)}_{fxd}(M, \mathbf{q}_0 - \widetilde{\mathbf{q}}_0)$.

Следствие 5.19. Для любого автомата $M \in \widetilde{\mathcal{A}}_{n,5} \cup \widetilde{\mathcal{A}}_{n,6}$ для каждого начального состояния $\mathbf{q}_0 \in K^n$ и любого входного символа $\mathbf{x} \in S^{(1)}_{fxd}(M, \mathbf{q}_0)$ истинно равенство

$$S^{(1)}_{fxd}(M, \mathbf{q}_0) = \{\mathbf{x} + \widetilde{\mathbf{x}} | \mathbf{x} \in S^{(1)}_{fxd}(M, \mathbf{0})\}.$$

Ясно, что соотношения, характеризующие вариацию поведения автоматов $M_5 \in \widetilde{\mathcal{A}}_{n,5}$ и $M_6 \in \widetilde{\mathcal{A}}_{n,6}$, могут быть получены из аналогичных соотношений для автоматов, соответственно, $M_1 \in \widetilde{\mathcal{A}}_{n,1}$ и $M_2 \in \widetilde{\mathcal{A}}_{n,2}$, если в этих соотношениях считать нулевыми все объекты, не входящие, соответственно, в (5.92) и (5.93).

Однако, ввиду простоты исследуемых моделей целесообразно рассмореть общий случай, т.е. когда вариации подвергается как начальное состояние, так и параметры.

Положим

$$\begin{cases} \widetilde{A} = A + \Delta A \\ \widetilde{B} = B + \Delta B \\ \widetilde{C} = C + \Delta C \\ \widetilde{D} = D + \Delta D \\ \widetilde{A} = A + \Delta A \\ \widetilde{\mathbf{q}}_t = \mathbf{q}_t + \Delta \mathbf{q}_t \\ \widetilde{\mathbf{x}}_t = \mathbf{x}_t + \Delta \mathbf{x}_t \\ \widetilde{\mathbf{y}}_t = \mathbf{y}_t + \Delta \mathbf{y}_t \end{cases}.$$

Вычитая из уравнений системы

$$\widetilde{M}_5 : \begin{cases} \widetilde{\mathbf{q}}_{t+1} = \widetilde{A}\widetilde{\mathbf{q}}_t + \widetilde{B}\widetilde{\mathbf{x}}_{t+1} \\ \mathbf{y}_{t+1} = \widetilde{C}\widetilde{\mathbf{q}}_t + \widetilde{D}\widetilde{\mathbf{x}}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

соответстующие уравнения системы (5.92), получим, что вариация поведения автомата $M_5 \in \widetilde{\mathcal{A}}_{n,5}$ при вариации начального состояния и параметров для всех $t \in \mathbf{Z}_+$ определяется соотношениями

$$\begin{cases} \Delta\mathbf{q}_{t+1} = A\Delta\mathbf{q}_t + B\Delta\mathbf{x}_{t+1} + \Delta A\mathbf{q}_t + \Delta B\mathbf{x}_{t+1} + \Delta A\Delta\mathbf{q}_t + \Delta B\Delta\mathbf{x}_{t+1} \\ \Delta\mathbf{y}_{t+1} = C\Delta\mathbf{q}_t + D\Delta\mathbf{x}_{t+1} + \Delta C\mathbf{q}_t + \Delta D\mathbf{x}_{t+1} + \Delta C\Delta\mathbf{q}_t + \Delta D\Delta\mathbf{x}_{t+1} \end{cases}.$$

Аналогичным образом, вычитая из уравнений системы

$$\widetilde{M}_6 : \begin{cases} \widetilde{\mathbf{q}}_{t+1} = \widetilde{A}\widetilde{\mathbf{q}}_t + \widetilde{B}\widetilde{\mathbf{x}}_{t+1} \\ \mathbf{y}_{t+1} = \widetilde{C}\widetilde{\mathbf{q}}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

соответстующие уравнения системы (5.92), получим, что вариация поведения автомата $M_5 \in \widetilde{\mathcal{A}}_{n,5}$ при вариации начального состояния и параметров для всех $t \in \mathbf{Z}_+$ определяется соотношениями

$$\begin{cases} \Delta\mathbf{q}_{t+1} = A\Delta\mathbf{q}_t + B\Delta\mathbf{x}_{t+1} + \Delta A\mathbf{q}_t + \Delta B\mathbf{x}_{t+1} + \Delta A\Delta\mathbf{q}_t + \Delta B\Delta\mathbf{x}_{t+1} \\ \Delta\mathbf{y}_{t+1} = C\Delta\mathbf{q}_{t+1} + \Delta C(\mathbf{q}_{t+1} + \Delta\mathbf{q}_{t+1}) \end{cases}.$$

5.7.2. Линейные автоматы с лагом l.

Обозначим через $\widetilde{\mathcal{A}}_{l,7}$ множество всех автоматов Мили

$$M_7 : \begin{cases} q_{t+l} = \sum\limits_{i=1}^{l} a_i q_{t+l-i} + bx_{t+1} \\ y_{t+1} = \sum\limits_{i=1}^{l} c_i q_{t+l-i} + dx_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \qquad (5.103)$$

а через $\widetilde{\mathcal{A}}_{l,8}$ множество всех автоматов Мура

$$M_8 : \begin{cases} q_{t+l} = \sum\limits_{i=1}^{l} a_i q_{t+l-i} + bx_{t+1} \\ y_{t+1} = \sum\limits_{i=1}^{l} c_i q_{t+l+1-i} \end{cases} \quad (t \in \mathbf{Z}_+), \qquad (5.104)$$

где $a_i, c_i, b, d \in K$ $(i = 1, \ldots, l)$ – параметры, $x \in K$ – входная переменная, $y \in K$ – выходная переменная, q – переменная состояния, а $\mathbf{q}_0 = (q_{l-1}, \ldots, q_1, q_0)^T$ – начальное состояние.

Перепишем (5.103) и (5.104) в матричном виде

$$M_7 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t + B\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C\mathbf{q}_t + D\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

$$M_8 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t + B\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C\mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

где

$$\mathbf{q}_t = (q_{t+l-1}, \ldots, q_{t+1}, q_t)^T \ (t \in \mathbf{Z}_+),$$

$$\mathbf{x}_{t+1} = (x_{t+l}, \underbrace{0, \ldots, 0}_{l-1})^T \ (t \in \mathbf{Z}_+),$$

$$\mathbf{y}_{t+1} = (y_{t+l}, \underbrace{0, \ldots, 0}_{l-1})^T \ (t \in \mathbf{Z}_+),$$

а $A, B, C, D \in \mathsf{M}_l$ – такие диагональные матрицы, что

$$A = \begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_l \end{pmatrix}, \quad B = \begin{pmatrix} b & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} c_1 & 0 & \ldots & 0 \\ 0 & c_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & c_l \end{pmatrix}, \quad D = \begin{pmatrix} d & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Таким образом, для автоматов $M_i \in \widetilde{\mathcal{A}}_{l,i}$ $(i = 7, 8)$ истинны все утверждения, полученные в п.5.7.1, при замене числа n числом l с учетом сужения входной и выходной полугрупп автоматов с множества $(K^n)^+$ до множества K^+.

Перечислим основные из таких утверждений.

Утверждение 5.18. Автомат $M_7 \in \widetilde{\mathcal{A}}_{l,7}$ является обратимым автоматом тогда и только тогда, когда $d \in K^{inv}$. При этом обратный автомат имеет вид

$$M_7^{-1}: \begin{cases} q_{t+l} = \sum\limits_{i=1}^{l} \alpha_i q_{t+l-i} + \beta x_{t+1} \\ y_{t+1} = \sum\limits_{i=1}^{l} \gamma_i q_{t+l-i} + \delta x_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

где

$$\begin{cases} \alpha_i = a_i - bd^{-1}c_i \ (i = 1, \ldots, l) \\ \beta = bd^{-1} \\ \gamma_i = -d^{-1}c_i \ (i = 1, \ldots, l) \\ \delta = d^{-1} \end{cases}.$$

Утверждение 5.19. Автомат $M_8 \in \widetilde{\mathcal{A}}_{l,8}$ является обратимым автоматом тогда и только тогда, когда $c_1, b \in K^{inv}$. При этом обратный автомат имеет вид

$$M_7^{-1}: \begin{cases} q_{t+l} = \sum\limits_{i=2}^{l} \alpha_i q_{t+l-i} + \beta x_{t+1} \\ y_{t+1} = \sum\limits_{i=1}^{l} \gamma_i q_{t+l-i} + \delta x_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

где

$$\begin{cases} \alpha_i = c_1^{-1}c_i \ (i = 2, \ldots, l) \\ \beta = c_1^{-1} \\ \gamma_i = -b^{-1}(c_1^{-1}c_{i+1} - a_i) \ (i = 1, \ldots, l-1) \\ \gamma_l = -b^{-1}a_l \\ \delta = b^{-1}c_1^{-1} \end{cases}.$$

Обозначим через $\widetilde{\mathcal{A}}_{l,i}^{inv}$ $(i = 7, 8)$ множество всех обратимых автоматов $M_i \in \widetilde{\mathcal{A}}_{l,i}$.

Из Из утверждений 5.18 и 5.19, а также из формул (5.20), (5.21) и (5.24) вытекает, что

$$|\widetilde{\mathcal{A}}_{l,i}| = |K|^{2l+9-i} \ (i = 7, 8),$$

$$|\widetilde{\mathcal{A}}_{l,i}^{inv}| = |K|^{2l+15-2i}|K^{inv}|^{i-6} \ (i = 7, 8),$$

$$\mathsf{P}_{\widetilde{\mathcal{A}}_{l,i}^{inv}} = \frac{|K^{inv}|^{i-6}}{|K|^{i-6}} \ (i = 7, 8).$$

Обозначим через $\widetilde{\mathcal{A}}_{l,i}^{sc}$ $(i = 7, 8)$ множество всех сильно связных автоматов $M_i \in \widetilde{\mathcal{A}}_{l,i}$, через $\widetilde{\mathcal{A}}_{l,i}^{p}$ $(i = 7, 8)$ множество всех перестановочных автоматов $M_i \in \widetilde{\mathcal{A}}_{l,i}$, а через $\widetilde{\mathcal{A}}_{l,i}^{u-inv}$ $(i = 7, 8;\ u \in \{sc, p\})$ – множество всех обратимых автоматов $M_i \in \widetilde{\mathcal{A}}_{l,i}^{u}$.

Эти нетривиальные подмножества автоматов характеризуются следующим образом.

Теорема 5.12. Для каждого числа $l \in \mathbf{N}$ $M_i \in \widetilde{\mathcal{A}}_{l,i}^{sc}$ $(i = 7, 8)$ тогда и только тогда, когда $b \in K^{inv}$.

Доказательство теоремы 5.12 аналогично доказательству теремы 5.13 из [52].

Следствие 5.20. Для каждого числа $l \in \mathbf{N}$ диаметр графа переходов любого автомата $M_i \in \widetilde{\mathcal{A}}_{l,i}^{sc}$ $(i = 7, 8)$ равен l.

Следствие 5.21. Для каждого числа $l \in \mathbf{N}$ истинно равенство

$$\widetilde{\mathcal{A}}_{l,8}^{sc-inv} = \widetilde{\mathcal{A}}_{l,8}^{inv}.$$

Теорема 5.13. Для каждого числа $l \in \mathbf{N}$ $M_i \in \widetilde{\mathcal{A}}_{l,i}^{p}$ $(i = 7, 8)$ тогда и только тогда, когда $a_l \in K^{inv}$.

Доказательство теоремы 5.13 аналогично доказательству теремы 5.14 из [52].

Следствие 5.22. Для каждого числа $l \in \mathbf{N}$ $M_7 \in \widetilde{\mathcal{A}}_{l,7}^{p}$ тогда и только тогда, когда $a_l, d \in K^{inv}$.

Следствие 5.23. Для каждого числа $l \in \mathbf{N}$ $M_8 \in \widetilde{\mathcal{A}}_{l,8}^{p}$ тогда и только тогда, когда $a_l, b, c_1 \in K^{inv}$.

5.8. Имитационная модель автомата.

В п.5.4 было отмечено, что задача параметрической идентификации представляет собой математическую модель атаки криптоаналитика на

секретный ключ средней или большой длительности симметричного поточного шифра. Однако, эта задача не всегда имеет единственное решение.

В то же время одной из разновидностей атаки криптоаналитика на шифр является попытка построения, на основе полученной им информации, некоторого алгоритма, который "достаточно хорошо"осуществляет расшифрование шифртекста. Такой алгоритм естественно назвать "имитационной моделью".

Рассмотрим особенности построения имитационной модели для нелинейных автоматов над кольцом $\mathcal{K} = (K, +, \cdot)$.

5.8.1. Основные понятия.

Пусть M – автомат над кольцом $\mathcal{K}$, заданный системой уравнений, зависящей от набора параметров $\mathbf{a} = (a_1, \ldots, a_l) \in K^l$, у которого множеством состояний является множество K^n, а входным и выходным алфавитом – множество K^m.

Зафиксируем отображение

$$g_{\mathbf{a}} : (K^m)^+ \to (K^m)^+.$$

Рассмотрим отображение

$$f_{(M,\mathbf{q}_0)} : (K^m)^+ \to (K^m)^+,$$

реализуемое инициальным автоматом $(M, \mathbf{q}_0)$ $(\mathbf{q}_0 \in K^n)$.

Пусть для входного слова $\mathbf{x}_1 \ldots \mathbf{x}_k \in K^{mk}$ $(k \in \mathbf{N})$

$$f_{(M,\mathbf{q}_0)}(\mathbf{x}_1 \ldots \mathbf{x}_k) = \mathbf{y}_1 \ldots \mathbf{y}_k$$

и

$$g_{\mathbf{a}}(\mathbf{x}_1 \ldots \mathbf{x}_k) = \widetilde{\mathbf{y}}_1 \ldots \widetilde{\mathbf{y}}_k.$$

Обозначим через $d_{\mathbf{q}_0,\mathbf{x}_1\ldots\mathbf{x}_k}(\widetilde{\mathbf{y}}_1 \ldots \widetilde{\mathbf{y}}_k)$ длину слова, полученного в результате вычеркивания из слова $\widetilde{\mathbf{y}}_1 \ldots \widetilde{\mathbf{y}}_k$ всех таких символов $\widetilde{\mathbf{y}}_i$, что $\widetilde{\mathbf{y}}_i \neq \mathbf{y}_i$ и положим

$$\alpha_{\mathbf{q}_0,k} = \frac{\sum\limits_{\mathbf{x}_1\ldots\mathbf{x}_k \in K^{mk}} d_{\mathbf{q}_0,\mathbf{x}_1\ldots\mathbf{x}_k}(\widetilde{\mathbf{y}}_1 \ldots \widetilde{\mathbf{y}}_k)}{|K|^{mk}},$$

$$\beta_{\mathbf{q}_0} = \lim_{k\to\infty} \frac{1}{k} \sum_{i=1}^{k} \alpha_{\mathbf{q}_0,i}$$

и

$$\gamma = \min_{\mathbf{q}_0 \in K^n} \beta_{\mathbf{q}_0}.$$

Отображение $g_{\mathbf{a}}$ назовем *имитационной моделью* автомата M, осуществляющей моделирование автомата M с асимптотической точностью, равной γ.

В частности, имитационную модель $g_{\mathbf{a}}$ автомата M назовем *асимптотически точной*, если $\gamma = 1$.

Рассмотрим возможность построения асимптотически точной имитационной модели для автоматов над кольцом $\mathcal{K}$.

5.8.2. Построение асимптотически точной имитационной модели нелинейного автомата с лагом 2.

Рассмотрим над кольцом $\mathcal{K}$ класс $\mathcal{A}_{2,9}$ нелинейных одномерных автоматов Мура M с лагом 2, определяемых системой уравнений

$$\begin{cases} q_{t+2} = a + bq_{t+1}^2 + cq_t + dx_{t+1} \\ y_{t+1} = eq_{t+2} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{5.105}$$

где $a, b, c \in K\backslash\{0\}$ и $d, e \in K^{inv}$, x_{t+1} и y_{t+1} – соответственно, входной и выходной символ в момент $t+1$, а $\mathbf{q}_t = (q_{t+1}, q_t)$ – состояние в момент t.

Замечание 5.2. Уравнение

$$q_{t+2} = a + bq_{t+1}^2 + cq_t + dx_{t+1}$$

представляет собой аналог над кольцом $\mathcal{K}$ ряда модельных хаотических отображений, в том числе, отображения Эно [38].

Из (5.105) вытекает, что

$$y_{t+1} = e(a + bq_{t+1}^2 + cq_t + dx_{t+1}) \ (t \in \mathbf{Z}_+). \tag{5.106}$$

Подставив $t = 0, 1, \ldots, l$ $(l > 2)$ в (5.106), с учетом 2-го уравнения системы (5.105), получим

$$\begin{cases} y_1 = ae + beq_1^2 + ceq_0 + dex_1 \\ y_2 = ae + be^{-1}y_1^2 + ceq_1 + dex_2 \\ y_i = ae + be^{-1}y_{i-1}^2 + cy_{i-2} + dex_i \ (i = 3, \ldots, l) \end{cases} . \qquad (5.107)$$

Из последних $l-2$ уравнений системы (5.107) вытекает, что при известном наборе параметров

$$(a, b, c, d, e) \in (K \backslash \{0\})^3 \times (K^{inv})^2, \qquad (5.108)$$

криптоаналитик, даже не располагая информацией о начальном состоянии автомата $M \in \mathcal{A}_{2,9}$, может идентифицировать суффикс $x_3 \ldots x_l$ входного слова, так как

$$x_i = (de)^{-1}(ae + be^{-1}y_{i-1}^2 + cy_{i-2} - y_i) \ (i = 3, \ldots, l).$$

Предположим теперь, что набор параметров (5.108) не известен криптоаналитику.

