

LONDON MATHEMATICAL
SOCIETY STUDENT TEXTS. 12

Undergraduate Algebraic Geometry

MILES REID, Mathematical Institute, University of Warwick

CAMBRIDGE UNIVERSITY PRESS
Cambridge
New York New Rochelle Melbourne Sydney

СОВРЕМЕННАЯ МАТЕМАТИКА

ВВОДНЫЕ КУРСЫ

М. РИД

АЛГЕБРАИЧЕСКАЯ ГЕОМЕТРИЯ ДЛЯ ВСЕХ

Перевод с английского
Б. З. ШАПИРО



МОСКВА «МИР»
1991



ОГЛАВЛЕНИЕ

Предисловие к русскому переводу	5
Предисловие	7
§ 0. Неформальное введение	8
Почему же алгебраическая геометрия? Проблема выбора материала; различные геометрические категории, необходимость привлечения коммутативной алгебры, частично определенная функция; репутация автора. Необходимые предварительные сведения, взаимоотношение курса с различными предметами, список рекомендуемых книг	
Гл. 1. Поиграем с плоскими кривыми	16
§ 1. Плоские коники	16
Общее представление о $\mathbb{P}^2$ и однородных координатах; соотношение между $\mathbb{A}^2$ и $\mathbb{P}^2$; параметризация. Каждая гладкая коника в $\mathbb{P}^2$ изоморфна $\mathbb{P}^1$. Простые случаи теоремы Безу: прямая пересекает кривую степени d в d точках, коника пересекает кривую степени d в $2d$ точках. Линейная система коник, проходящих через точки $P_1, \dots, P_n$.	
§ 2. Кубики и групповой закон	32
Кривая $(y^2 = x(x-1)(x-\lambda))$ не может быть рационально параметризована. Линейные системы $S_d(P_1, \dots, P_n)$; пучок кубик, проходящих через 8 точек «в общем положении». Групповой закон на кубике. «Таинственная» гексаграмма Паскаля.	
Добавление к гл. 1. Кривые и их род	48
Топология неособых плоских комплексных кубик. Неформальное обсуждение рода кривой: топология, дифференциальная геометрия, модули, теория чисел, Морделл—Вейль—Фальтингс.	
Гл. 2. Категория аффинных многообразий	54
§ 3. Аффинные многообразия и Nullstellensatz	54
Нётеровы кольца, теорема Гильберта о базисе; соответствия V и I , неприводимые алгебраические множества, топология Зарисского, формулировка Nullstellensatz. Неприводимая гиперповерхность. Нормализация Нётер и доказательство Nullstellensatz; редукция к случаю гиперповерхности.	
§ 4. Функции на многообразиях	73
Координатное кольцо и полиномиальные отображения, морфизмы и изоморфизмы, аффинные многообразия. Поле рациональных функций и рациональные отображения, доминантные рациональные отображения и композиция рациональных отображений. Стандартные открытые множества. Закон сложения на эллиптической кривой является морфизмом.	

Гл. 3. Приложения	88
§ 5. Проективная и бирациональная геометрии	88
Мотивировка: существуют многообразия, не содержащиеся ни в каком аффинном многообразии. Однородные соответствия V и I . Проективное и аффинное. Примеры: квадратичные поверхности, поверхность Веронезе. Бирациональная эквивалентность, рациональные многообразия. Каждое многообразие бирационально эквивалентно гиперповерхности. Произведения.	
§ 6. Касательное пространство и неособость, размерность	102
Мотивировка: теорема о неявной функции, многообразия и гладкие многообразия. Определение аффинного касательного пространства. Множество неособых точек является плотным. Касательное пространство и m/m^2 , инвариантное определение касательного пространства. Размерность X равна $\text{tr deg}_k k(X)$. Разрешение особенностей с помощью раздутий.	
§ 7. 27 прямых на кубической поверхности	112
Прямые на неособой кубической поверхности S . Доказательство существования прямой методом исключения. Пять пар прямых, пересекающих данную прямую. S рациональна. Классическая конфигурация из 27 прямых. Гессиан. Случай, когда все прямые рациональны.	
§ 8. Заключительные комментарии	125
История и социологический аспект. Выбор тем, высоконаучные комментарии и технические замечания. Вместо предисловия. Благодарности.	
Предметный указатель	143

ББК 22.14
Р49
УДК 512.7

Рид М.
Р49 Алгебраическая геометрия для всех: Пер. с англ. — М.:
Мир, 1991. — 151 с.
ISBN 5-03-001792-5

Автор, известный английский математик, поставил себе целью преодолеть страх математиков перед алгебраической геометрией, подобный страху нематематиков перед математикой. Примеры, задачи, рисунки и мотивировки занимают в книге больше места, чем формальный аппарат теории. Автор осторожно доводит читателя до содержательных результатов теории проективных алгебраических многообразий и оставляет его после критического обсуждения обобщений и обоснований (пучки, схемы и т. п.). Секреты специалистов, обычно сообщаемые лишь ученикам наедине, опубликованы здесь в открытую.

Для математиков всех специальностей от студентов-младшекурсников до алгебраических геометров, а также физиков-теоретиков.

Р 1602050000 — 246
041(01)—91 9 — 91

ББК 22.14

Редакция литературы по математическим наукам

ISBN 5-03-001792-5 (русск.)
ISBN 0-521-35662-8 (англ.)

© Cambridge University Press, 1988
© перевод на русский язык, с авторскими изменениями и дополнениями, Б. З. Шапиро, 1991

ПРЕДИСЛОВИЕ К РУССКОМУ ПЕРЕВОДУ

Алгебраическая геометрия оказала большое влияние на развитие математики. Это объясняется, главным образом, ее тесными связями с другими разделами: анализом (эллиптические, абелевы и автоморфные функции, дифференциальные уравнения), теорией чисел, алгеброй. В последние десятилетия интерес к алгебраической геометрии значительно увеличился в связи с ее многочисленными приложениями к математической физике. Сейчас ее методы применяются не только математиками, но и в многочисленных физических работах.

Круг лиц, интересующихся алгебраической геометрией, очень расширился, но это пока мало отразилось на соответствующей учебной литературе. Существует много прекрасных руководств, в которых излагаются определенные разделы алгебраической геометрии, но, по большей части, — это монографии, использующие довольно сложный математический аппарат и, главное, предполагающие уже некоторые навыки чтения математической литературы. Предлагаемая читателю книга профессора Уорикского университета Майлза Рида «Алгебраическая геометрия для всех» занимает совершенно особое место. Автор — известный специалист в области алгебраической геометрии, один из создателей яркого и быстро развивающегося сейчас направления в этой области. Его книга не ставит цели изложить глубокие результаты и методы алгебраической геометрии, имеющие многочисленные приложения. Зато в ней читатель найдет мотивировки основных понятий, тщательное исследование некоторых ключевых примеров: то, что составляет дух алгебраической геометрии и без понимания чего изучение специальной литературы ничего не дает. Автор не уклоняется от разъяснения вопросов, которые обычно обходят: например, чем в принципе отличаются друг от друга запасы непрерывных, дифференцируемых, аналитических и рациональных функций? Или: зачем вводится проективное пространство?

Первая глава книги — это мост, соединяющий алгебраическую геометрию с элементарной аналитической геометрией. В ней речь идет всего лишь о плоских кривых 2-й и 3-й степени, но уже здесь возникают важные для всей алгебраической геометрии понятия и постановки вопросов. На основе накопленного фактического материала автор может пояснить без доказательств основные свойства

кривых произвольной степени, связанные с понятием рода кривой, которое он обсуждает в его топологическом, дифференциально-геометрическом и теоретико-числовом аспектах. Уже на примере плоских кривых выясняется, что геометрическую интуицию алгебраической геометрии можно поставить на твердую почву, лишь привлекая некоторый алгебраический аппарат. Эти связи исследуются во второй главе. Наконец, в третьей главе демонстрируется эффективность введенной алгебраической техники. Она дает возможность строго определить понятие размерности алгебраического многообразия, особой и неособой точки, касательного пространства, бирационального соответствия. Все эти понятия находят применение в предпоследнем параграфе, где доказывается один из самых известных и красивых результатов алгебраической геометрии: существование 27 прямых на неособой поверхности 3-й степени.