Следующая теорема показывает, что в этом случае построение имитационной модели автомата $M \in \mathcal{A}_{2,9}$ является актуальной задачей.

Теорема 5.14. Никакой простой эксперимент с автоматом $M \in \mathcal{A}_{2,9}$ не дает возможность вычислить точное решение задачи его параметрической идентификации. Однако, может существовать простой эксперимент с автоматом $M \in \mathcal{A}_{2,9}$, который дает возможность построить асимптотически точную имитационную модель, причем только параметр $c \in K$ будет вычислен точно.

Доказательство. Предположим, что начальное состояние автомата $M \in \mathcal{A}_{2,9}$ известно экспериментатору.

Пусть $\mathbf{q}_0 = (0, 0)$. Тогда система уравнений (5.107) принимет вид

$$\begin{cases} u_1 + x_1u_4 = y_1 \\ u_1 + y_1^2u_2 + x_2u_4 = y_2 \\ u_1 + y_{i-1}^2u_2 + y_{i-2}u_3 + x_iu_4 = y_i \ (i = 3, \ldots, l) \end{cases} , \qquad (5.109)$$

где u_i $(i = 1, \ldots, 4)$ – такие неизвестные, что

$$(u_1, u_2, u_3, u_4) = (ae, be^{-1}, c, de). \qquad (5.110)$$

Матрица системы уравнений (5.109) имеет вид

$$A = \begin{pmatrix} 1 & 0 & 0 & x_1 \\ 1 & y_1^2 & 0 & x_2 \\ 1 & y_2^2 & y_1 & x_3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & y_{l-1}^2 & y_{l-2} & x_l \end{pmatrix}.$$

Если существует такое входное слово $x_1 \dots x_l \in K^l$ заранее неизвестной длины $l \geq 4$, что матрица A содержит обратимую матрицу 4-го порядка, то может быть вычислено единственное решение (u_1, u_2, u_3, u_4) системы уравнений (5.109).

Из (5.110) вытекает, что тем самым будут вычислены величины ae, be^{-1}, c и de, т.е. только параметр c автомата $M \in \mathcal{A}_{2,9}$ будет вычислен точно.

При этом, из (5.109) вытекает, что

$$\begin{cases} y_1 = u_1 & + x_1 u_4 \\ y_2 = u_1 + y_1^2 u_2 & + x_2 u_4 \\ y_i = u_1 + y_{i-1}^2 u_2 + y_{i-2} u_3 + x_i u_4 \ (i = 3, \dots, l) \end{cases}, \tag{5.111}$$

где значения u_j $(j = 1, \dots, 4)$ определены равенством (5.110).

Пусть $\mathbf{q}_0 \neq (0, 0)$. Тогда система уравнений (5.107) принимет вид

$$\begin{cases} v_1 + q_1^2 v_2 & + q_0 v_4 & + x_1 v_6 = y_1 \\ v_1 & + y_1^2 v_3 + q_1 v_4 & + x_2 v_6 = y_2 \\ v_1 & + y_{i-1}^2 v_3 & + y_{i-2} v_5 + x_i v_6 = y_i \ (i = 3, \dots, l) \end{cases}, \tag{5.112}$$

где v_i $(i = 1, \dots, 6)$ – такие неизвестные, что

$$(v_1, v_2, v_3, v_4, v_5, v_6) = (ae, be, be^{-1}, ce, c, de). \tag{5.113}$$

Матрица системы уравнений (5.112) имеет вид

$$B = \begin{pmatrix} 1 & q_1^2 & 0 & q_0 & 0 & x_1 \\ 1 & 0 & y_1^2 & q_1 & 0 & x_2 \\ 1 & 0 & y_2^2 & 0 & y_1 & x_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & y_{l-1}^2 & 0 & y_{l-2} & x_l \end{pmatrix}.$$

Если существует такое входное слово $x_1 \dots x_l \in K^l$ заранее неизвестной длины $l \geq 6$, что матрица B содержит обратимую матрицу 6-го порядка, то может быть вычислено единственное решение $(v_1, \dots, v_6)$ системы уравнений (5.112).

Из (5.113) вытекает, что тем самым будут вычислены величины ae, be, be^{-1}, ce, c и de, т.е. только параметр c автомата $M \in \mathcal{A}_{2,9}$ будет вычислен точно.

При этом, из (5.112) вытекает, что

$$\begin{cases} y_1 = v_1 + q_1^2 v_2 & + q_0 v_4 & + x_1 v_6 \\ y_2 = v_1 & + y_1^2 v_3 + q_1 v_4 & + x_2 v_6 \\ y_i = v_1 & + y_{i-1}^2 v_3 & + y_{i-2} v_5 + x_i v_6 \ (i = 3, \dots, l) \end{cases},$$

где значения v_j $(j = 1, \dots, 6)$ определены равенством (5.113).

Предположим теперь, что начальное состояние автомата $M \in \mathcal{A}_{2,9}$ не известно экспериментатору.

Учитывая, что ситуации различаются при $\mathbf{q}_0 = (0, 0)$ и $\mathbf{q}_0 \neq (0, 0)$, отбросим в системе уравнений (5.112) первые два уравнения. Получим систему уравнений

$$w_1 + y_{i-1}^2 w_2 + y_{i-2} w_3 + x_i w_4 = y_i \ (i = 3, \dots, l), \tag{5.114}$$

где

$$(w_1, w_2, w_3, w_4) = (ae, be^{-1}, c, de). \tag{5.115}$$

Матрица системы уравнений (5.114) имеет вид

$$C = \begin{pmatrix} 1 & y_2^2 & y_1 & x_3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & y_{l-1}^2 & y_{l-2} & x_l \end{pmatrix}.$$

Если существует такое входное слово $x_1 \dots x_l \in K^l$ заранее неизвестной длины $l \geq 6$, что матрица C содержит обратимую матрицу 4-го порядка, то может быть вычислено единственное решение (w_1, w_2, w_3, w_4) системы уравнений (5.114).

Из (5.115) вытекает, что тем самым будут вычислены величины ae, be^{-1}, c и de, т.е. только параметр c автомата $M \in \mathcal{A}_{2,9}$ будет вычислен точно.

При этом, из (5.114) вытекает, что имитационная модель, моделирующая поведение автомата $M \in \mathcal{A}_{2,9}$ на суффиксах входных слов, полученных отбрасыванием префикса длины 2, имеет вид

$$y_i = w_1 + y_{i-1}^2 w_2 + y_{i-2} w_3 + x_i w_4 \ (i = 3, \dots, l), \tag{5.116}$$

где значения w_j $(j = 1, \dots, 4)$ определены равенством (5.115).

Ясно, что (5.116) – асимптотически точная имитационная модель автомата $M \in \mathcal{A}_{2,9}$.

□

Следствие 5.24. Кратный эксперимент с автоматом $M \in \mathcal{A}_{2,9}$ не дает возможность вычислить точное решение задачи его параметрической идентификации. Однако, может существовать кратный эксперимент с автоматом $M \in \mathcal{A}_{2,9}$, который дает возможность построить асимптотически точную имитационную модель, причем только параметр $c \in K$ будет вычислен точно.

Доказательство. В процессе кратного эксперимента с автоматом $M \in \mathcal{A}_{2,9}$ будет построено несколько систем уравнений (5.109), (5.112) или (5.116) (число этих систем уравнений равно кратности эксперимента).

Однако, решение этих систем определяет точно такие же комбинации параметров, как и в случае простого эксперимента.

□

Полученные результаты показывают, что при построении асимптотически точной имитационной модели автомата $M \in \mathcal{A}_{2,9}$, экспериментатор вынужден осуществлять поиск по множеству, содержащему не менее $|K|^4$ элементов.

Отсюда вытекает, что сложность построения асимптотически точной имитационной модели автомата $M \in \mathcal{A}_{2,9}$ достаточно высока (достаточно

положить $\mathcal{K} = \mathcal{Z}_{p^k}$, где p – простое число, для записи которого необходимо 100 бит).

Тем не менее, асимптотически точная имитационная модель (5.116) имеет достаточно простой вид.

Это обусловлено тем, что функция выходов автомата $M \in \mathcal{A}_{2,9}$ является линейной функцией от одной из компонент состояния.

Отсюда вытекает, что актуальной является задача выделения классов обратимых автоматов над кольцом $\mathcal{K}$, для которых любая асимптотически точная имитационная модель существенно сложнее, чем система уравнений, определяющая автомат.

6. ТЕОРИЯ СХЕМ И АЛГЕБРАИЧЕСКИЕ КРИВЫЕ

В п.1.2.3 было отмечено, что алгебраические характеристики многообразия могут быть сформулированы в терминах его координатного кольца.

Для многообразия над полем координатное кольцо характеризуется тем, что оно является ассоциативно-коммутативным кольцом с единицей, удовлетворяющим следующим трем условиям:

1) является алгеброй над некоторым полем;

2) конечно порождено над этим полем;

3) не имеет нильпотентных элементов.

В то же время исследование алгебраических многообразий (в частности, алгебраических кривых) в терминах морфизмов естественно привело к разработке математического аппарата, предназначенного для их определения с использованием произвольного ассоциативно-коммутативного кольца с единицей.

Общее понятие, к которому приходят таким образом называется *схемой*. Это понятие дает возможность охватить более широкое множество объектов, чем алгебраические многообразия.

Последнее обусловлено следующими двумя обстоятельствами.

Во-первых, кольца, используемые в определении схемы, могут не быть алгебрами над полем (что, в частности, дает возможность эффективно применять теорию схем при исследовании проблем теории чисел).

Во вторых, кольца, используемые в определении схемы, могут содержать нильпотентные элементы (что, в частности, дает возможность применять в алгебраической геометрии понятия дифференциальной геометрии, связанные с бесконечно малым изменением точек или подмногообразий на алгебраическом многообразии).

Целью настоящего раздела является краткое изложение основ теории схем и характеристика в терминах этой теории некоторых свойств алгебраических кривых.

В настоящем разделе под кольцом понимается ассоциативно-коммутативное кольцо с единицей.

В пп.6.1 и 6.2 рассмотрены два основных понятия, используемых при определении схемы, а именно: *спектр кольца* (п.6.1) и *пучек* (п.6.2). В п. 6.3. охарактеризовано понятие схема. В п.6.4 введено понятие *векторное расслоение*. Это понятие характеризуется тем, что для неособого проективного многообразия над алгебраически замкнутым полем определенные на нем категория локально свободных пучков конечного ранга и категория векторных расслоений эквивалентны (см., напр., [31]). В п.6.5 приведено вычисление структурного пучка для произвольных коммутативных колец с единицей, специализированы результаты теории схем в направлении схемного расширения понятия алгебраическая кривая и в направлении определения групповых схем, а также даны примеры, иллюстрирующие некоторые определения и результаты. Представленное здесь обобщает рассмотрения некоторых из ранее представленных разделов.

Материал, представленный в настоящем разделе, изложен в соответствии с подходом, принятым в [31,75,83,85,92,105,107,118].

6.1. Спектры колец.

В п.1.2 показано, что каждому многоообразию V (в частности, алгебраической кривой) может быть сопоставлено координатное кольцо, в терминах которого могут быть сформулированы и исследованы алгебраические характеристики многообразия V.

Рассмотрим обратную задачу, а именно: как с произвольным кольцом $\mathcal{K}$ сопоставить геометрический объект V, который в случае, когда этот объект является многообразием, а $\mathcal{K}$ – его координатным кольцом, приводит к обычным конструкциям, построенным на многообразии.

Замечание 6.1. Содержательно решение этой задачи означает разработку математического аппарата, обеспечивающего выполнение построений, представленных в замечании 3.3, в обратном порядке.

6.1.1. Основные понятия.

Спектром кольца $\mathcal{K} = (K, +, \cdot)$ (обозначается $\mathtt{Spec}\,\mathcal{K}$) называется множество всех его простых идеалов, отличных от кольца $\mathcal{K}$. Сами эти идеалы называются *точками* спектра.

Пример 6.1. 1. Для кольца $\mathcal{Z} = (\mathbf{Z}, +, \cdot)$

$$\mathtt{Spec}\ \mathcal{Z} = \{(0)\} \cup \{(p) | p\ -\ \text{простое число}\}.$$

2. Если $\mathcal{L}_x$ – локальное кольцо точки x неприводимой алгебраической кривой Γ, определенной над некоторой областью целостности, т.е. кольцо всех таких рациональных функций $\frac{f}{g}$, определенных на кривой Γ, что

$$g(x) \neq 0,$$

то $\mathtt{Spec}\ \mathcal{L}_x$ состоит из двух точек: нулевого и максимального идеалов.

Замечание 6.2. Пусть $\mathcal{K}$ – кольцо регулярных функций, определенных на аффинном многообразии V.

Геометрический смысл множества простых идеалов кольца $\mathcal{K}$ состоит в том, что это множество является множеством всех неприводимых подмногообразий многообразия V (т.е. точек, неприводимых кривых или поверхностей).

Если φ – гомоморфизм кольца $\mathcal{K}_1$ в кольцо $\mathcal{K}_2$, то для любого простого идеала I_2 кольца $\mathcal{K}_2$ его прообраз

$$I_1 = \varphi^{-1}(I_2)$$

является простым идеалом кольца $\mathcal{K}_1$.

Таким с каждым гомоморфизмом φ кольца $\mathcal{K}_1$ на кольцо $\mathcal{K}_2$ можно сопоставить *ассоциированное* с ним такое отображение

$$^a\varphi : \mathtt{Spec}\,\mathcal{K}_2 \to \mathtt{Spec}\,\mathcal{K}_1,$$

что

$$^a\varphi(I_2) = I_1 \Leftrightarrow \varphi(I_1) = I_2 \ (I_i \in \mathtt{Spec}\,\mathcal{K}_i \ (i = 1, 2)).$$

Пример 6.2. Подмножество элементов кольца называется *мультипликативным множеством*, если оно содержит единицу и замкнуто относительно операции умножения.

По аналогии с тем, как это было сделано в замечении 1.16, для любого мультипликативного множества S кольца $\mathcal{K} = (K, +, \cdot)$ можно построить кольцо частных

$$\mathcal{K}_S = (K_S, +, \cdot).$$

Множество K_S является фактор-множеством множества всех упорядоченных пар (x, s) $(x \in K, s \in S)$ по отношению эквивалентности $\equiv_S$, определенному следующим образом

$$(x_1, s_1) \equiv_S (x_2, s_2) \Leftrightarrow (\exists s_3 \in S)(s_3(a_1 s_2 - a_2 s_1) = 0)$$

а операции осуществляются на основе формул

$$(x_1, s_1) + (x_2, s_2) = (x_1 s_2 + x_2 s_1, s_1 s_2),$$

$$(x_1, s_1) \cdot (x_2, s_2) = (x_1 x_2, s_1 s_2).$$

Если

$$S = \{1\} \cup \{a^n | n \in \mathbf{N}\} \ (a \in K),$$

то вместо $\mathcal{K}_S = (K_S, +, \cdot)$ пишут $\mathcal{K}_a = (K_a, +, \cdot)$.

Отметим, что если $0 \in S$, то $\mathcal{K}_S$ – одноэлементное кольцо.

Отображение $\varphi : K \to K_S$, определенное равенством

$$\varphi(x) = (x, 1),$$

является гомоморфизмом кольца $\mathcal{K}$ в кольцо $\mathcal{K}_S$.

Для ассоциированного отображения $^a\varphi : \mathtt{Spec}\,\mathcal{K}_S \to \mathtt{Spec}\,\mathcal{K}$ множество $\mathrm{Val}\,(^a\varphi)$ состоит из всех простых идеалов кольца $\mathcal{K}$, не содержащих ни одного элемента множества S.

При этом, для обратного отображения

$$(^a\varphi)^{-1} : \mathrm{Val}\,(^a\varphi) \to \mathtt{Spec}\,\mathcal{K}_S$$

истинно равенство

$$({}^a\varphi)^{-1}(I) = \{(x,s)|x \in I, s \in S\} \ (I \in \mathrm{Val}\,({}^a\varphi)).$$

Каждой точке $I \in \mathtt{Spec}\,\mathcal{K}$ может быть сопоставлено факторкольцо $\mathcal{K}/_{\equiv_I}$. Кольцо частных $\mathcal{L}_I$ этого фактор-кольца называется *локальным кольцом* простого идеала I.

Пример 6.3. 1. Пусть $\mathcal{K} = \mathcal{Z}$. Тогда:

1) если $I = (p)$ (p – простое число), то $\mathcal{L}_I$ – это кольцо всех рациональных чисел, знаменатели которых взаимно просты с p;

2) если $I = (0)$, то $\mathcal{L}_I$ – это кольцо $\mathcal{Q}$ всех рациональных чисел.

2. Пусть для кольца $\mathcal{K} = (K, +, \cdot)$ мультипликативное множество имеет вид

$$S = K \backslash I \ (I \in \mathtt{Spec}\,\mathcal{K}).$$

Тогда

$$\mathcal{K}_S = \mathcal{L}_I.$$

Точка $I \in \mathtt{Spec}\,\mathcal{K}$ называется *простой* (или *регулярной*), если локальное кольцо $\mathcal{L}_I$ нетерово и регулярно.

Замечание 6.3. Пусть $\mathcal{L} = (L, +, \cdot)$ – нетерово кольцо, а J – его максимальный идеал. Наименьшее число r таких элементов $x_1, \ldots, x_r \in J$, что

$$(x_1, \ldots, x_r) \supset J^k$$

для некоторого $k > 0$, называется размерностью кольца $\mathcal{L}$ (обозначается $\dim \mathcal{L}$).

В соответствии с леммой Накаямы идеал J порождается

$$n = \dim_{\mathcal{L}/_{\equiv_J}}(\mathcal{J}/_{\equiv_{J^2}})$$

элементами, где $\mathcal{J} = (J, +, \cdot)$.