Книга написана ясно, прозрачно и интересно. Она читается легко и с удовольствием. Чтение ее требует самых минимальных математических познаний, которыми обладает студент 3-го курса математических и физических факультетов или технических институтов. Исключением являются, может быть, некоторые простейшие алгебраические понятия: кольца, идеала, поля... С ними легко познакомиться по любому курсу «Высшей алгебры».

Книга М. Рида несомненно облегчит широкому кругу лиц, интересующихся алгебраической геометрией, проникновение в эту область математики.

При подготовке перевода был использован любезно предоставленный автором текст второго английского издания.

И. Р. Шафаревич.

ПРЕДИСЛОВИЕ

В последние годы появилось несколько хороших учебников по алгебраической геометрии для аспирантов или студентов старших курсов, но среди них (насколько мне известно) нет пособия, предназначенного для начального ознакомления с предметом. Эти скромные записки возникли из лекционного курса, который я читал два года подряд для третьекурсников Уорикского университета. Цель их — дать замкнутое введение в алгебраическую геометрию именно на этом уровне.

§ 0. Неформальное введение

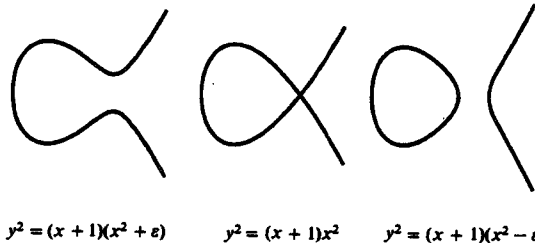
Цель этого параграфа — дать представление о предмете как элементе математической культуры. Логически он не является частью курса, и достаточно его просто бегло пролистать.

(0.1) Грубо говоря, (алгебраическое) многообразие¹⁾ — это совокупность точек, определяемая системой полиномиальных уравнений:

$$V = \{P \in k^n \mid f_i(P) = 0\} \subset k^n,$$

где k — поле, а $f_i \in k[X_1, \dots, X_n]$ — многочлены.

Примерами могут служить плоские кривые $C: (f(x, y) = 0)$ в $\mathbb{R}^2$ или в $\mathbb{C}^2$.



$$y^2 = (x+1)(x^2 + \varepsilon) \quad y^2 = (x+1)x^2 \quad y^2 = (x+1)(x^2 - \varepsilon)$$

При попытке исследовать V сами собой возникают некоторые вопросы.

Теоретико-числовые вопросы. Например, как для $k = \mathbb{Q}$ и $V \subset \mathbb{Q}^n$ найти все точки многообразия V или убедиться в их отсутствии? По ряду исторических причин представляет интерес следующий частный случай: сколько решений имеет уравнение

$$x^n + y^n = 1, \quad x, y \in \mathbb{Q}, \quad n \geq 3?$$

Вопросы такого типа обычно называют *диофантовыми задачами*.

Топологические вопросы. Какова топология многообразия V в наиболее часто встречающихся случаях $k = \mathbb{R}$ или $k = \mathbb{C}$? Очевид-

¹⁾ В этой книге слово «многообразие» (variety) обычно означает «алгебраическое многообразие». Гладкие, топологические и др. многообразия (manifolds) снабжаются соответствующими эпитетами. — Прим. перев.

ными топологическими инвариантами являются, например, компоненты связности изображенных выше кубических кривых.

Вопросы из теории особенностей. Какова топология многообразия V в окрестности точки $P \in V$? Пусть $f: V_1 \rightarrow V_2$ — регулярное отображение одного многообразия в другое (например, полиномиальное отображение $\mathbb{R}^2 \rightarrow \mathbb{R}$); какова топология и геометрия отображения f в окрестности точки $P \in V_1$?

(0.2) Имеются два возможных подхода к изучению многообразий.

Конкретный подход. Для заданных многочленов f_i зачастую нам помогают понять устройство многообразия V те или иные ухищрения, использующие явный вид f_i . Это прекрасно удается, когда размерность n и степени многочленов f_i малы или когда f_i подобраны особенно удачно. Но трудности быстро возрастают, и скоро наступает момент, когда с помощью одной лишь изобретательности в вычислениях продвинуться достаточно далеко не удастся.

Общий подход. Изучение свойств многообразия V сразу подводит нас к таким ключевым понятиям, как регулярные функции на V , неособость, касательные плоскости, размерность многообразия и т. д. Например, то обстоятельство, что кривые, скажем упомянутые выше кубики, одномерны, известно читателю из элементарной геометрии, а что может представлять собой особенность, сразу становится ясным из приведенного выше рисунка.

При написании вводного курса по алгебраической геометрии возникает следующая изначальная проблема: достаточно приемлемое изложение «общего» подхода требует введения такого количества определений, что они заполняют весь курс, вытесняя из него содержательную часть. Таким образом, тут необходим компромисс, и я решил осветить небольшую часть общей теории, постоянно работая с конкретными примерами. Поэтому книга покрывает всего лишь часть основного материала, который следовало бы изложить в систематическом курсе. С другой стороны, я надеюсь, что каждый параграф снабжен достаточным числом упражнений и примеров.

(0.3) Главная особенность алгебраической геометрии — применение исключительно полиномиальных функций (вместе с рациональными). А почему? Рассмотрим на открытом интервале $U \subset \mathbb{R}$ сле-

дующие кольца функций:

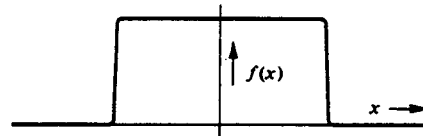
$C^0(U)$ — кольцо всех непрерывных функций $f: U \rightarrow \mathbb{R}$;

$C^\infty(U)$ — кольцо всех гладких (т. е. бесконечно дифференцируемых) функций;

$C^\omega(U)$ — кольцо всех аналитических функций (т. е. сходящихся степенных рядов);

$\mathbb{R}[X]$ — кольцо многочленов, рассматриваемых как полиномиальные функции на U .

Имеют место очевидные включения $\mathbb{R}[X] \subset C^\omega(U) \subset C^\infty(U) \subset C^0(U)$. Эти кольца функций соответствуют важным геометрическим категориям: $C^0(U)$ — категории топологических пространств, $C^\infty(U)$ — гладкой категории (категории гладких многообразий), $C^\omega(U)$ — категории вещественно-аналитических многообразий, $\mathbb{R}[X]$ — категории алгебраических многообразий. Необходимо отметить, что за каждым из этих включений стоят огромные различия, приводящие к несхожести важнейших характерных свойств геометрий в разных категориях. Так, любое введение меры на $C^0(U)$, хотя это и не подчеркивается в начальном курсе анализа, приводит к тому, что гладкие функции будут иметь меру 0 среди непрерывных (более того, если наудачу выбрать непрерывную функцию, то с вероятностью 1 она окажется нигде не дифференцируемой, подобно траектории броуновского движения). Отличие $C^\omega(U)$ от $C^\infty(U)$ можно продемонстрировать на примере поведения функции $f(x) = \exp(-1/x^2)$; это стандартная гладкая функция, ряд Тейлора которой в точке 0 к ней не сходится. Пользуясь ей, можно легко построить гладкую «шапочку» $f: \mathbb{R} \rightarrow \mathbb{R}$, такую, что $f(x) = 1$ при $|x| \leq 0,9$ и $f(x) = 0$ при $|x| \geq 1$.