Таким образом,

$$\dim \mathcal{L} \leq \dim_{\mathcal{L}/_{\equiv_J}}(\mathcal{J}/_{\equiv_{J^2}}).$$

Кольцо $\mathcal{L}$ называется *регулярным*, если в этом неравенстве имеет место знак равенства, т.е. если

$$\dim \mathcal{L} = \dim_{\mathcal{L}/_{\equiv_J}}(\mathcal{J}/_{\equiv_{J^2}}).$$

Если J_I – максимальный идеал локального кольца $\mathcal{L}_I$ ($I \in \mathtt{Spec}\,\mathcal{K}$), то

$$\mathtt{k}(I) := \mathcal{L}_I/_{\equiv_{J_I}}$$

является полем, а $\mathcal{J}_I/_{\equiv_{J_I^2}}$ – векторным пространством над этим полем. (причем конечномерным пространством, если кольцо $\mathcal{L}_I$ – нетерово).

Векторное пространство

$$\Theta_I = \mathcal{HOM}_{\mathtt{k}(I)}(\mathcal{J}_I/_{\equiv_{J_I^2}}, \mathtt{k}(I))$$

называется *касательным пространством* в точке $I \in \mathtt{Spec}\,\mathcal{K}$.

6.1.2. Спектральная топология.

Зафиксируем кольцо $\mathcal{K} = (K, +, \cdot)$ и следующим образом построим топологию на множестве $\mathtt{Spec}\,\mathcal{K}$ (эта топология и называется *спектральной топологией* или *топологией Зарисского*).

Сопоставим с каждым подмножеством $A \subseteq K$ подмножество

$$V(A) = \{I \in \mathtt{Spec}\,\mathcal{K} | A \subseteq I\}. \tag{6.1}$$

В дальнейшем, для краткости, вместо $V(\{a\})$ будем писать $V(a)$.

Из (6.1) вытекает, что:

1) для любого не более, чем счетного, семейства $\{A_\mathtt{j}\}_{\mathtt{j}\in\mathtt{J}}$ подмножеств множества K истинно равенство

$$V\left(\bigcup_{\mathtt{j}\in\mathtt{J}} A_\mathtt{j}\right) = \bigcap_{\mathtt{j}\in\mathtt{J}} V(A_\mathtt{j}); \tag{6.2}$$

2) для любых $A_1, A_2 \subseteq K$ истинно равенство

$$V(A_1) \cup V(A_2) = V(I)\ , \tag{6.3}$$

где I – пересечение идеалов, порожденных множествами A_1 и A_2;

3) для любого гомоморфизма φ кольца $\mathcal{K}_1 = (K_1, +_1, \cdot_1)$ в кольцо $\mathcal{K}_2 = (K_2, +_2, \cdot_2)$ истинно равенство

$$({}^{a}\varphi)^{-1}(V(A)) = V(\varphi(A)) \ (A \subseteq K_1). \tag{6.4}$$

Подмножество $X \subseteq \mathtt{Spec}\,\mathcal{K}$ называется:

1) *замкнутым*, если существует такой идеал Y кольца $\mathcal{K}$, что

$$X = V(Y);$$

2) *открытым*, если $K\backslash X$ – замкнутое множество.

Из (6.2) и (6.3) вытекает, что эти определения корректны.

Охарактеризуем построенную топологию.

Главными открытыми множествами в $\mathtt{Spec}\,\mathcal{K}$ называются такие множества

$$D(a) = (\mathtt{Spec}\,\mathcal{K})\backslash V(a),$$

что элемент $a \in K$ не является нильпотентным элементом кольца $\mathcal{K}$.

Отметим, что для любых, не являющихся нильпотентными, элементов $a, b \in K$, включение

$$D(a) \subseteq D(b)$$

истинно тогда и только тогда, когда существуют такие $n \in \mathbf{N}$ и $x \in K$, что

$$a^n = bx. \tag{6.5}$$

Главные открытые множества образуют *базис* в построенной топологии. При этом топологическое пространство $\mathtt{Spec}\,\mathcal{K}$ *бикомпактно*, т.е. из любого его покрытия главными открытыми множествами можно выбрать конечное подпокрытие.

Замыканием точки $I \in \mathtt{Spec}\,\mathcal{K}$ называется множество

$$V(I) = \bigcap_{A \supseteq I} V(A).$$

Из этого определения вытекает, что точка $I \in \mathtt{Spec}\,\mathcal{K}$ замкнута тогда и только тогда, когда I – максимальный идеал кольца $\mathcal{K}$.

Замечание 6.4. 1. Пусть кольцо $\mathcal{K}$ не содержит делителей нуля. Тогда идеал (0) является простым идеалом, содержащимся в каждом простом идеале. Это означает, что замыкание точки (0) совпадает со всем пространством $\mathtt{Spec}\,\mathcal{K}$. Таким образом, если кольцо $\mathcal{K}$ не содержит делителей нуля, то идеал (0) – *всюду плотная точка* пространства $\mathtt{Spec}\,\mathcal{K}$.

2. Всюду плотная точка пространства $\mathtt{Spec}\,\mathcal{K}$ (если она существует) называется *общей точкой пространства* $\mathtt{Spec}\,\mathcal{K}$. Возникает вопрос:

Когда существует общая точка пространства $\mathtt{Spec}\,\mathcal{K}$?

Ответ на этот вопрос следующий: общая точка пространства $\mathtt{Spec}\,\mathcal{K}$ существует тогда и только тогда, когда прост нильрадикал (т.е. идеал, состоящий из всех нильпотентных элементов) кольца $\mathcal{K}$. Простой нильрадикал и определяет единственную общую точку пространства $\mathtt{Spec}\,\mathcal{K}$.

Из (6.4) вытекает, что если φ – гомоморфизм кольца $\mathcal{K}_1 = (K_1, +_1, \cdot_1)$ в кольцо $\mathcal{K}_2 = (K_2, +_2, \cdot_2)$, то при ассоциированном отображении ${}^a\varphi$ прообраз любого открытого множества является открытым множеством. Это означает, что для любого гомоморфизма φ кольца $\mathcal{K}_1$ в кольцо $\mathcal{K}_2$ ассоциированное отображение ${}^a\varphi$ является непрерывным отображением.

Замечание 6.5. 1. Для любого кольца $\mathcal{K} = (K, +, \cdot)$ замкнутые множества в $\mathtt{Spec}\,\mathcal{K}$ гомеоморфны спектрам некоторых колец.

Действительно, для любого замкнутого множества X в $\mathtt{Spec}\,\mathcal{K}$ истинно равенство

$$X = V(I),$$

где I – идеал, идеал кольца $\mathcal{K}$.

Пусть φ – естественный гомоморфизм кольца $\mathcal{K}$ на кольцо $\mathcal{K}/_{\equiv_I}$. Тогда отображение ${}^a\varphi$ является гомеоморфизмом множества $\mathtt{Spec}\,(\mathcal{K}/_{\equiv_I})$ на замкнутое множество X, т.е. замкнутое множество X гомеоморфно спектру кольца $\mathcal{K}/_{\equiv_I}$.

2. Главное открытое множество $D(a)$ гомеоморфно спектру кольца частных $\mathcal{K}_a$,

3. Ясно, что $\mathtt{Spec}$ представляет собой функтор из категории ассоциативно-коммутативных колец с единицей в категорию топологических пространств.

Пример 6.4. Пусть S – мультипликативная система в кольце $\mathcal{K} = (K, +, \cdot)$, а φ – гомоморфизм кольца $\mathcal{K}$ в кольцо $\mathcal{K}_S$, определенный в примере 6.2.

Рассмотрим множество $\mathrm{Val}\,({}^a\varphi)$ как топологическое подпространство топологического пространства $\mathtt{Spec}\,\mathcal{K}$, т.е. замкнутыми множествами считаем множества $X \cap \mathrm{Val}\,({}^a\varphi)$, где X – замкнутое множество пространства $\mathtt{Spec}\,\mathcal{K}$.

Тогда непрерывными являются оба отображения ${}^a\varphi$ и $({}^a\varphi)^{-1}$, т.е. топологическое пространство $\mathtt{Spec}\,\mathcal{K}_S$ гомеоморфно топологическому пространству $\mathrm{Val}\,({}^a\varphi)$.

Топологическое пространство X называется *неприводимым*, если в нем не существуют такие непустые собственные замкнутые подмножества X_1, X_2, что

$$X = X_1 \cup X_2.$$

Говорят, что *размерность* топологического пространство X равна n, если в нем существует возрастающая последовательность непустых неприводимых замкнутых множеств

$$X_0 \subset X_1 \subset \cdots \subset X_n,$$

и не существует указанной последовательности с большим числом членов.

Истинны следующие утверждения:

1) если $\mathcal{K}$ – нетерово локальное кольцо, то размерность кольца $\mathtt{Spec}\,\mathcal{K}$ конечна и совпадает с размерностью кольца $\mathcal{K}$;

2) кольцо, имеющее конечное число образующих над кольцом конечной размерности, имеет конечную размерность;

3) кольцо целых алгебраических чисел поля алгебраических чисел имеет размерность 1.

6.2. Предпучки и пучки.

Понятие *пучка*, введенное Лере, оказалось очень полезным инструментом в исследовании функций на вещественных, комплексных и арифметических многообразиях.

Исторически одной из мотивировок введения пучков были задачи и методы теории функций одной и многих комплексных переменных, в частности, задачи и методы теории римановых поверхностей. Используются пучки множеств, абелевых групп, колец, модулей над кольцами, а также и других алгебраических структур [31].

Один из подходов к теории пучков, который допускает как обобщение на достаточно общие категории, так и конкретизацию на отдельные задачи, основывается на первоначальном введении *предпучков* и их последующей специализации на пучки.

Именно такой подход и рассматривается ниже.

6.2.1. Основные понятия.

Пусть с каждым открытым множеством U топологического пространства X сопоставлено некоторое множество $\mathcal{F}(U)$, причем для любых открытых множеств U, V $(U \subseteq V)$ задано такое отображение

$$\rho_U^V : \mathcal{F}(V) \to \mathcal{F}(U),$$

что выполнены следующие три условия:

1) $|\mathcal{F}(\emptyset)| = 1$;

2) для любого открытого множества U отображение ρ_U^U является тождественным отображением;

3) для любых таких открытых множеств U, V, W, что

$$U \subseteq V \subseteq W$$

истинно равенство

$$\rho_U^W = \rho_U^V \rho_V^W .$$

Такая система множеств и отображений называется *предпучком* и часто обозначается $\mathcal{F}$ (если хотят подчеркнуть, что отображение ρ_U^V относится именно к пучку $\mathcal{F}$, то пишут $\rho_{U,\mathcal{F}}^V$).

Замечание 6.6. 1. Предпучок на топологическом пространстве представляет собой контрвариантный функтор из категории открытых покрытий этого пространства и их вложение в категорию множеств и их отображений.

2. Различный выбор элемента $\mathcal{F}(\emptyset)$ приводит к *изоморфным* предпучкам. Поэтому для задания предпучка достаточно зафиксировать множества $\mathcal{F}(U)$ для непустых открытых множеств U.

Если все множества $\mathcal{F}(U)$ являются группами, модулями над кольцом или кольцами, то говорят о предпучке, соответственно, групп, модулей над кольцом или колец.

Пример 6.5. 1. Превратим неприводимое квазипроективное многообразие X в топологическое пространство, считая, что замкнутыми множествами являются алгебраические подмногообразия многообразия X.

Для любого открытого множества U в качестве $\mathcal{F}(U)$ выберем множество всех рациональных функций, регулярных в каждой его точке, а для любых открытых множеств U, V $(U \subseteq V)$ в качестве ρ_U^V – ограничение функции, заданной на V, на множество U.

В результате построен предпучок колец $\mathcal{F}$, называемый *предпучком регулярных функций*.

2. Для заданного кольца $\mathcal{K} = (K, +, \cdot)$ *структурный предпучек* $\mathfrak{O}$ на топологическом пространстве $\mathtt{Spec}\,\mathcal{K}$ определяется следующим образом:

1) для каждого главного открытого множества $D(a)$

$$\mathfrak{O}(D(a)) = K_a;$$

2) для любых таких, не являющихся нильпотентными, элементов $a, b \in K$, что

$$D(a) \subseteq D(b)$$

гомоморфизм $\rho_{D(a)}^{D(b)}$ кольца $\mathcal{K}_b$ в кольцо $\mathcal{K}_a$ определяется равенством

$$\rho_{D(a)}^{D(b)}\left(\frac{c}{b^k}\right) = \frac{cx^k}{b^{nk}},$$

где элемент $x \in K$ и число $n \in \mathbf{N}$ определяются равенством (6.5);

3) для любого открытого множества $U \subseteq \mathtt{Spec}\,\mathcal{K}$

$$\mathfrak{O}(U) = \varprojlim \mathfrak{O}(D(a)),$$

где проективный предел берется по всем $D(a) \subseteq D(U)$ относительно системы гомоморфизмов $\rho_{D(a)}^{D(b)}$ $(D(a) \subseteq D(b))$.

Замечание 6.7. *Проективный предел* системы множеств определяется следующим образом.

Пусть задана система множеств $\{A_\alpha\}_{\alpha\in\mathtt{I}}$, где $\mathtt{I}$ – частично упорядоченное множество, а также для любых $\alpha, \beta \in \mathtt{I}$ $(\alpha \leq \beta)$ задано такое отображение $f_\alpha^\beta : A_\beta \to A_\alpha$, что выполнены следующие два условия:

1) f_α^α $(\alpha \in \mathtt{I})$ – тождественное отображение;

2) для любых таких $\alpha, \beta, \gamma \in \mathtt{I}$, что $\alpha \leq \beta \leq \gamma$, истинно равенство

$$f_\alpha^\gamma = f_\alpha^\beta f_\beta^\gamma.$$

Проективным пределом системы множеств $\{A_\alpha\}_{\alpha\in\mathtt{I}}$ относительно системы отображений $\{f_\alpha\}_{\alpha\in\mathtt{I}}$ (обозначается $\varprojlim A_\alpha$) называется подмножество прямого произведения $\prod\limits_{\alpha\in\mathtt{I}} A_\alpha$, состоящее из всех таких элементов $x = \{x_\alpha\}_{\alpha\in\mathtt{I}}$, что

$$x_\alpha = f_\alpha^\beta x_\beta$$

для всех $\beta \geq \alpha$. При этом отображения

$$x \to x_\alpha \ (x \in \varprojlim A_\alpha)$$

называются *естественными отображениями* проективного предела.

Если $\{A_\alpha\}_{\alpha\in\mathtt{I}}$ является системой групп, колец или модулей, то $\varprojlim A_\alpha$ является алгебраической структурой того же типа.

Пучком на топологическом пространстве X называется такой предпучок $\mathcal{F}$, что для любого открытого множества $U \subseteq X$ и для любого его открытого покрытия

$$U = \bigcup_{\alpha\in\mathtt{I}} U_\alpha$$

выполнены следующие два условия:

1) если

$$\rho^U_{U_\alpha} s_1 = \rho^U_{U_\alpha} s_2$$

для $s_1, s_2 \in \mathcal{F}(U)$ и всех U_α, то $s_1 = s_2$;

2) если $s_\alpha \in \mathcal{F}(U_\alpha)$ $(\alpha \in \mathtt{I})$ таковы, что

$$\rho^{U_\alpha}_{U_\alpha\cap U_\beta} s_\alpha = \rho^{U_\beta}_{U_\alpha\cap U_\beta} s_\beta$$

то существует такой элемент $s \in \mathcal{F}(U)$, что $s_\alpha = \rho^U_{U_\alpha} s$ для всех U_α.

Замечание 6.8. Понятие *пучок* отражает следующее свойство *локальности* отображений, определенных на топологическом пространстве X.

Пусть X является объединением открытых множеств U_α. Тогда любое отображение f, определенное на X, однозначно определяется своими сужениями на множества U_α.

Если на каждом множестве U_α определено отображение f_α, причем сужения f_α и f_β на множество $U_\alpha \cap U_\beta$ совпадают, то существует такое отображение f, определенное на всем топологическом пространстве X, что каждое отображение f_α является сужением f на множество U_α.

Таким образом, понятия непрерывной, дифференцируемой или регулярной функции имеет локальный характер.

Пример 6.6. Структурный предпучок $\mathfrak{O}$ на топологическом пространстве $\mathtt{Spec}\ \mathcal{K}$ является пучком.

6.2.2. Слои предпучков и пучков.

Пусть на топологическом пространстве X определен такой предпучок $\mathcal{F}$, что для всех открытых множеств U множества $\mathcal{F}(U)$ являются подмножествами одного и того же множества.

Для любой точки $x \in X$ обозначим через $\mathcal{F}_x$ объединение всех открытых множеств $\mathcal{F}(U)$, содержащих эту точку.

Пример 6.7. 1. Пусть $\mathcal{F}$ – пучок всех непрерывных функций, определенных на топологическом пространстве X. Тогда множество $\mathcal{F}_x$ $(x \in X)$ состоит из *ростков* функций, непрерывных в некоторой окрестности точки x (т.е. является результатом отождествления функций, совпадающих в некоторой окрестности точки x);

2. Пусть $\mathcal{F}$ – пучок всех регулярных функций, определенных на неприводимом квазипроективном многообразии, то $\mathcal{F}_x$ $(x \in X)$. Тогда множество $\mathcal{F}_x$ $(x \in X)$ состоит из всех элементов локального кольца точки x.

В случае произвольного пучка, определенного на топологическом пространстве X, множества $\mathcal{F}(U)$ могут быть подмножествами различных множеств. Однако их связь через гомоморфизмы ρ_U^V $(U \subseteq V)$ дает возможность заменить объединение всех открытых множеств $\mathcal{F}(U)$, содержащих точку $x \in X$, *индуктивным пределом* семейства множеств.