Гладкая «шапочка»

Аналитическая функция на U , напротив, продолжается (как сходящийся степенной ряд) до функции, комплексно-аналитической в подходящей области в $\mathbb{C}$. Поэтому если $f \in C^\omega(U)$ обращается в нуль на вещественном интервале, то она тождественно равна нулю (согласно результатам из комплексного анализа). Это — одно из проявлений свойства «жесткости», характерного для аналитической геометрии в противоположность дифференциальной топологии.

(0.4) Полиномиальных функций крайне мало, ведь кольцо многочленов $\mathbb{R}[X]$ является счетномерным линейным $\mathbb{R}$ -пространством, тогда как уже кольцо $C^\omega(U)$ несчетно, и даже переход к рациональным функциям (т. е. расширение кольца $\mathbb{R}[X]$ до его поля частных $\mathbb{R}(x)$) дает не слишком много. В разд. (2.2) будет приведен пример «жесткости», характерной для алгебраической геометрии. Возможность построения геометрии, используя только это множество функций, замечательна уже сама по себе, и не удивительно, что при разработке этой теории возникает ряд трудностей:

Построение теории на базе коммутативной алгебры. Топология и дифференциальная топология могут использовать всю совокупность результатов ε - δ -анализа, изучаемого в целом ряде предметов на I и II курсах. В алгебраической геометрии с ее кольцами многочленов нам вместо него придется изучать кольцо $k[X_1, \dots, X_n]$ и его идеалы. Другими словами, вместо математического анализа нам нужно разрабатывать коммутативную алгебру. В качестве типичного примера возьмем Nullstellensatz¹⁾. Несмотря на очевидность ее интуитивного смысла (различные идеалы функций в $k[X_1, \dots, X_n]$ определяют разные многообразия $V \subset k^n$), ее доказательство содержит длинное отступление, связанное с условиями конечности в коммутативной алгебре.

Рациональные отображения и функции. Другой трудностью, возникающей из-за желания работать с многочленами, является необходимость введения «частично определенных» функций. В дальнейшем мы увидим, что в силу упомянутой выше «жесткости» для некоторых (в действительности для всех проективных) многообразий не существует отличной от константы регулярной функции (см. упр. 5.1, 5.12 и обсуждения в разд. (8.10)). Рациональные функции (т. е. «функции» вида $f = g/h$, где g и h — многочлены) не определены там, где знаменатель обращается в нуль. У алгебраических геометров имеется хотя и часто порицаемая, но твердо укоренившаяся традиция использовать термины «рациональная функция» и «рациональное отображение» для обозначения функций и отображений, определенных лишь частично. Таким образом, рациональное отображение $f: V_1 \rightarrow V_2$ вовсе не является отображением; в таких случаях становится также общепринятым употребление стрелки с разры-

¹⁾ Теорему Гильберта о нулях. См. замечание автора и примечание переводчика на стр. 62. — Прим. перев.

вом. (Читателю, у которого это вызывает чувство дискомфорта, я рекомендовал бы сразу прекратить чтение и заняться вместо этого теорией категорий.)

Эта трудность — не такой уж и пустяк. Даже регулярные отображения (или морфизмы, а они-то и являются настоящими отображениями) приходится определять как рациональные отображения, регулярные во всех точках $P \in V$ (т. е., точнее говоря, можно выбрать знаменатель так, чтобы он не обращался в нуль в точке P). С этим же тесно связана сложность внутреннего определения многообразия. В этом курсе (и, насколько мне известно, в других сходных курсах) определяются аффинные многообразия $V \subset \mathbb{A}^n$ и квазипроективные многообразия $V \subset \mathbb{P}^n$, но определение многообразия как такового без апелляции к объемлющему пространству отсутствует. Грубо говоря, многообразием следовало бы считать то, что получается при «склеивании» некоторого числа аффинных многообразий по изоморфным открытым подмножествам. Однако язык, на котором мы в настоящий момент изъясняемся и на котором даже изоморфизм определяется более или менее явно лишь с помощью рациональных функций, слишком груб для этого. Подходящим средством описания этого «склеивания» являются пучки, которые подробно рассматриваются в специальных учебниках.

(0.5) Сказав столько о недостатках алгебраического подхода к геометрии, замечу, что на сегодняшний день почти все важные алгебраические многообразия, возникающие где бы то ни было, являются квазипроективными, и можно их с большим удовольствием изучать, не слишком заботясь о тонкостях определений.

Чисто алгебраические конструкции алгебраической геометрии являются ее наиболее существенными достоинствами: ее можно применять к любому полю, а не только к $\mathbb{R}$ или $\mathbb{C}$. Так, можно рассматривать геометрию над полями характеристики p . Не говорите: «Подумаешь, экая важность — характеристика p . Это же просто конечные поля». Во-первых, на геометрию над конечными полями опираются существенные разделы теории групп, равно как и большие куски из комбинаторики, используемые в информатике. Во-вторых, имеется много интересных бесконечных полей характеристики p . Кроме того, на более глубоком уровне, конечные поля присутствуют и работают в самих $\mathbb{Q}$ и $\mathbb{C}$. Большинство глубоких результатов об арифметике многообразий над $\mathbb{Q}$ существенно используют геометрию над $\mathbb{C}$ или над конечными полями и их алгебраическими замыканиями.

Завершим на этом наше введение. Неформальные обсуждения

будут продолжены в разд. (2.15), а общеобразовательные беседы — в заключительном § 8.

(0.6) Структура книги такова. Главы 1 и 3 предназначены для описания некоторых важных задач, которые можно исследовать средствами алгебраической геометрии. Глава 2 является введением в упоминавшуюся в разд. (0.4) коммутативную алгебру и в категорный язык алгебраической геометрии. (Читатель, склонный к мигрени, может в этой главе принять некоторые из доказательств на веру, так как этот материал стандартен, а профессиональная репутация автора пользуется заслуженным уважением.)

§ 8 содержит всякую всячину, которая может оказаться интересной или полезной читателю, но не укладывается в рамки основного текста, как-то: немного об истории и о социологическом аспекте современной алгебраической геометрии, указания на связь основного материала с более продвинутыми разделами, технические замечания и т. д.

Предварительные сведения, необходимые для этого курса

Алгебра: квадратичные формы, простейшие свойства коммутативных колец и их идеалов, области главных идеалов и однозначное разложение на множители.

Теория Галуа: поля, кольца многочленов, конечные расширения, алгебраические и трансцендентные расширения, сепарабельность.

Топология и геометрия: определение топологического пространства, проективное пространство $\mathbb{P}^n$. (Впрочем, этот вопрос будет подробно рассмотрен далее.)

Математический анализ в $\mathbb{R}^n$: частные производные, теорема о неявной функции. (Впрочем, по мере необходимости я буду напоминать все нужные сведения.)

Коммутативная алгебра: желателен (но не обязателен) опыт работы с коммутативными кольцами.

Взаимоотношения данного курса с различными предметами

Комплексный анализ. Алгебраическая кривая над $\mathbb{C}$ является одномерным комплексным многообразием, а регулярные функции на ней голоморфны. Таким образом, наш курс тесно связан с теорией комплексных функций (даже если эта связь и не всегда очевидна).

Алгебраическая теория чисел. Например, связь с последней теоремой Ферма.

Теория катастроф. Катастрофы являются особенностями, которые практически всегда задаются многочленами, так что изучение геометрии особенностей — это алгебраическая геометрия в чистом виде.

Коммутативная алгебра. Алгебраическая геометрия служит мотивировкой для изучения коммутативной алгебры, а коммутативная алгебра составляет технический аппарат алгебраической геометрии, так что оба этих предмета взаимно обогащают друг друга.

Упражнения к § 0

0.1. (a) Покажите, что x при фиксированных значениях (y, z) является кратным корнем уравнения $x^3 + xy + z = 0$ тогда и только тогда, когда $x = -3z/2y$ и $4y^3 + 27z^2 = 0$;

(b) это уравнение имеет 3 простых корня по x тогда и только тогда, когда $4y^3 + 27z^2 < 0$;

(c) нарисуйте поверхность $S: (x^3 + xy + z = 0)$ в $\mathbb{R}^3$ и ее проекцию на плоскость (y, z) ;

(d) а теперь для проверки загляните в любую книгу или статью по теории катастроф.