Замечание 6.9. Определение *индуктивного предела*, по своей сути, отличается от определения *проективного предела* только тем, что для индуктивного предела множество индексов $\mathtt{I}$ системы множеств $\{A_\alpha\}_{\alpha\in\mathtt{I}}$ является линейно упорядоченным множеством, т.е. $\{A_\alpha\}_{\alpha\in\mathtt{I}}$ – семейство множеств.

По-видимому, одним из наиболее известных примеров индуктивного предела для кольца является индуктивный предел такого семейства идеалов $\{I_\alpha\}_{\alpha\in\mathtt{I}}$, что $I_\alpha \subseteq I_\beta$ $(\alpha \leq \beta)$.

В этом случае индуктивным пределом является идеал $\bigcup\limits_{\alpha\in\mathtt{I}} I_\alpha$, а отображения f_α^β $(\alpha \leq \beta)$ являются вложениями.

Рассмотрим теперь произвольный предпучок $\mathcal{F}$ на топологическом пространсте X.

Слоем $\mathcal{F}_x$ $(x \in X)$ предпучка $\mathcal{F}$ в точке x называется индуктивный предел множеств $\mathcal{F}(U)$ для всех U $(x \in U)$ относительно системы отображений ρ_U^V $(U \subseteq V)$.

Замечание 6.10. Из этого определения вытекает, что элемент множества $\mathcal{F}_x$ $(x \in X)$ задается элементом любого из множеств $\mathcal{F}(U)$ $(x \in U)$. При этом элементы $u \in \mathcal{F}(U)$ и $v \in \mathcal{F}(V)$ отождествляются, если существует такое открытое множество $W = U \cap V$ $(x \in W)$, что

$$\rho_W^U u = \rho_W^V v.$$

Пример 6.8. Слоем структурного пучка $\mathfrak{O}$ кольца $\mathcal{K}$ в точке $I \in \mathtt{Spec}\ \mathcal{K}$ является локальное кольцо $\mathcal{L}_I$ простого идеала I.

Для любого открытого множества U и любой точки $x \in U$ определен естественный гомоморфизм

$$\rho_x^U : \mathcal{F}(U) \to \mathcal{F}_x.$$

Отсюда вытекает, что если $\mathcal{F}$ – пучок, и для элементов $u_1, u_2 \in \mathcal{F}(U)$ равенство

$$\rho_x^U u_1 = \rho_x^U u_2$$

истинно для всех точек $x \in U$, то $u_1 = u_2$.

Таким образом, для пучка $\mathcal{F}$ элементы множества $\mathcal{F}(U)$ могут быть заданы множествами элементов

$$\{u_x \in \mathcal{F}_x | x \in U\}, \tag{6.6}$$

удовлетворяющими следующему условию: для точки $x \in U$ существует такая окрестность W $(W \subseteq U)$ и такая точка $w \in \mathcal{F}(W)$, что

$$u_y = \rho_y^W w$$

для всех точек $y \in W$.

Пусть $\mathcal{F}$ – предпучок, не являющийся пучком. Обозначим через $\mathcal{F}'(U)$ множество всех множеств (6.6), удовлетворяющих указанному выше условию. Вводя отображения

$$\rho_U^V : \{v_x \in \mathcal{F}_x | x \in V\} \to \{v_y \in \mathcal{F}_y | y \in U\} \ (U \subseteq V),$$

мы получим пучок, *ассоциированный с предпучком* $\mathcal{F}$.

6.3. Схемы.

Рассмотрим теперь понятие схемы, охарактеризуем основные свойства схем и выделим те из них, которые являются многообразиями.

6.3.1. Основные понятия.

Окольцованным пространством называется пара $(X, \mathfrak{A}_X)$, где X – топологическое пространство, а $\mathfrak{A}_X$ – пучок колец, называемый *структурным пучком* окольцованного пространства.

Морфизмом окольцованного пространства $(X, \mathfrak{A}_X)$ в окольцованное пространство $(Y, \mathfrak{A}_Y)$ называется такая совокупность, состоящая из непрерывного отображения

$$\varphi : X \to Y$$

и гомоморфизмов

$$\psi_U : \mathfrak{A}_Y(U) \to \mathfrak{A}_X(\varphi^{-1}(U)),$$

определенных для каждого открытого множества $U \subseteq Y$, что для любых открытых множеств $U, V \subseteq Y$ $(U \subseteq V)$ истинно равенство

$$\rho_U^V(\psi_V(\mathfrak{A}_X(\varphi^{-1}(V)))) = \psi_U(\rho_{\varphi^{-1}(U)}^{\varphi^{-1}(V)}(\mathfrak{A}_X(\varphi^{-1}(V)))).$$

Морфизм окольцованного пространства $(X, \mathfrak{A}_X)$ в окольцованное пространство $(Y, \mathfrak{A}_Y)$, как правило, обозначается $\varphi : (X, \mathfrak{A}_X) \to (Y, \mathfrak{A}_Y)$.

Пример 6.9. Любое кольцо $\mathcal{K}$ определяет окольцованное пространство $(\mathtt{Spec}\ \mathcal{K}, \mathfrak{O}_\mathcal{K})$, где $\mathfrak{O}_\mathcal{K}$ – структурный пучек на топологическом пространстве $\mathtt{Spec}\ \mathcal{K}$.

Окольцованное пространство $(\mathtt{Spec}\ \mathcal{K}, \mathfrak{O}_\mathcal{K})$ обозначается $\mathtt{Spec}\ \mathcal{K}$.

Покажем, что любой гоморфизм λ кольца $\mathcal{K}^{(1)}$ в кольцо $\mathcal{K}^{(2)}$ определяет морфизм окольцованного пространства $\mathtt{Spec}\ \mathcal{K}^{(2)}$ в окольцованное пространство $\mathtt{Spec}\ \mathcal{K}^{(1)}$.

Выберем в качестве отображения φ ассоциированное отображение ${}^a\lambda$.

Тогда для любого главного открытого множества $D(b) \subseteq \mathtt{Spec}\ \mathcal{K}^{(1)}$ истинно равенство

$$\varphi^{-1}(D(b)) = D(\lambda(b)).$$

Для любого, не являющегося нильпотентным, элемента b кольца $\mathcal{K}^{(1)}$ отображение

$$\frac{c}{b^n} \to \frac{\lambda(c)}{(\lambda(f))^n}$$

определяет гомоморфизм $\psi_{D(b)}$ кольца

$$\mathcal{K}_b^{(1)} = \mathfrak{O}_{\mathcal{K}^{(1)}}(D(b))$$

в кольцо

$$\mathcal{K}_{\lambda(b)}^{(2)} = \mathfrak{O}_{\mathcal{K}^{(2)}}(\varphi^{-1}(D(b))).$$

А так как гомоморфизмы $\psi_{D(b)}$ могут быть продолжены до гомоморфизмов

$$\psi_U : \mathfrak{O}_{\mathcal{K}^{(1)}}(U)) \to \mathfrak{O}_{\mathcal{K}^{(2)}}(\varphi^{-1}(U)),$$

определенных для любых открытых множеств $U \subseteq \mathtt{Spec}\ \mathcal{K}^{(1)}$, то φ – морфизм окольцованного пространства $\mathtt{Spec}\ \mathcal{K}^{(2)}$ в окольцованное пространство $\mathtt{Spec}\ \mathcal{K}^{(1)}$.

Замечание 6.11. Морфизмы вида ${}^a\lambda$ не исчерпывают множество всех возможных морфизмов окольцованного пространства $\mathtt{Spec}\ \mathcal{K}^{(2)}$ в окольцованное пространство $\mathtt{Spec}\ \mathcal{K}^{(1)}$.

Морфизм φ окольцованного пространства $\mathtt{Spec}\,\mathcal{K}^{(2)}$ в окольцованное пространство $\mathtt{Spec}\,\mathcal{K}^{(1)}$ называется *локальным*, если для любого открытого множества $U \subseteq \mathtt{Spec}\,\mathcal{K}^{(1)}$, любого такого элемента $I^{(2)} \in \mathtt{Spec}\,\mathcal{K}^{(2)}$, что $\varphi(I^{(2)}) \in U$ и любого элемента $f \in \mathfrak{O}_{\mathcal{K}^{(1)}}(U))$ истинна формула

$$f(\varphi(I^{(2)})) = 0 \Leftrightarrow (\psi_U \circ f)(I^{(2)}) = 0.$$

Истинно утверждение: *любой локальный морфизм* φ окольцованного пространства $\mathtt{Spec}\,\mathcal{K}^{(2)}$ в окольцованное пространство $\mathtt{Spec}\,\mathcal{K}^{(1)}$ *единственным образом представим в виде* ${}^a\lambda$, *где* λ – *гомоморфизм кольца* $\mathcal{K}^{(1)}$ *в кольцо* $\mathcal{K}^{(2)}$.

Для любого окольцованного пространства $(X, \mathfrak{A}_X)$ и любого открытого множества $U \subseteq X$, ограничив пучок $\mathfrak{A}_X$ на множество U, мы получим окольцованное пространство $(U, \mathfrak{A}_X|_U)$. Таким образом, открытое множество U может рассматриваться как окольцованное пространство.

Схемой называется такое окольцованное пространство $(X, \mathfrak{A}_X)$, что для каждой точки $x \in X$ существует такая окрестность U_x и такое кольцо $\mathcal{K}$, что окольцованное пространство $(U_x, \mathfrak{A}_X|_{U_x})$ изоморфно окольцованному пространству $\mathtt{Spec}\,\mathcal{K}$ для некоторого кольца $\mathcal{K}$. Указанная окрестность U_x называется *аффинной окрестностью* точки x.

Схема $(X, \mathfrak{A}_X)$ обозначается X, если это не вызывает недоразумений.

Пример 6.10. Для любого кольца $\mathcal{K}$ окольцованное пространство $\mathtt{Spec}\,\mathcal{K}$ является схемой. При этом, для любой точки схемы $\mathtt{Spec}\,\mathcal{K}$ существует аффинная окрестность. Такие схемы называются *аффинными*.

Морфизм схемы X в схему Y определяется как локальный морфизм соответствующих окольцованных пространств.

Схема X, для которой задан морфизм в $\mathtt{Spec}\,\mathcal{K}$ для некоторого кольца $\mathcal{K}$ называется *схемой над кольцом* $\mathcal{K}$. Для любого морфизма схем над кольцом $\mathcal{K}$ все отображения ψ_U являются гомоморфизмами алгебр над кольцом $\mathcal{K}$.

Замечание 6.12. Структурный пучок $\mathfrak{A}_X$ схемы X обладает тем свойством, что для любой точки $x \in X$ его слой $(\mathfrak{A}_X)_x$ является локальным кольцом.

Поэтому локальные свойства аффинных схем автоматически переносятся на произвольные схемы.

Кроме того, на схемы переносятся следующие понятия, определенные для квазипроективных многообразий.

Рациональным морфизмом схемы X в схему Y называется класс эквивалентных морфизмов $\varphi : U \to Y$, где U – открытое плотное множество в X. При этом, морфизмы $\varphi : U \to Y$ и $\varphi : V \to Y$ *эквивалентны*, если они совпадают на $U \cap V$.

Схемы X и Y *эквивалентны*, если у них существуют изоморфные открытые плотные множества.

Схема X называется *нетеровой*, если если для нее существует такое конечное покрытие аффинными открытыми множествами

$$X = \bigcup_{i=1}^{n} U_i,$$

где

$$U_i = \mathtt{Spec}\, \mathcal{K}_i \ (i = 1, \ldots, n),$$

что все кольца $\mathcal{K}_i$ $(i = 1, \ldots, n)$ – нетеровы.

Схема X над кольцом $\mathcal{K}$ называется *схемой конечного типа*, если в указанном выше конечном покрытии каждое кольцо $\mathcal{K}_i$ $(i = 1, \ldots, n)$ – алгебра конечного типа над $\mathcal{K}$.

6.3.2. Операции над схемами.

Возникает вопрос:

Можно ли восстановить схему, зная ее открытое покрытие?

Формально эта задача имеет следующий вид.

Дано. Система схем U_α $(\alpha \in \mathtt{J})$. Такие системы открытых подмножеств $U_{\alpha,\beta} \subseteq U_\alpha$ $(\alpha, \beta \in \mathtt{J})$, что $U_{\alpha,\alpha} = U_\alpha$ для всех $\alpha \in \mathtt{J}$. Система изоморфизмов $\varphi_{\alpha,\beta} : U_{\alpha,\beta} \to U_{\beta,\alpha}$ схем.

Найти. Такую схему X, ее открытое покрытие $X = \bigcup\limits_{\alpha\in\mathtt{J}} V_\alpha$ и систему гомоморфизмов $\psi_\alpha : U_\alpha \to V_\alpha$ $(\alpha \in \mathtt{J})$, что:

1) отображение $\psi_\alpha|_{U_{\alpha,\beta}}$ – изоморфизм схем $U_{\alpha,\beta}$ и $V_\alpha \cap V_\beta$;

2) отображение $\psi_\beta \circ \varphi_{\alpha,\beta} \circ \psi_\alpha^{-1}$ $(\alpha \in \mathtt{J})$ – тождественное отображение на множестве $V_\alpha \cap V_\beta$.

Если эта задача имеет решение, то схема X называется *склеиванием* системы схем U_α $(\alpha \in \mathtt{J})$.

Критерием существования склеивания X системы схем U_α $(\alpha \in \mathtt{J})$ является выполнение следующих трех условий:

1) $\varphi_{\alpha,\alpha} = 1$ для всех $\alpha \in \mathtt{J}$;

2) $\varphi_{\alpha,\beta} \circ \varphi_{\beta,\alpha} = 1$ для всех $\alpha, \beta \in \mathtt{J}$;

3) отображение $\varphi_{\alpha,\beta}|_{U_{\alpha,\beta}\cap U_{\alpha,\gamma}}$ $(\alpha, \beta, \gamma \in \mathtt{J})$ – изоморфизм $U_{\alpha,\beta} \cap U_{\alpha,\gamma}$ и $U_{\beta,\alpha} \cap U_{\beta,\gamma}$, причем

$$\varphi_{\alpha,\gamma}|_{U_{\alpha,\beta}\cap U_{\alpha,\gamma}} = \varphi_{\alpha,\beta}|_{U_{\alpha,\beta}\cap U_{\alpha,\gamma}} \circ \varphi_{\beta,\gamma}|_{U_{\beta,\alpha}\cap U_{\beta,\gamma}} \ (\alpha, \beta, \gamma \in \mathtt{J}).$$

Пример 6.11. Зафиксируем кольцо $\mathcal{K}$. Выделим в кольце частных $\overline{\mathcal{K}[x_0, x_1, \ldots, x_n]}$ подкольца

$$\overline{\mathcal{K}}_i = \mathcal{K}\left[\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}\right] \ (i \in \mathbf{Z}_{n+1})$$

и положим

$$U_i = \mathtt{Spec}\, \overline{\mathcal{K}}_i \ (i \in \mathbf{Z}_{n+1}),$$

$$U_{ij} = D\left(\frac{x_j}{x_i}\right) \ (i, j \in \mathbf{Z}_{n+1}).$$

Ясно, что

$$U_{ij} = \mathtt{Spec}\, \overline{\mathcal{K}}_{i,j} \ (i, j \in \mathbf{Z}_{n+1}),$$

где кольцо $\overline{\mathcal{K}}_{i,j}$ состоит из всех таких элементов

$$\frac{f(x_0, x_1, \ldots, x_n)}{x_i^p x_j^q} \ (p, q \in \mathbf{Z}_+),$$

что $f(x_0, x_1, \ldots, x_n) \in \mathcal{K}[x_0, x_1, \ldots, x_n]$ – однородный многочлен степени $p + q$.

Так как

$$\overline{\mathcal{K}}_{i,j} = \overline{\mathcal{K}}_{j,i} \ (i, j \in \mathbf{Z}_{n+1}),$$

то определен изоморфизм $\varphi_{ij} : U_{ij} \to U_{ji}$, причем выполнены приведенные выше три условия. Поэтому можно построить склеивание $\mathbf{P}^n_{\mathcal{K}}$ системы схем U_i $(i \in \mathbf{Z}_{n+1})$.

Схема $\mathbf{P}^n_{\mathcal{K}}$ называется *проективным пространством* над кольцом $\mathcal{K}$.

Морфизм схем $\varphi : Y \to X$ называется *замкнутым вложением*, если для каждой точки $x \in X$ существует такая аффинная окрестность U, что $\varphi^{-1}(U)$ – афинная схема, а гомоморфизм $\psi : \mathfrak{O}_X(U) \to \mathfrak{O}_Y(\varphi^{-1}(U))$ является эпиморфизмом. При этом сама схема Y называется *замкнутой подсхемой* схемы X.

Замечание 6.13. Замкнутые подсхемы схема $\mathbf{P}^n_{\mathcal{K}}$ называются *проективными схемами* над над кольцом $\mathcal{K}$.

Схема X называется *приведенной*, если кольца $\mathfrak{O}_X(U)$ не имеют нильпотентных элементов. С каждой схемой X может быть сопоставлена приведенная замкнутая подсхема X_{red}, топологическое пространство которой совпадает с X. В схеме X_{red} для любого открытого множества

$U \subseteq X$ кольцо $\mathfrak{O}_{X_{\text{red}}}$ определяется как фактор-кольцо кольца $\mathfrak{O}_X(U)$ по его нильрадикалу.

Рассмотрим схемы X, Y и S, для которых существуют морфизмы $\varphi : X \to S$ и $\psi : Y \to S$ (в этом случае говорят, что X и Y являются схемами над S).

Произведением схем X и Y над S называется такая схема $X \times_S Y$ над S, что:

1) существуют такие морфизмы $p_X : X \times_S Y \to X$ и $p_Y : X \times_S Y \to Y$, что истинно равенство

$$\varphi \circ p_X = \psi \circ p_y;$$

2) для любой такой схемы Z, что существуют такие морфизмы $u : Z \to X$ и $v : Z \to Y$ существует такой морфизм $hZ \to X \times_S Y$, что истинны равенства

$$\begin{cases} u = p_X \circ h \\ v = p_Y \circ h \end{cases}.$$

Замечание 6.14. 1. Морфизмы p_X и p_y называются *проекциями* схемы $X \times_S Y$, соответственно, на схему X и на схему Y.

2. Морфизм h часто представляют в виде

$$h = (u, v).$$

Поэтому когда вместо схем рассматриваются их морфизмы, то схему $X \times_S Y$ называют *расслоенным произведением* морфизмов φ и ψ.

3. Любую схему можно рассматривать как схему над кольцом $\mathcal{Z}$. Поэтому, для любых схем X и Y определено их произведение над кольцом $\mathcal{Z}$. Это произведение обозначается $X \times Y$.

4. Произведение схем ассоциативно, т.е. для любых схем X, Y и Z над S истинно равенство

$$(X \times_S Y) \times_S Z = X \times_S (Y \times_S Z).$$

Диагональю схемы X называют образ такого морфизма

$$\Delta : X \to X \times_S X,$$

что

$$\Delta = (1, 1).$$

Схема X над S называется *отделимой* над S, если ее диагональ замкнута.

Замечание 6.15. Если схема X отделима над кольцом $\mathcal{Z}$, то ее называют *отделимой.*

Понятие схемы дает возможность определить следующую конструкцию, наиболее близкую к квазипроективным многообразиям.

Определение 6.1. *Многообразием* над алгебраически замкнутым полем $\mathcal{K} = (K, +, \cdot)$ называется приведенная отделимая схема конечного типа над $\mathcal{K}$.

Замечание 6.16. Существуют многообразия над алгебраически замкнутым полем, которые нельзя вложить ни в какое проективное пространство

Морфизмом схем называется их морфизм, как схем, а *аффинным многообразием* называется многообразие, являющееся аффинной схемой.

Замечание 6.17. Из определения 6.1 вытекает, что любое многообразие X имеет конечное покрытие

$$X = \bigcup_{i=1}^{n} U_i,$$

где U_i $(i = 1, \ldots, n)$ – аффинные многообразия. Отсюда вытекает, что X имеет конечную размерность.

Если X неприводимо, то все U_i $(i = 1, \ldots, n)$ в X и

$$\dim X = \dim U_i.$$

Кроме того, все U_i $(i = 1, \ldots, n)$ бирационально изоморфны. Поэтому все поля рациональных функций $\mathcal{K}(U_i$ $(i = 1, \ldots, n)$ изоморфны. Поле, получающееся в результате отождествления этих полей, называется *полем рациональных функций* на X и обозначается $\mathcal{K}(X)$.

6.4. Векторные расслоения.

Понятие *векторное расслоение*, тесно связано с понятием морфизма многообразий над S. Глубокая внутренняя связь понятия *векторное расслоение* с понятием *пучек* проявляется, в частности, в том, что для неособого проективного алгебраического многообразия над алгебраически замкнутым полем, определенные на нем категория локально свободных пучков конечного ранга и категория векторных расслоений эквивалентны (см., напр., [31]).

6.4.1. Основные понятия.

Если векторное пространство B_x зависит от точки x непрерывно (в некотором смысле) и, даже голоморфно, когда X есть риманова поверхность или комплексное многообразие, то говорят о непрерывном и голоморфном векторных расслоениях на X.

Формально, определение векторного расслоения имеет следующий вид.

Определение 6.2. Пусть B и X есть топологические пространства, $p : B \to X$ – непрерывное отображение, а каждый слой $B_x = p^{-1}(x)$ $(x \in X)$ наделен структурой n-мерного векторного пространства над полем $\mathcal{K} = (K, +, \cdot)$. Тогда $p : B \to X$ (или $B \to X$, или, еще короче, само B) называют *векторным расслоением* ранга n над X, если для каждой точки $x \in X$ существует открытая окрестность U и гомеоморфизм

$$h : B_U (:= p^{-1}(U)) \to U \times K^n$$

со следующими свойствами:

1) h – послойное отображение, т.е. для каждой последовательности отображений

$$U \overset{p}{\leftarrow} B_U \overset{h}{\to} U \times K^n \overset{pr_U}{\to} U$$

истинно равенство

$$pr \circ h = p;$$

2) для каждой точки $x \in U$ отображение $h|_{B_x}$ является изоморфизмом векторного пространства B_x на $\{x\} \times K^n$.

Замечание 6.18. Мы будем, в основном, рассматривать алгебраические многообразия и морфизмы между ними. Поэтому, в большинстве случаев $p : B \to X$ есть морфизм многообразий, слоями которого в случае линейного расслоения являются векторные пространства.

В случае многообразий над полем вещественных чисел ранг n расслоения иногда называют *размерностью* расслоения, и говорят о вещественных расслоениях размерности n.

Отображение h называют *линейной картой* B над U.

Если $\mathtt{U} = \{U_i\}_{i \in I}$ – открытое покрытие X и $h_i : B_{U_i} \to U \times K^n$ – линейные карты, то семейство $\{h_i\}_{i \in I}$ называют *атласом* расслоения B.

Векторное расслоение B ранга n называют *тривиальным*, когда существует глобальная линейная карта $h : B \to U \times K^n$.

По определению, векторное расслоение локально тривиально. Поэтому в локальных исследованиях понятие векторного расслоения не вносит ничего нового, и играет определенную роль в исследовании глобальных проблем.

Определение 6.3. *Сечением* векторного расслоения $p : B \to X$ называется такой морфизм $s : X \to B$, что $p \circ s = 1$ на X.

Определение 6.4. *Линейным расслоением* (или *расслоением на прямые*) называют векторное расслоение ранга 1.

Замечание 6.19. Пусть E и F – векторные расслоения на топологическом пространстве X.

Естественным образом (с соответствующими модификациями) может быть определено множество гомоморфизмов E в F (обозначается $\mathtt{Hom}(E, F)$), а также двойственное к E расслоение (обозначается E^*). Кроме того, могут быть определены операции: прямая сумма (обозначается $E \oplus F$), тензорное произведение (обозначается $E \otimes F$), m-я внешняя степень расслоениея E (обозначается $\Lambda^m E$).

В частности, если n – ранг расслоения E, то линейное расслоение $\Lambda^n E$, как правило, обозначается $\det E$.

Как обычно, обозначим через

$$\mathcal{GL}(n, \mathcal{K}) = (GL(n, \mathcal{K}), \cdot)$$

группу обратимых $n \times n$-матриц над полем $\mathcal{K}$.

Истинно следующее утверждение.

Утверждение 6.1. Пусть $\mathcal{K}$ есть поле действительных чисел или поле комплексных чисел, $p : B \to X$ – векторное расслоение ранга n над топологическим пространством X, а $h_i : B_{U_i} \to B \times K^n$ $(i \in I)$ – атлас для B. Тогда существуют такие однозначно определенные непрерывные отображения

$$g_{ij} : U_i \cap U_j \to GL(n, \mathcal{K}),$$

что для отображений

$$\varphi_{ij} : h_i \circ h_j^{-1} : (U_i \cap U_j) \times K^n \to (U_i \cap U_j) \times K^n$$

выполнены условия

$$\varphi_{ij}(x, t) = (x, g_{ij}(x)t) \ ((x, t) \in (U_i \cap U_j) \times K^n).$$

Кроме того, над $U_i \cap U_j \cap U_l$ выполняются коциклическое соотношение

$$g_{ij} g_{jl} = g_{il}.$$

Отображения g_{ij} $(i, j \in I)$ называются *функциями перехода*, а семейство $\{g_{ij}\}_{i,j \in I}$ – *коциклом*, соответствующим атласу $\{h_i\}_{i \in I}$.

Рассмотрим случай римановых поверхностей. При изложении этого материала мы следуем [75,107].

Пусть X есть риманова поверхность, $p : B \to X$ – векторное расслоение ранга n над X и

$$\mathtt{H} = \{h_i : B_{U_i} \to U \times \mathbf{C}^n \ (i \in I)\}$$

есть атлас для B.

Атлас $\mathtt{H}$ называют *голоморфным*, если голоморфны все соответствующие ему функции перехода

$$g_{ij} : U_i \cap U_j \to GL(n, \mathcal{K}).$$

Два атласа $\mathtt{H}_1$ и $\mathtt{H}_2$ называют *голоморфно согласованными*, если $\mathtt{H}_1 \cup \mathtt{H}_2$ – атлас.

Легко видеть, что голоморфная согласованность есть отношение эквивалентности. Класс эквивалентности голоморфно согласованных атласов называют *голоморфной линейной структурой*.

Голоморфное векторное расслоение на римановой поверхности X представляет собой векторное расслоение $B \to X$ вместе с голоморфной линейной структурой.

Голоморфное векторное расслоение $B \to X$ называют *голоморфно тривиальным*, если его голоморфная линейная структура содержит атлас, состоящий из одной единственной карты $B \to X \times \mathbf{C}^n$.

Пусть $\mathfrak{O}$ – пучок голоморфных функций на римановой поверхности X, U – открытое множество в X, а

$$\mathcal{GL}(n, \mathfrak{O}(U)) = (GL(n, \mathfrak{O}(U)), \cdot)$$

является группой обратимых $n \times n$-матриц с элементами из $\mathfrak{O}(U)$.

Нетрудно видеть, что группы $\mathcal{GL}(n, \mathfrak{O}(U))$ образуют пучок на X, и существуют однозначно определенные голоморфные отображения

$$g_{ij} : U_i \cap U_j \to GL(n, \mathfrak{O}(U))$$

для которых выполняются коциклические соотношения

$$g_{ij}g_{jl} = g_{il}.$$

Имеет место следующая теорема.

Теорема 6.1. Пусть X есть риманова поверхность, $\mathtt{U} = \{U_i\}_{i\in I}$ – открытое покрытие X, а $\{g_{ij}\}_{i,j\in I}$ – соответствующие коциклы. Тогда существует голоморфное векторное расслоение $p : B \to X$ ранга n и голоморфный атлас

$$\mathtt{H} = \{h_i : B_{U_i} \to U \times \mathbf{C}^n \ (i \in I)\}$$

расслоения B с функциями перехода g_{ij}.

6.4.2. Вещественные касательные расслоения одномерной и двумерной сфер.

Рассмотрим вначале построение касательного расслоения на двумерной сфере

$$S^2 = \{x = (x_1, x_2, x_3) | x_1^2 + x_2^2 + x_3^2 = 1\}.$$

Замечание 6.20. Комплексификация этой сферы дает алгебраическую кривую рода 0.

Открытое покрытие сферы S^2 задается локальными покрытиями (картами) (U_i, φ_i), где

$$U_i = \{x \in S^2 | x_i > 0\} \ (i = 1, 2, 3),$$

$$U_{3+i} = \{x \in S^2 | x_i < 0\} \ (i = 1, 2, 3),$$

$$\varphi_1(x) = (u_1 \ (= x_2), u_2 \ (= x_3)),$$

$$\varphi_2(x) = (v_1 \ (= x_1), v_2 \ (= x_3)),$$

$$\varphi_3(x) = (w_1 \ (= x_1), w_2 \ (= x_2)),$$

а отображения φ_4, φ_5 и φ_6 определяются по симметрии.

Замечание 6.21. Нетрудно убедиться в том, что, например,

$$\varphi_2^{-1}(v_1, v_2) = \left(v_1, \sqrt{1 - v_1^2 - v_2^2}, v_2\right).$$

Остальные обратные отображения определяются аналогичным образом.

Так как

$$\bigcup_{i=1}^{3} U_i = S^2$$

и

$$\bigcup_{i=4}^{6} U_i = S^2,$$

то $\{(U_i, \varphi_i)|i = 1, 2, 3\}$ (соответственно, $\{(U_{i+3}, \varphi_i)|i = 1, 2, 3\}$) являются атласами для S^2.

Пересечение $U_1 \cap U_2$ непусто. Таким образом,

$$\varphi_1(x_1, x_2, x_3) = (u_1, u_2),$$

$$\varphi_2(x_1, x_2, x_3) = (v_1, v_2),$$

и отображение

$$\varphi_1 \circ \varphi_2^{-1}(v_1, v_2) = \left(u_2\,(= v_2), u_1 = \left(\sqrt{1 - v_1^2 - v_2^2}\right)\right)$$

является диффеоморфизмом между $\varphi_1(U_1 \cap U_2)$ и $\varphi_2(U_1 \cap U_2)$. Этот диффеоморфизм называют *координатной заменой на пересечении.*

Рассмотрим связь между локальными покрытиями и стереографической проекцией сферы S^2.

Существуют следующие две карты для стереографической проекции

$$(U_1, \varphi_1) = \left(S^2 \backslash \{(0, 0, 1)\}, \left(\frac{x_1}{1 - x_3}, \frac{x_2}{1 - x_3}\right)\right)$$

и

$$(U_2, \varphi_2) = \left(S^2 \backslash \{(0, 0, -1)\}, \left(\frac{x_1}{1 + x_3}, \frac{x_2}{1 + x_3}\right)\right).$$

Следовательно,

$$U_1 \cap U_2 = \{x \in S^2 |\, |x_3| < 1\}.$$

Пусть (u_1, u_2) и $(v_1, v_2$ есть локальные координаты, соответственно, на U_1 и на U_2. В пересечении $U_1 \cap U_2$ мы имеем

$$\varphi_1^{-1}(u_1, u_2) = \left(\frac{2u_1}{u_1^2 + u_2^2 + 1}, \frac{2u_2}{u_1^2 + u_2^2 + 1}, \frac{u_1^2 + u_2^2 - 1}{u_1^2 + u_2^2 + 1} \right),$$

$$\varphi_2^{-1}(v_1, v_2) = \left(\frac{2v_1}{v_1^2 + v_2^2 + 1}, \frac{2v_2}{v_1^2 + v_2^2 + 1}, \frac{1 - v_1^2 - v_2^2}{v_1^2 + v_2^2 + 1} \right).$$

Таким образом,

$$\varphi_1 \circ \varphi_2^{-1}(v_1, v_2) = (v_1, v_2),$$

$$\varphi_2 \circ \varphi_1^{-1}(u_1, u_2) = (u_1, u_2),$$

т.е. мы получили диффеоморфизмы между $\varphi_1(U_1 \cap U_2)$ и $\varphi_2(U_1 \cap U_2)$.

Вычислим касательные расслоения на одномерной сфере S^1 и на двумерной сфере S^2 (см., напр., [92,118]). В обоих случаях касательные расслоения являются дифференцируемыми многообразиями.

Касательное расслоение TS^1 на S^1 есть прямое произведение $S^1 \times \mathbf{R}$ окружности на вещественную ось.

Следовательно, TS^1 есть тривиальное расслоение и многообразие S^1 параллелизуемое.

Замечание 6.22. Построение касательного расслоения для плоской неособой аффинной кривой Γ, заданной многочленом $F(x, y)$ над полем $\mathcal{K} = (K, +, \cdot)$ осуществляется следующим образом.

Точку $P = (a, b) \in \Gamma$ называют *простой*, если $\mathsf{D}_x F(x, y)|_P \neq 0$ или $\mathsf{D}_y F(x, y)|_P \neq 0$. В этом случае прямую

$$\mathsf{D}_x F(x, y)|_P (x - a) + \mathsf{D}_y F(x, y)|_P (y - b) = 0$$

называют *касательной* к Γ в точке P.

Если все точки кривой Γ простые, то получаем касательное расслоение $T\Gamma$ на Γ.

Касательное расслоение TS^2 на S^2 может быть определено тремя локальными картами в смысле векторных расслоений.

Пусть

$$U_i = \{x \in S^2 | \, |x_i| < 1\} \ (i = 1, 2, 3).$$

Тогда

$$S^2 = \bigcup_{i=1}^{3} U_i.$$

Пусть

$$E = \{(x, t) \in \mathbf{R}^3 \times \mathbf{R}^3 | x \in S^2 \& < x, t >= 0\},$$

где $< x, t >$ – скалярное произведение.

Положив $x = (x_1, x_2, x_3)$ и $t = (u, v, w)$ получим, что гомоморфизмы

$$\Phi_1 : p^{-1}(U_1) \to U_1 \times \mathbf{R}^2,$$

$$\Phi_2 : p^{-1}(U_2) \to U_2 \times \mathbf{R}^2,$$

$$\Phi_3 : p^{-1}(U_3) \to U_3 \times \mathbf{R}^2,$$

определяемые, соответственно, формулами

$$(x_1, x_2, x_3; u, v, w) \mapsto (x_1, x_2, x_3; vx_3 - wx_2, u),$$

$$(x_1, x_2, x_3; u, v, w) \mapsto (x_1, x_2, x_3; wx_1 - ux_3, v),$$

$$(x_1, x_2, x_3; u, v, w) \mapsto (x_1, x_2, x_3; ux_2 - vx_1, w),$$

определяют атлас $\{(U_i, \Phi_i) | i = 1, 2, 3\}$ касательного расслоения TS^2.

Известно, что TS^2 не является тривиальным расслоением и, следовательно, многообразие S^2 не является параллелизуемым.

Приведенные выше расслоения сфер в действительности являются векторными расслоениями. Это означает, что в случае S^2 имеются единственные такие непрерывные отображения

$$g_{ij} : U_i \cap U_j \to GL(2, \mathbf{R}) \ (i, j = 1, 2, 3),$$

что отображения

$$\psi_{ij} = \Phi_i \circ \Phi_j^{-1} : (U_i \cap U_j) \times \mathbf{R}^2 \to (U_i \cap U_j) \times \mathbf{R}^2 \ (i, j = 1, 2, 3)$$

удовлетворяют условию

$$\psi_{ij}(x,y) = (x, g_{ij}(x)y) \ ((x,y) \in (U_i \cap U_j) \times \mathbf{R}^2).$$

В случае TS^2 эти функции переходов g_{ij} имеют вид

$$g_{21}(x) = -\frac{1}{x_2^2 + x_3^2} \begin{pmatrix} x_1x_2 & x_3 \\ -x_3 & x_1x_2 \end{pmatrix},$$

$$g_{32}(x) = -\frac{1}{x_1^2 + x_3^2} \begin{pmatrix} x_2x_3 & x_1 \\ -x_1 & x_2x_3 \end{pmatrix},$$

$$g_{13}(x) = -\frac{1}{x_1^2 + x_2^2} \begin{pmatrix} x_1x_3 & x_2 \\ -x_2 & x_1x_3 \end{pmatrix}.$$

6.4.3. Дивизоры и линейные расслоения.

Пусть многообразие X есть неособая проективная кривая Γ на проективной плоскости $\mathbf{P}^2 = \mathbf{P}^2_{\mathcal{K}}$ над алгебраически замкнутым полем $\mathcal{K} = (K, +, \cdot)$.

Для каждой прямой L, лежащей в проективной плоскости $\mathbf{P}^2$ рассмотрим пересечение $L \cap \Gamma$ прямой L с кривой Γ (которое состоит из конечного множества точек кривой Γ).

Если степень кривой Γ равна d, то Γ имеет с учетом кратности ровно d точек пересечения с прямой L.

Пусть

$$L \cap \Gamma = \sum n_i P_i,$$

где $P_i \in \Gamma$ – различные точки, а n_i – их кратности пересечения.

При изменении L получается семейство дивизоров, параметризованное множеством всех прямых из $\mathbf{P}^2$, т.е. параметризованное множеством $(\mathbf{P}^2)^*$.

Это множество дивизоров называют *линейной системой дивизоров* на кривой Γ.

Дивизор пересечения

$$D = \sum n_i P_i = \sum_{P \in \Gamma} n(P) \cdot P,$$

а также и другие дивизоры на кривой Γ иногда записывают в виде

$$D = \sum n_P \cdot P,$$

где $P \in \Gamma$, полагая $n_P = 0$ для всех P, кроме их конечного числа. Также используют запись $n_P = \nu_P(D)$.

Таким образом,

$$\deg(D) = \sum n_P = \sum \nu_P(D).$$

В частности, для рациональной функции $f \in K(\Gamma)$, дивизор функции f, обозначаемый через (f), определяется как

$$\begin{cases} (f) = \sum\limits_{P \in \Gamma} \nu_P(f) \cdot P \\ \deg(f) = 0 \end{cases}.$$

Пусть теперь X есть риманова поверхность, а D – дивизор на X.

С дивизором D ассоциируют голоморфное линейное расслоение B_D, а также соответствующий пучек голоморфных сечений B_D.

Существуют открытое покрытие $\mathtt{U} = \{U_i\}_{i \in I}$ поверхности X и такие мероморфные функции $\psi_i \in \mathcal{M}(U_i)$ $(i \in I)$, что

$$(\psi_i) = D$$

на множестве U_i. Тогда

$$g_{ij} = \frac{\psi_i}{\psi_j} \ (i, j \in I)$$

на пересечении $U_i \cap U_j$, так как ψ_i и ψ_j имеют те же самые нули и полюса на $U_i \cap U_j$.

Семейство $\{g_{i,j}\}_{i,j \in I}$ образует коцикл и, по теореме 6.1, B_D есть голоморфное линейное расслоение, соответствующее этому коциклу.

Пусть

$$D = \sum n_P \cdot P$$

есть дивизор на компактной римановой поверхности S и

$$\deg(D) = \sum n_P.$$

Если все $n_P = 0$, то полагают $D = 0$.

Дивизор называют *целым* или *эффективным*, если все $n_P \geq 0$, причем только для конечного, не равного нулю, числа показателей истинно неравенство $n_P > 0$. Для таких дивизоров полагают $D > 0$.

Дивизор D_1 *кратен* дивизору D_2, если $D_1 - DE_2$ – целый дивизор.

Голоморфные и мероморфные дифференциалы на римановой поверхности S называют *абелевыми дифференциалами*. С абелевым дифференциалом ω может быть сопоставлен его дивизор (ω) (см., напр., [75]).

Истинна следующая теорема.

Теорема 6.2. (Риман-Рох). Пусть S есть компактная риманова поверхность рода g, D есть дивизор, $r(-D)$ есть размерность векторного пространства $\mathcal{L}(-D)$ мероморфных функций, являющихся кратными дивизора $(-D)$, а $i(D)$ – размерность векторного пространства абелевых дифференциалов на S, кратных дивизору D. Тогда

$$r(-D) = \deg(D) + i(D) - g + 1.$$

Замечание 6.23. В отличие от [75] мы используем аддитивную запись дивизоров, что, безусловно, не влияет на формулировку основного результата – теоремы Римана-Роха. Доказательство аналогично доказательству из [75].

Теорема Римана-Роха распространяется, в частности, на поля алгебраических функций от одной переменной с полем констант $\mathcal{K}$ (см., напр., [75]).

В частности, для кривых рода 1 (эллиптических кривых) над алгебраически замкнутым полем, размерность $r(-D)$ пространства $\mathcal{L}(-D)$ определяется условиями

$$r(-D) = \begin{cases} 0, & \text{если } \deg(D) < 0 \\ 1, & \text{если } \deg(D) = 0 \\ \deg(-D), & \text{если } \deg(-D) \geq 1 \end{cases}.$$

6.4.4. Пучки и векторные расслоения.

В этом пункте мы рассматриваем проективные алгебраические многообразия, определенные на них векторные расслоения и пучки над алгебраически замкнутым полем $\mathcal{K} = (K, +, \cdot)$.

Пусть $B \to X$ есть векторное расслоение над алгебраическим многообразием X, $U \subseteq X$, а $\mathcal{L}_B(U)$ – множество сечений B над U.

Для любых сечений $s_1, s_2 \in \mathcal{L}_B(U)$ истинно равенство

$$(s_1 + s_2)(x) = s_1(x) + s_2(x) \ (x \in U).$$

Кроме того, для каждого $s \in \mathcal{L}_B(U)$ и каждой регулярной функции f на U истинно равенство

$$(fs)(x) = f(x)s(x) \ (x \in U),$$

где $f(x) \in K$ действует на векторном пространстве B_x.

Следовательно, $\mathcal{L}_B(U)$ есть модуль над множеством $\mathfrak{O}_X(U)$ регулярных функций на U, и по множествам $\mathcal{L}_B(U)$ сечений расслоения B определяется локально свободный пучек модулей $\mathbb{B}_B$ над структурным пучком $\mathfrak{O}_X$:

$$\mathbb{B} \cong \bigoplus_{i=1}^{n} \mathfrak{O}_X.$$

Для векторного расслоения B над алгебраическим многообразием X обозначим через $\mathbb{B}$ пучок ростков регулярных сечений B, а через $\mathfrak{V}(B)$ – векторное пространство глобальных регулярных сечений, т.е.

$$\mathfrak{V}(B) = H^0(X, \mathbb{B}).$$

Отметим следующие результаты Ж.-П. Серра о векторных расслоениях над произвольными алгебраическими многообразиями X (теоремы 6.3 и 6.4).

Пусть H есть линейное расслоение, соответствующее дивизору гиперплоского сечения и пусть

$$D(n) = B \otimes H^n,$$

где

$$H^n = \underbrace{H \otimes \cdots \otimes H}_{n}$$

есть тензорное произведение над полем комплексных чисел.

Теорема 6.3. Для достаточно большого числа n (зависящего от расслоения B) канонический гомоморфизм $\mathfrak{V}(B(n)) \to (B(n))_x$ является эпиморфизмом для всех $x \in X$.

Теорема 6.4. Для достаточно большого числа n (зависящего от расслоения B) истинны равенства

$$H^q(X, \mathbb{B}(n)) = 0 \ (q > 0).$$

Если расслоение B таково, что $\mathfrak{V}(B) \to B_x$ есть эпиморфизм, то говорят, что B имеет достаточно сечений.

Векторное расслоение B называют *обильным*, если оно имеет достаточно сечений и если $H^q(X, \mathbb{B}(n)) = 0$ при $q > 0$.

6.4.5. Векторные расслоения и пучки на алгебраических кривых над алгебраически замкнутым полем.

В [105] установлено, что для рациональной кривой любое векторное расслоение есть прямая сумма линейных расслоений.

Случай эллиптических кривых исследован в [85]. Приведем основные результаты для этого случая.

Пусть $\mathcal{B}(r, d)$ есть множество неразложимых векторных расслоений размерности r и степени d над неособой алгебраической кривой Γ.

Теорема 6.5. [85]. Существует такое целое число $n(g, r, d)$, что $B(n)$ обильно для всех $B \in \mathcal{B}(r, d)$ и всех $n \geq n(g, r, d)$.

Теорема 6.6. [85]. Пусть Γ есть эллиптическая кривая с нейтральным элементом (т.е. нулем группового закона) E. Множество $\mathcal{B}(r, d)$ может быть отождествлено с Γ следующим способом:

$$\det : \mathcal{B}(r, d) \to \mathcal{B}(1, d)$$

соответствует $n : \Gamma \to \Gamma$, где

$$n(x) = n \cdot x = \underbrace{x + \cdots + x}_{n}$$

и $n = (r, d)$ есть наибольший общий делитель r и d.

Следствие 6.1. Пусть $n = (r, d) = 1$. Тогда, если $B \in \mathcal{B}(r, d)$, то:

1) соответствие $B \to \det B$ устанавливает взаимно-однозначное соответствие $\mathcal{B}(r, d) \to \mathcal{B}(1, d)$;

2) существует такое линейное расслоение L степени 0, что

$$B \cong \mathcal{B}(r,d)_E \otimes L;$$

3) $\mathcal{B}(r,d)_E \otimes L \cong \mathcal{B}(r,d)_E$ тогда и только тогда, когда $L^r \cong 1$;

4) $(\mathcal{B}(r,d)_E)^* \cong \mathcal{B}(r,-d)_E$.

Теорема 6.6 и следствие 6.1 дают классификацию векторных расслоений на эллиптической кривой.

6.5. Элементы теории одномерных схем.

Рассмотрено вычисление структурного пучка для произвольных коммутативных колец с единицей. Кроме того, результаты теории схем специализируются в направлении схемного расширения понятия алгебраическая кривая и в направлении определения групповых схем. Представленный материал обобщает некоторые результаты, рассмотренные выше. Далее все кольца предполагаются коммутативными и с единицей, отличной от нуля.

6.5.1. $\mathtt{Spec}\,\mathcal{K}$.

Пусть $\mathcal{K} = (K, +, \cdot)$ – коммутативное кольцо с единицей. По кольцу $\mathcal{K}$ определяется топологическое пространство $\mathtt{Spec}\,\mathcal{K}$. Точками этого пространства являются простые идеалы кольца $\mathcal{K}$. Если $\mathfrak{a} \subseteq K$ есть некоторый идеал, то множество

$$V(\mathfrak{a}) = \{\mathfrak{p} \subseteq K | \mathfrak{a} \subseteq \mathfrak{p},\ \mathfrak{p} - \text{ простой идеал}\}$$

называется замкнутым множеством, определяемым $\mathfrak{a}$. Если $x \in \mathtt{Spec}\,\mathcal{K}$, то идеал, соответствующий точке x, обозначаем $\mathfrak{p}_x$. Элементы $f \in K$ могут рассматриваться как функции на $\mathtt{Spec}\,\mathcal{K}$.

Замечание 6.24. Говоря далее о делителях нуля, понимаем под этим собственные делители нуля.

Так как идеал $\mathfrak{p}_x$ – простой, то кольцо $\mathcal{K}/_{\mathfrak{p}_x}$ является целостным, т.е. коммутативным кольцом с единицей без делителей нуля. Пусть $\mathtt{k}(x)$ – поле отношений кольца $\mathcal{K}/_{\mathfrak{p}_x}$. Для каждой точки x определен гомоморфизм $\varphi_x : K \to \mathtt{k}(x)$.

Для $f \in K$ полагают

$$f(x) = \varphi_x(f)\ (\in \mathtt{k}(x)).$$

Так как $\mathcal{K}$ – кольцо, то

$$(f+g)(x) = f(x) + g(x).$$

Равенство $f(x) = 0$ истинно тогда и только тогда, когда $x \in \mathcal{N}$, где

$$\mathcal{N} = \bigcap_{x \in \mathtt{Spec}\ \mathcal{K}} \mathfrak{p}_x$$

представляет собой нильрадикал, т.е. множество всех нильпотентных элементов кольца $\mathcal{K}$.

Существует биекция между множествами $\mathtt{Spec}\,\mathcal{K}$ и $\mathtt{Spec}\,\mathcal{K}/_{\mathcal{N}}$, т.е. теоретико-множественно они совпадают.

$\mathtt{Spec}\,\mathcal{K}$ называется редуцированными, если в кольце $\mathcal{K}$ нет нильпотентных элементов.

В терминах значении функций на $\mathtt{Spec}\,\mathcal{K}$ можно определить топологию. Именно, если $E \subseteq K$, то определяют $V(E)$ как множество всех общих нулей функций из E, т.е.

$$V(E) = \{x \in \mathtt{Spec}\,\mathcal{K} | (f \in E \Rightarrow f(x) = 0) \& f \in \mathfrak{p}_x\}.$$

Множества $V(E)$ (после проверки аксиом топологического пространства) объявляют замкнутыми множествами топологии на $\mathtt{Spec}\,\mathcal{K}$.

Для точки $x \in \mathtt{Spec}\,\mathcal{K}$ определяется ее замыкание. Именно, замыканием $\{\overline{x}\}$ точки x называется множество таких точек $y \in \mathtt{Spec}\,\mathcal{K}$, что $\mathfrak{p}_y \supseteq \mathfrak{p}_x$. Точку x иногда называют общей точкой своего замыкания (например, неприводимая алгебраическая кривая - общая точка точек, лежащих на ней). Если $y \in \{\overline{x}\}$, то y называют специализацией точки x.

Замечание 6.25. Если y есть специализация x, то для всякого $f \in K$

$$f(x) = 0 \Rightarrow f(y) = 0.$$

Топологическое пространство X называется неприводимым, если оно не может быть представлено в виде $X = X_1 \cup X_2$, где X_1, X_2 $(X_1 \neq X_2)$ – непустые замкнутые множества.

Если нильрадинал $\mathcal{N}$ – простой идеал, то $\mathtt{Spec}\,\mathcal{K} = \{\overline{x}\}$. Приводимое топологическое пространство не содержит общих точек.

Выше для идеала I было определено соответствующее ему замкнутое множество $V(I)$. По множеству V соответствующий ему идеал $I(V)$ определяют следующим образом:

$$I(V) = \{f \in K | (\forall x \in V)(f(x) = 0)\}.$$

Истинно следующее равенство

$$I(V(\mathfrak{a})) = \{f \in K | f^n \in \mathfrak{a},\ n > 0\} = \mathfrak{r}(\mathfrak{a}),$$

где $\mathfrak{r}(\mathfrak{a})$ – есть радикал идеала $\mathfrak{a}$.

Таким образом, имеется биективное соответствие между замкнутыми подмножествами $\mathtt{Spec}\,\mathcal{K}$ и радикальными идеалами из $\mathcal{K}$.

Топологическое пространство называют нетеровым, если для всякого замкнутого множества V из $\mathtt{Spec}\,\mathcal{K}$ существует такая конечная цепочка собственных включений

$$V \supset V_1 \supset \cdots \supset V_{n+1} = \emptyset.$$

Если кольцо $\mathcal{K}$ – нетерово, то $\mathtt{Spec}\,\mathcal{K}$ нетерово. Обратное, вообще говоря, места не имеет.

Истинна следующая теорема.

Теорема 6.7. Пусть X есть нетерово топологическое пространство. Тогда существует такое число $n \in \mathbf{N}$, что

$$X = \bigcup_{i=1}^{n} X_i,$$

где X_i $(i = 1, \ldots, n)$ – максимальные неприводимые замкнутые подмножества.

Указанные в теореме 6.7 подмножества X_i $(i = 1, \ldots, n)$ называются неприводимыми компонентами пространства X.

6.5.2. Структурный пучок на $\mathtt{Spec}\,\mathcal{K}$.

Напомним, что предпучном называют контравариантный функтор из категории топологического пространства в категорию множеств.

Так как само топологическое пространство можно рассматривать как категорию, то определено понятие предпучка на топологическом пространстве X. Если $\{U_i\}$ – открытое покрытие X, а $\mathcal{F}$ – предпучок на

X, то можно рассматривать предпучки, в которых все $\mathcal{F}(U_i)$ являются группами, кольцами и т.д., говоря при этом о предпучке групп, колец и т.д.

Например, если каждому $U_i \subseteq X$ мы сопоставляем одно и тоже множество M, то получаем постоянный предпучок M.

Пучки, как известно, выделяют из предпучков следующей аксиомой:

(S) пусть для всякого открытого $U \subseteq X$ и всякого открытого покрытия $U = \cup U_\alpha$ выполняются условия (ρ – есть отображение ограничения):

1) если $\rho^U_{U_\alpha} f_1 = \rho^U_{U_\alpha} f_2$ для $f_1, f_2 \in \mathcal{F}(U)$ и для всех U_α, то $f_1 = f_2$;

2) если для всякого α так выбраны $f_\alpha \in \mathcal{F}(U_\alpha)$, что для всех (α, β)

$$\rho^{U_\alpha}_{U_\alpha \cap U_\beta}(f_\alpha) = \rho^{U_\beta}_{U_\alpha \cap U_\beta}(f_\beta),$$

то существует единственный такой $f \in \mathcal{F}(U)$, что $f_\alpha = \rho^U_{U_\alpha}(f)$.

Элементы множества $\mathcal{F}(U)$ называют сечениями предпучка $\mathcal{F}$ на множестве U.

Если предпучок удовлетворяет аксиоме (S), то его называют пучком.

Построим известным способом по постоянному предпучку $\mathcal{F}_1 = M$ на X постоянный пучок: множество M можно рассматривать как топологическое пространство с дискретной топологией.

Полагаем

$$\mathcal{F}(U) = \{\text{непрерывные функции из } U \text{ в } M\},$$

т.е. локально постоянные функции.

Проверка аксиом пучка демонстрирует их выполнение, тем самым получаем постоянный пучок $\mathcal{F} = \overline{M}$.

Напомним определение структурного пучка на $\mathtt{Spec}\,\mathcal{K}$. Будем различать два случая:

(i) $\mathcal{K}$ – область целостности;

(i) $\mathcal{K}$ – произвольное коммутативное кольцо с единицей.

Рассматриваем последовательно эти случаи.

Случай (i). $\mathcal{K}$ – область целостности, $X = \mathtt{Spec}\,\mathcal{K}$, а $\overline{\mathcal{K}} = (\overline{K}, +, \cdot)$ – кольцо частных кольца $\mathcal{K}$.

Пучок функций $\mathfrak{O}_X$ на X определяют следующим образом. Пусть $U \subseteq X$ открыто в X. Полагаем

$$\mathfrak{O}(U) = \left\{ a \in \overline{K} \middle| (\forall x \in U)(\exists f_x, g_x \in K) \& (g_x(x) \neq 0) \& \left(a = \frac{f_x}{g_x} \right) \right\}.$$

Отметим, что все $\mathfrak{O}(U)$ являются подкольцами поля $\overline{\mathcal{K}}$, причем

$$\mathfrak{O}(\emptyset) = \{0\}.$$

Если $V \subseteq U \subseteq X$, то определены отображения вложения

$$\rho_V^U : \mathfrak{O}(U) \to \mathfrak{O}(V),$$

которые удовлетворяют аксиомам предпучка. Проверка (которую мы опускаем) показывает, что выполняются и аксиомы пучка.

Таким образом, мы получили пучок колец $\mathfrak{O} = \mathfrak{O}_X$ на спектре области целостности, который называют структурными пучком на $\mathtt{Spec}\,\mathcal{K}$.

Вычислим его слои.

Напомним, что слоем $\mathcal{F}_x$ предпучка $\mathcal{F}$ в точке $x \in X$ называют индуктивный предел множеств $\mathcal{F}(U)$ для всякого $x \in U$ относительно системы отображений ρ_V^U $(V \subseteq U)$.

Тем самым $\mathfrak{O}_x$ является локальным кольцом простого идеала $\mathfrak{p}_x$.

Пример 6.12. 1. Пусть $\mathcal{K} = \mathcal{Z}$. Тогда

$$\mathtt{Spec}\ \mathcal{Z} = \{(0)\} \cup \{(p) | p \ - \text{ простое число}\},$$

$$\mathtt{k}(0) = \mathcal{Q},$$

$$\mathtt{k}(p) = \mathcal{Z}/_{(p)} = \mathcal{F}_p,$$

$$\mathfrak{O}_{(0)} = \mathcal{Q},$$

$$\mathfrak{O}_{(p)} = \left\{ p^m \frac{a}{b} \middle| (a,b) = 1 \ \& \ b \not\equiv 0 \ (mod\, p) \ \& \ m \in \mathbf{Z}_+ \right\}.$$

2. Пусть $\mathcal{A}$ – поле и $\mathcal{K} = \mathcal{A}[x]$. Тогда

$$\mathtt{Spec}\ \mathcal{K} = \{(0)\} \cup \{(f) | f \ - \text{ неприводимый многочлен в } \mathcal{A}[x]\},$$

$$\mathtt{k}(0) = \mathcal{A},$$

$$\mathtt{k}((f)) = \mathcal{A}[x]/_{(f)} = \mathcal{A}(\alpha),$$

где α – корень f,

$$\mathfrak{O}_{(0)} = \mathcal{A},$$

$$\mathfrak{O}_{(f)} = \left\{ (f)^m \frac{g}{h} \middle| (g,h) = 1 \ \& \ h \not\equiv 0 \ (mod\, f) \ \& \ m \in \mathbf{Z}_+ \right\}.$$

Отметим, что если $\mathcal{A}$ – алгебраически замкнутое поле, то

$$\mathtt{k}((f)) = \mathcal{A},$$

а

$$\mathtt{Spec}\ \mathcal{A}[x] = \mathbf{A}_1^x$$

является аффинной прямой.

Случай (ii). Пусть $\mathcal{K}$ – коммутативное кольцо с единицей, не являющееся областью целостности. Мультипликативным подмножеством $S \subseteq K$ кольца $\mathcal{K}$ называют подмножество множества K, замкнутое относительно операции умножения.

Вообще говоря, единица может и не принадлежать множеству S, но ниже мы рассматриваем случай, когда единица принадлежит множеству S.

Кольцом частных $\mathcal{K}_S$ кольца $\mathcal{K}$ относительно множества S называют множество

$$K_S = \left\{ \frac{f}{s} \middle| f \in K, \ s \in S \right\},$$

причем

$$\frac{f_1}{s_1} = \frac{f_2}{s_2}$$

тогда и только тогда, когда существует такое $t \in S$, что

$$t(f_1 s_2 - f_2 s_1) = 0.$$

Отметим, что если $0 \in S$, то $K_S = \{0\}$.

Операции $\frac{f_1}{s_1} + \frac{f_2}{s_2}$ и $\frac{f_1}{s_1} \cdot \frac{f_2}{s_2}$ определяются обычным способом.

Существует гомоморфизм

$$h_S = h : K \to K_S,$$

определенный формулой

$$h(f) = \frac{f}{1},$$

который, вообще говоря, не является мономорфизмом, если $\mathcal{K}_S$ содержит делители нуля.

Напомним свойства отображения h:

1) если $s \in S$, то $h(s)$ обратим в $\mathcal{K}_S$;

2) если $a \in K_S$, то $a = \frac{h(f)}{h(s)}$;

3) пусть $\varphi : A \to B$ – гомоморфизм колец, причем такой, что $\varphi(s)$ для всякого s обратим в $\mathcal{B}$. Тогда φ можно пропустить через $\mathcal{A}_S$, т.е. имеет место известная коммутативная диаграмма с единственным $\overline{\varphi}$ (универсальность $\mathcal{A}_S$ относительно гомоморфизмов φ).

Пример 6.13. 1. Пусть $S = \{f^n | f \in K,\ n \in \mathbf{Z}_+\}$. Тогда

$$K_f = \left\{ \frac{g}{f^n} \middle| g \in K,\ n \in \mathbf{Z}_+ \right\},$$

причем если f нильпотентен, то $K_f = \{0\}$.

2. Пусть $S_x = K \backslash \rho_x$, где $x \in \mathtt{Spec}\ \mathcal{K}$. Тогда $K_{S_x} = K_x$.

3. Пусть S – множество регулярных элементов (т.е. не являющихся делителями нуля) кольца $\mathcal{K}$. Тогда $\mathcal{K}$ – полное кольцо частных, а h_S – мономорфизм.

Пучок локальных колец в случае произвольного кольца $\mathcal{K}$ строят следующим образом: $\mathfrak{O}_x = \mathcal{K}_x$, как и в случае области целостности, но

$$\mathfrak{O}(U) \subseteq \prod_{x \in U} K_x,$$

причем

$$\mathfrak{O}(U) = \left\{ \left(a_x \middle| (\exists V_x \subseteq U)(\exists (f_x, g_x))(\forall y \in V_x) \left(a_y = \frac{f}{g} \& g(y) \neq 0 \right) \right) \right\}.$$

Несложная проверка (которую мы опускаем) показывает, что это пучок локальных колец, для которого $\rho_V^U : \mathfrak{O}(U) \to \mathfrak{O}(V)$ есть отображение вида $\prod\limits_{x \in U} K_x \to \prod\limits_{x \in V} K_x$, обозначаемый через $\mathfrak{O}$ или $\mathfrak{O}_X$, слоями которого являются локальные кольца $\mathfrak{O}_x$.

Напомним способом выбора открытых множеств топологии Зарисского на X.

Если $E \subseteq A$, то

$$V(E) = \bigcap_{f \in E} V(f)$$

есть замкнутое множеств. Тогда

$$U = X \backslash V(E) = \bigcup_{f \in E} (X \backslash V(f)) = \bigcup_{f \in E} D(f),$$

где

$$D(f) = \{x | f(x) \neq 0\}$$

называют главными открытыми множествами. По этим множествам строится пучок, причем имеет место равенство

$$\mathfrak{O}(D(f)) = K_f.$$

В частности, если $f = 1$, $D(1) = X$, то $\mathfrak{O}(x) = K$.

Суммируем вышеприведенное в виде следующего утверждения.

Утверждение 6.2. Гомоморфизм колец $\varphi : A \to B$ определяет отображение

$$\varphi^* : \mathtt{Spec}\, \mathcal{B} \to \mathtt{Spec}\, \mathcal{A}.$$

Если $U = D(f) \subseteq \mathtt{Spec}\, \mathcal{A}$, то

$$(\varphi^*)^{-1}(U) = D(\varphi(f)).$$

Отображение

$$\varphi : \left\{ \frac{a}{f^n} \middle| n \in \mathbf{Z}_+ \right\} \to \left\{ \frac{\varphi(a)}{(\varphi(f))^n} \middle| n \in \mathbf{Z}_+ \right\}$$

определяет гомоморфизм $\mathfrak{O}_A(U)$ $(= \mathcal{A}_f)$ в $\mathfrak{O}_B((\varphi^*)^{-1}(U))$ $(\mathcal{B}_{\varphi(f)})$.

6.5.3. Одномерные схемы, плоские и собственные морфизмы.

В терминах алгебраических многообразий алгебраической кривой называют алгебраическое многообразие размерности 1.

Так как теория схем расширяет понятие алгебраического многообразия, то целесообразно рассмотреть в контексте теории схем расширения понятия алгебраическая кривая, и, в частности, эллиптическая кривая.

Рассмотрим $\mathcal{Z}$-схемы X конечного типа. Аналогами алгебраических кривых в этом случае являются одномерные $\mathcal{Z}$-схемы. Как и в случае алгебраических кривых, рассмотрение одномерных схем сводится к рассмотрению неприводимых одномерных схем.

Пусть X – такая неприводимая одномерная схема, $\mathtt{k}(X)$ – поле рациональных функций на X.

Если характеристика $\mathtt{k}(X)$ равна 0, то каждая такая схема изоморфна некоторой аффинной схеме $\mathtt{Spec}\,\mathfrak{O}_K$, где $\mathfrak{O}_K$ – есть кольцо целых поля $\mathtt{k}(X)$. Для различных таких схем сами поля $\mathtt{k}(X)$ являются конечными алгебраическими полями рациональных чисел.

Если характеристика $\mathtt{k}(X)$ не равна 0, то полю $\mathtt{k}(X)$ сопоставляется канонически геометрически неприводимая регулярная проективная кривая с таким полем функций.

Для схемного расширения понятия эллиптической кривой (т.е. понятия, охватывающего более широкие классы объектов, нежели классические алгебраические кривые), нам нужны понятия плоского морфизма, собственного морфизма и понятие комплексного аналитического пространства. Напомним их.

Определение 6.5. Модуль $\mathcal{M}$ над кольцом $\mathcal{K}$ – плоский, если для любого идеала $\mathfrak{a} \subseteq K$ эпиморфизм $\mathfrak{a} \otimes M \to \mathfrak{a}M$, где $a \otimes m \to am$, является изоморфизмом.

Морфизм схем $f : X \to S$ называют плоским, если для всякой точки $x \in X$ кольцо $\mathfrak{O}_x$ плоско как модуль над кольцом $\mathfrak{O}_{f(x)}$. В этом случае также говорят, что схема X плоская над S.

Непосредственным следствием этого определения является следующее утверждение.

Утверждение 6.3. Если кольцо $\mathcal{K}$ является полем $\mathtt{k}$, то модуль $\mathcal{M}$ – плоский.

Морфизм $f : X \to \mathtt{Spec}\,\mathcal{K}$ является плоским. Поэтому схема X является плоской над $\mathtt{Spec}\,\mathcal{K}$.

Кольцо $\mathcal{K}$ можно рассматривать как модуль над самим собой, ввиду коммутативности кольца $\mathcal{K}$, как левый и правый одновременно. Из определения плоского модуля следует, что кольцо $\mathcal{K}$ является плоским

модулем над самим собой. Напомним также, что прямая сумма плоских модулей является плоским модулем. Отсюда вытекает следующее утверждение.

Утверждение 6.4. Свободные модули над $\mathcal{K}$ являются плоскими.

Морфизм схем $f : X \to Y$ называют замкнутым, если образ любого замкнутого множества замкнут. Морфизм называют универсально замкнутым, если он замкнут и для любого морфизма $f : Y' \to Y$ соответствующий морфизм $f' : X' \to Y'$, полученный расширением базы, тоже замкнут.

Морфизм $f : X \to Y$ называют собственным, если он отделим, конечного типа и универсально замкнут.

Пусть $\mathbf{C}^n$ есть линейное n-мерное комплексное пространство с обычной хаусдорфовой топологией, $\Delta = \{|z_i| < 1 | i = 1, \ldots, n\}$ есть полидиск, а $f_1, \ldots, f_m$ – аналитические функции на Δ.

Пусть $V \subseteq \Delta$ есть замкнутое множество, образованное общими нулями функций $f_1, \ldots, f_m$, а $(f_1, \ldots, f_m)$ – идеал, порожденный этими функциями.

Для открытого множества W в Δ и открытого множества U на V, где $U = V \cap W$, определим пучок колец

$$\mathfrak{O}_V(U) = \mathfrak{O}_\Delta(W)/_{(f_1,\ldots,f_m)},$$

где $\mathfrak{O}_\Delta$ – пучок ростков аналитических функций на Δ.

Комплексным аналитическим пространством называют топологическое пространство X с пучком колец $\mathfrak{O}_X$, которое может быть покрыто открытыми множествами, каждое из которых изоморфно, как окольцованное пространство, окольцованному пространству вида

$$(V, \mathfrak{O}_V(U)\ (= \mathfrak{O}_\Delta(W)/_{(f_1,\ldots,f_m)})).$$

Пусть $h : X \to S$ – морфизм схем. Задать групповую схему на X означает задать такие три морфизма схем μ, ε, i, означающих, соответственно, групповой закон

$$\mu : X \times_S X \to X,$$

единичный элемент

$$\varepsilon : S \to X$$

и обратный элемент

$$i : X \to X$$

что

$$\mu \cdot (\mu, 1) = \mu \cdot (1, \mu),$$
$$\mu \cdot (\varepsilon \cdot h, 1) = \mu \cdot (1, \varepsilon \cdot h) = 1,$$
$$\mu \cdot (i, 1) = \mu \cdot (1, i) = \varepsilon \cdot h.$$

Пример 6.14. Пусть $\mathcal{G} = (G, \cdot)$ – конечная группа порядке n, а $\mathcal{K}_1$ – кольцо функций на $\mathcal{G}$ со значениями в коммутативном кольце $\mathcal{K}_2$. Тогда $G = \mathtt{Spec}\ \mathcal{K}_1$ есть конечная коммутативная групповая схема порядка n над кольцом $\mathcal{K}_2$.

Следуя Делиню, определим эллиптическую кривую над комплексным аналитическим пространством S как собственный и плоский морфизм аналитических пространств

$$f : E \to S,$$

снабженный сечением ε, слоями которого являются эллиптические кривые, представленные в разделе 3.

Эллиптическая кривая над S обладает одним и только одним S-групповым законом

$$\mu : E \times_S E \to E,$$

единицей которого является сечение ε.

СПИСОК ЛИТЕРАТУРЫ

1. Алгебраическая теория чисел / Под ред. Дж. Касселс, А. Фрелих. – М.: Мир, 1969. – 483 с.
2. *Антонов А.В.* Оценка вычислительных затрат на функционирование криптосистемы, использующей методы хаотической динамики, при решении задач защиты информации в информационно-коммуникационных системах и сетях // Прикладная радиоэлектроника. – 2007. – № 2. – С. 105-109.
3. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. – М.: Мир, 1979. – 536 с.
4. *Болотов А.А., Гашков С.Б., Фролов А.Б.* Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006. – 280 с.
5. *Боревич З.И., Шафаревич И.Р.* Теория чисел. – М.: Наука, 1985. – 503 с.
6. *Ван дер Варден Б.Л.* Алгебра. – М.: Наука, 1976. – 624 с.
7. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.
8. *Вейль Г.* О равномерном распределении чисел по модулю один. – В кн.: Избранные труды. – М.: Наука, 1980. - С. 58-93.
9. *Виноградов И.М.* Основы теории чисел. – М.: Наука, 1965. – 172 с.
10. *Виноградов И.М.* Метод тригонометрических сумм в теории чисел. – М.: Наука, 1980. - 144 с.
11. *Глазунов Н.М.* Структуры данных и символьные преобразования в некоторых прикладных задачах алгебры и анализа. – В кн.: Труды Международной конференции «Аналитические вычисления на ЭВМ и их применения в теоретической физике». – Дубна: ОИЯИ. – 1983. – С. 102-106.
12. *Глазунов Н.М.* Численно-аналитические вычисления и нестандартные арифметики. – В кн.: Труды Международной конференции «Аналитические вычисления на ЭВМ и их применения в теоретической физике». – Дубна: ОИЯИ. – 1985. – С. 143-148.
13. *Глазунов Н.М., Ковалевич Е.И.* Библиотека программ целочисленной арифметики неограниченной разрядности, и интервальной

арифметики, и их реализация на Ассемблере ЕС ЭВМ. – В кн.: Труды семинара по интервальной математики. – Саратов: ВЦ СГУ. – 1990. – С. 3-9.

14. *Глазунов Н.М., Карпинский Ф.В., Корняк В.В.* Решение задач алгебры, анализа и математической физики на системах аналитических вычислений на ЭВМ // Кибернетика. – 1991. – № 2. – С. 23-29.

15. *Глазунов Н.М.* Конструктивные результаты в вычислении группы Морделла-Вейля эллиптических кривых над Q. – В кн.: Тезисы докладов Международной конференции «Современные проблемы теории чисел», Тула, 1993. – С. 34.

16. *Глазунов Н.М.* On some algebraic curves, their moduli spaces and Zeta Functions. – В кн.: Тезисы докладов: «Украинский математический конгресс». – Киев: Институт математики НАНУ. – 2001. – С. 20.

17. *Глазунов Н.М.* О пространствах модулей, равнораспределенности, оценках и рациональных точках алгебраических кривых // Укр. мат. журнал. – 2001. – Т. 53. – № 9. – С. 1174-1183.

18. *Глазунов Н.М.* Об алгебраических кривых над конечными полями, пространствах модулей и дзета функциях. – В кн.: Труды VII Международного Семинара «Дискретная математика и ее приложения». Ч. II. – М.: МГУ. – 2001. – С. 256-259.

19. *Глазунов Н.М., Постников А.Г.* О существовании рациональных точек на кривой $y^2 = f(x)$ над простым конечным полем. – В кн.: Постников А.Г. Избранные труды. – М.: Физматлит, 2005. – С. 450-453.

20. *Глазунов Н.М.* Методы обоснования арифметических гипотез и компьютерная алгебра // Программирование. – 2006. – № 3. – С.10-16.

21. *Глазунов Н.М., Кравчук И.В.* Компьютерная система для исследования задач распределения значений числовых последовательностей // Проблеми автоматизації та управління. – 2008. – № 1 (23). – С. 278-283.

22. *Глазунов Н.М.* Моделирование числовых последовательностей и меры. – В кн.: Материалы IX Международной научно-технической конференции «АВІА-2009». Т. 1. – Киев: Национальный авиационный университет, 2009. – С. 4.83-4.85.

23. *Глазунов Н.М.* Отображения Клостермана-Хассе и их кодирование. – В кн.: Материалы Международного Семинара «Дискретная математика и ее приложения». Ч. II. – М.: МГУ. – 2010. – 3 с.

24. *Гилл А.* Введение в теорию конечных автоматов. – М.: Наука, 1966. – 272 с.

25. *Гилл А.* Линейные последовательностные машины. – М.: Наука, 1974. – 298 с.

26. *Глушков В.М.* Синтез цифровых автоматов. – М.: Физматлит, 1962. – 476 с.

27. *Гриффитс Ф., Харрис Дж.* Принципы алгебраической геометрии. Т. 1,2. – М.: Мир, 1982. – 862 с.

28. *Гурвиц А., Курант Р.* Теория функций. – М.: Наука, 1968. – 618 с.

29. *Зарисский О., Самюэль П.* Коммутативная алгебра. Т.1. – М.: ИЛ, 1963. – 374 с.

30. *Зарисский О., Самюэль П.* Коммутативная алгебра. Т.2. – М.: ИЛ, 1963. – 438 с.

31. *Касивара М., Шапира П.* Пучки на многообразиях. – М.: Мир, 1997. – 655 с.

32. *Коблиц Н.* Введение в эллиптические и модулярные формы. – М.: Мир, 1988. – 320 с.

33. *Ковалев А.М., Скобелев В.Г.* Два подхода к защите информации: комбинаторика и хаос // Искусственный интеллект. – 2004. – № 3. – С. 806-815.

34. *Ковалев А.М., Скобелев В.Г.* Модели и методы защиты информации на основе комбинаторики и хаоса // Известия Таганрогского радиотехнического университета. – 2004. – № 9. – С. 135-142.

35. *Ковалев А.М., Скобелев В.Г.* Построение поточных шифров над конечными кольцами // В кн.: Труды Международной научно-технической конференции «Интеллектуальные и многопроцессорные системы». – Таганрог, РФ: ТРТУ, 2005. – С.94-101.

36. *Кокс Д., Литтл Дж., О'Ши Д.* Идеалы, многообразия и алгоритмы. – М.: Мир, 2000. – 687 с.

37. *Коробов Н.М.* Тригонометрические суммы и их приложения. –М.: Наука, 1989. – 237 с.

38. *Кузнецов С.П.* Динамический хаос. – М.: Физматлит, 2001. – 296 с.

39. *Курош А.Г.* Лекции по общей алгебре. – М.: Наука, 1973. – 400 с.

40. *Ленг С.* Алгебра. – М.: Мир, 1968. – 564 с.

41. *Ленг С.* Введение в алгебраические и абелевы функции. – М.: Мир, 1976. – 136 с.

42. *Ленг С.* Эллиптические функции. – М.: Наука, 1984. – 312 с.

43. *Ленг С.* Основы диофантовой геометрии. – М.: Мир, 1986. – 446 с.

44. *Мальцев А.И.* Алгебраические системы. – М.: Наука, 1970. – 329 с.

45. *Постников А.Г.* Избранные труды. – М.: Физматлит, 2005. – 512 с.

46. *Постникова Л.П.* Тригонометрические суммы и теория сравнений по простому модулю. – М: МГПИ, 1973. – 140 с.

47. *Рид М.* Алгебраическая геометрия для всех. – М.: Мир, 1991. – 151 с.

48. *Серр Ж.-Р.* Курс арифметики. – М.: Мир, 1972. – 184 с.

49. *Серр Ж.-Р.* Абелевы l-адические представления и эллиптические кривые. – М.: Мир, 1972. – 191 с.

50. *Скобелев В.В.* Исследование структуры множества линейных БПИ-автоматов над кольцом $\mathcal{Z}_{p^k}$ // Доповіді НАНУ. – 2007. – № 10. – С. 44-49.

51. *Скобелев В.В.* Анализ структуры класса линейных автоматов над кольцом $\mathcal{Z}_{p^k}$ // Кибернетика и системный анализ. – 2008. – № 3. – С. 60-74.

52. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАНУ. – 2009. – 479 с.

53. *Скобелев В.В.* Точная формула для числа обратимых матриц над конечным кольцом // Труды ИПММ НАНУ. – 2009. – Т. 18. – С. 155-158.

54. *Скобелев В.В.* «Ленточная теорема» и ее приложения // Прикладная дискретная математика. – 2009. – № 4. – С. 84-89.

55. *Скобелев В.В., Скобелев В.Г.* Анализ автоматов над конечным кольцом // В кн.: Праці Міжнародного симпозіума «Питання оптимізації обчислень (ПОО-XXXV) (Кацівелі, 24-29 вересня 2009 р.), Т.2. – Київ: ІК ім. В.М. Глушкова НАНУ, 2009. – С. 310-315.

56. *Скобелев В.В., Скобелев В.Г.* Анализ нелинейных автоматов с лагом 2 над конечным кольцом // Прикладная дискретная математика. – 2010. – № 1. – С. 68-85.

57. *Скобелев В.В., Скобелев В.Г.* О сложности анализа автоматов над конечным кольцом // Кибернетика и системный анализ. – 2010. – № 4. – С. 17-30.

58. *Скобелєв В.В.* Про деякі властивості кубічних кривих ліній над кільцями // Вісник Київського університету. Серія: фізико-математичні науки, 2011. – Вип. 2. – С. 147-150.

59. *Скобелев В.В.* О двух последовательностях множеств отображений абстрактных множеств в дедекиндовы кольца // Кибернетика и системный анализ. – 2011. – № 5.

60. *Скобелев В.В.* Анализ некоторых отображений множеств в дедекиндовы кольца // Доповіді НАНУ. – 2011. – № 3. – С. 41-45.

61. *Скобелев В.Г., Сухинин В.А.* Шифры на основе систем Спротта // Вестник Томского государственного университета. Приложение – 2007. – № 23. – С. 122-126.

62. *Скобелев В.Г.* О некоторых свойствах нелинейных БПИ-автоматов над кольцом $\mathcal{Z}_{p^k}$ // Прикладная электроника. – 2007. – Т.6. – № 2. – С. 288-299.

63. *Скобелев В.Г., Сухинин В.А.* Идентификация автомата в классе автоматов Спротта // Прикладная дискретная математика. – 2008. – № 1. – С. 131-135.

64. *Скобелев В.Г., Зайцева Э.Е.* Анализ класса легко вычислимых перестановок // Кибернетика и системный анализ. – 2008. – № 5. – С. 12-24.

65. *Скобелев В.Г.* Введение в криптологию: [учебное пособие]. – Донецк: Юго-Восток, 2008. – 175 с.

66. *Скобелев В.Г.* Об одном семействе легко вычислимых перестановок над конечным кольцом // В кн.: Труды VIII Международной конференции «Идентификация систем и задачи управления (SICPRO 09), Москва, Россия, 26-30 января, 2009 г.). – М.: ИПУ РАН, 2009. – С. 1518-1528.

67. *Скобелев В.Г.* Комбинаторно-алгебраические модели в криптографии // Прикладная дискретная математика. Приложение. – 2009. – № 2. – С. 74-114.

68. *Скобелев В.Г.* Анализ задачи параметрической идентификации нелинейных автоматов над конечным кольцом // Проблемы управления и информатики. – 2010. – № 5. – С. 37-41.

69. *Скобелев В.Г.* Восстановление вектора начального состояния нелинейных автоматов над конечным кольцом // Проблемы управления и информатики. – 2010. – № 6. – С. 31-34.

70. *Скобелев В.Г.* Анализ атак на квантовый протокол передачи ключа // Прикладная дискретная математика. – 2008. – № 1. – С. 33-38.

71. *Скобелєв В.Г.* Аналіз автомата Реслера над скінченним кільцем // Вісник Київського університету. Серія: фізико-математичні науки, 2010. – Вип. 4. – С. 177-180.

72. *Скобелев В.Г.* Анализ автомата Спротта над конечным кольцом // Труды ИПММ НАНУ. – 2010. – Т. 21. – С. 194-199.

73. *Скобелев В.Г.* Автоматы над конечным кольцом: неподвижные точки автоматных отображений // Доповіді НАНУ. – 2011. – № 6.

74. *Скобелев В.Г.* О некоторых множествах автоматов над конечными кольцами // Кибернетика и системный анализ. – 2011. – № 2. – С. 27-30.

75. *Спрингер Д.* Введение в теорию римановых поверхностей. – М.: ИЛ, 1961.

76. *Сухинин В.А., Скобелев В.Г.* Эквивалентность состояний систем Спротта // Труды ИПММ НАНУ. – 2007. – Т. 14. – С. 174-186.

77. *Сухинин В.А., Скобелев В.Г.* Алгоритмы и сложность идентификации автоматов Спротта над кольцом $\mathcal{Z}_{p^k}$ // В кн.: Труды VII Международной конференции «Идентификация систем и задачи управления (SICPRO 08), Москва, Россия, 28-31 января, 2008 г.). – М.: ИПУ РАН, 2008. – С. 1107-1153.

78. *Сухинин В.А., Скобелев В.Г.* Автоматизированная система анализа автоматов над конечными кольцами // В кн.: Труды Международной конференции «Моделирование 2008 (Киев, 14-16 мая 2008 г.)», Т.1. – Киев: ИПМЭ НАНУ, 2008. – С. 156-160.

79. *Трахтенброт Б.А., Барздинь Я.М.* Конечные автоматы (поведение и синтез). – М.: Наука, 1970. – 400 с.

80. *Халмош П.* Теория меры. – М.: Физ.-мат. ГИЗ, 1953. – 280 с.

81. *Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.

82. *Шафаревич И.Р.* Основы алгебраической геометрии. Т.1. – М.: Наука, 1988. – 352 с.

83. *Шафаревич И.Р.* Основы алгебраической геометрии. Т.2. – М.: Наука, 1988. – 304 с.

84. *Alexandr J., Yorke J.* // Ergod. Theory Dyn. Syst. – 1984. – 4. – P. 1-23.

85. *Atiyah M.F.* Vector bundles over an elliptic curve // Proc. London Math. Soc. – 1957. – № 7. – P. 414-452.

86. *Blankard F.* // Theor. Comput. Sci. // 1989. – 65. – P. 131-141.

87. *Birch B.J., Swinnerton-Dyer H.P.F.* Notes on elliptic curves I // Journ. Rein. Angew. Math. – 1963. – 212. – P. 7-25.

88. *Birch B.J., Swinnerton-Dyer H.P.F.* Notes on elliptic curves II // Journ. Rein. Angew. Math. – 1965. – 218. – P. 79-108.

89. *Birch B.J.* How the number of points of elliptic curves over a fixed prime field varies // Journ. London Math. Soc. – 1968. – 43. – p. 57-60.

90. *Bose C.* // Ergod. Theory Dyn. Syst. – 1989 – 9. – P. 1-17.

91. *Brown G., Yin Q.* // Ergod. Theory Dyn. Syst. – 2000 – 20. – P. 1275-1285.

92. *Chillingworth D.* Differential topology with a view to applications. – London: Pitman Pub., 2006.

93. *Conway J.H., Sloane N.J.* Sphere packings, lattices and groups. – NY-Berlin: Springer-Verlag, 1988. – 663 p.

94. *Dajani K., Kraailikamp C., Solomyak B.* // Acta Math. Acad. Sci. Hung. – 1996. – 73. P. 97-109.

95. *Glazunov N.M.* Number theory, dynamical systems and distribution of numerical sequenses. – In: Proceedings of International Conference «Fractals in Graz. 2001». – Graz (Austria): Techn. Univ. of Graz. – 2001. – P. 14-15.

96. *Glazunov N.M.* Mirror symmetry: algebraic geometry and special Lagrangian fibrations aspects. – In: Proceedings of International Conference «Symmetry-2001», Part 2. – Kiev: Institute of Mathematics of NAS of Ukraine, 2002. – P. 623-628.

97. *Glazunov N.M.* On algebraic geometric and computer algebra aspects of mirror symmetry. – In Proceedings of International Conference «Computer Algebra and its Applications to Physics». – Dubna (RF): Joint Institute of Nuclear Research. – 2002. – P. 104-113.

98. *Glazunov N.M.* On computational aspects of Fourier-Mukai transform. – In Proceedings of International Conference «Symmetry in Nonlinear Mathematical Physics», Part 3. – 2004. – P. 1087-1093.

99. *Glazunov N.M.* Categorization of Fourier transforms, efficient computation and computing intelligence // Nuclear Instruments&Methods in Physics Research. – 2004. – Vol. 534. – P. 324-328.

100. *Glazunov N.M.* Computer algebra of vector bundles, foliations and zeta functions and a context of noncommutative geometry. – 20 p. http://arXiv.org/abs/math.AG/0101202.

101. *Glazunov N.M.* Homological and homotopical algegra of supersymmetries and integralibity to string theory. – In Proceedings of International Workshop « New Trends in Science and Technology» (NTST 08). – Ankara, 2008. – 6 p. http://ntst08.cankaya.edu.tr/proceedings.

102. *Glazunov N.M.* Homological and homotopical algegra of supersymmetries and integralibity to string theory (introduction and preliminaries) – 12 p. – E-print. Los Alamos arXiv: 0805.4161.

103. *Glazunov N.M.* Transformations: dynamics and complexity. – In: Proceedings of The 3rd Conference on non-linear science and complexity (NSC10). – Ankara (Turkey): Cankaya Univ., 2010. – 4 p.

104. *Glazunov N.M.* Dynamics, coding and entropies. - In: Proceedings of the Fourth World Congress «Aviation in the XXI century». – Kiev: National Aviation Univ., 2010. – 4 p.

105. *Grothendieck A.* Sur la classification des fibres holomorphes sur la sphere de Riemann // Amer. J. Math. – 1956. – 79. – P. 121-138.

106. *Faltings G.* Resent progress in Diophantine geometry // Lecture Notes in Math. – 1991. – № 1525. – P. 78-86.

107. *Forster O.* Lectures on Riemann surfaces. – NY: Springer-Verlag, 1981.

108. *Jenkinson O.* A partial order on $\times 2$-invariant measures // Math. Res. Lett. – 2008. – № 5-6. – P. 893-900.

109. *Katz N.M.* Gauss sums, Klosterman sums, and monodromy groups. – Princeton: Princeton Univ. Press, 1988. – 186 p.

110. *Kitchens B.* Symbolic dynamics. One-sided, two-sided and countable Markov shifts. – Berlin: Springer-Verlag. – 1998. – 253 p.

111. *Kwon, Doyng* The natural extensions of β-transformations which generalize baker's transformations // Nonlinearity. – 2009. – 22. – № 2. – P. 301-310.

112. *Lensta H.W.* Factorizing integers with elliptic curves // Ann. of Math. – 1987. – V. 126. – P. 649-673.

113. *Perry W.* // Acta Math. Acad. Sci. Hung. – 1960. – 11. – P. 477-493.

114. *Reney W.* // Acta Math. Acad. Sci. Hung. – 1957. – 8. – P. 401-416.

115. *Silverman J.* Advanced topics in the arithmetic of elliptic curves. –NY: Springer-Verlag, 1994. – 430 p.

116. *Skobelev V.G.* On complexity of checking of cryptosystems // IEEE East-West Design and Test Workshop (EWDTW'06), Sochi, Russia, September 15-19, 2006: Proceedings. – P. 82-88.

117. *Skobelev V.G.* Fault-tolerant discrete dynamical systems over finite ring // CADSM 2007, Lviv-Polyana, 20-24 February, 2007: IX$^{\text{th}}$ International Conference: Proceedings. – P. 357-361.

118. *Tamura I.* Topology of foliation: an introduction. – Providence: AMS. – 1991.

Підписано до друку 05.05.2011 р. Формат 60х84 1/16.
Ум. друк. арк. 20,25. Друк лазерний. Зам. № 645. Накл. 300 прим.

Надруковано в ТОВ «Цифрова типографія»
Адреса: м. Донецьк, вул. Челюскінців, 291а, тел.: (062) 388-07-31, 388-07-30