0.2. Пусть $f \in \mathbb{R}[X, Y]$ и $C: (f = 0) \subset \mathbb{R}^2$. Назовем точку $P \in C$ *изолированной*, если существует $\varepsilon > 0$, такое, что $C \cap B(P, \varepsilon) = P$. Приведите пример, когда C имеет изолированные точки. Докажите, что если $P \in C$ — изолированная точка, то $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ должна иметь в точке P максимум или минимум, и выведите отсюда, что частные производные $\partial f / \partial x$ и $\partial f / \partial y$ обращаются в точке P в нуль. Это доказывает, что изолированная точка вещественной кривой является особой.

0.3. Кубические кривые. (i) Нарисуйте график функции $y = 4x^3 + 6x^2$ и найдите точки его пересечения с горизонтальными прямыми $y = t$ для целых t в интервале $[-1, 3]$;

(ii) нарисуйте кубические кривые $y^2 = 4x^3 + 6x^2 - t$ для тех же значений t .

Список рекомендуемых книг

Большая часть приведенной ниже литературы является учебниками для студентов-старшекурсников. На некоторые из них в основном тексте имеются ссылки.

Fulton W. Algebraic curves, Springer. (Эта книга является наиболее толковой из серьезных учебников и не требует других пособий. Главы 1–6 вполне могут служить элементарным введением, хотя местами материал изложен сухо.)

Шафаревич И. Р. Основы алгебраической геометрии. — М.: Наука, 1972. (Это — серьезный учебник, но гл. 1 и § 2.1 — вполне подходящий материал для начального курса.)

Гриффитс П., Харрис Дж. Принципы алгебраической геометрии. В 2-х т. — М.: Мир, 1982. (Комплексно-аналитический подход.)

Мамфорд Д. Алгебраическая геометрия. Комплексные проективные многообразия. — М.: Мир, 1979.

Mumford D. Introduction to algebraic geometry. (Эта книга не слишком проста для начального чтения, но она непосредственно подводит к ключевым моментам. Многие алгебраические геометры моего поколения познакомились со своей специальностью по этим заметкам. Недавно она вышла в серии Springer Lectures Notes of Math. 1358 и, таким образом, теперь уже имеется не только в виде маленькой красной книги.)

Kendig K. Elementary algebraic geometry, Springer. (Изучаются взаимоотношения между алгебраической и комплексно-аналитической геометриями.)

Хартсхорн Р. Алгебраическая геометрия. — М.: Мир, 1982. (Настольная книга профессиональных алгебраических геометров, включающая в себя намного более сложный материал. Содержание гл. 1 можно рассматривать как начальный курс в очень сжатой форме.)

Берже М. Геометрия, тт. 1 и 2. — М.: Мир, 1984. (Особенно существенны некоторые сведения из параграфов в ч. 4 о квадратичных формах и квадриках.)

Атья М., Макдональд И. Введение в коммутативную алгебру. — М.: Мир, 1972. (Прекрасный учебник.)

Kunz E. Introduction to commutative algebra and algebraic geometry, Birkhäuser.

Matsumura H. Commutative ring theory, Cambridge. (Более углубленный курс коммутативной алгебры.)

Mumford D. Curves and their jacobians. Univ. of Michigan Press. (Эти лекции предназначены для широкого круга читателей, но сложность материала в них быстро возрастает.)

Клеменс Г. Мозаика теории комплексных кривых. — М.: Наука, 1984. (Содержит много интересного.)

Brieskorn E., Knörrer H. Plane algebraic curves, Birkhäuser.

Beauville A. Complex algebraic surfaces, LMS Lecture Notes, Cambridge. (Имеется также издание на французском языке в серии Astérisque.)

Kollár J. The structure of algebraic threefolds: An introduction to Mori's program, Bull. Amer. Math. Soc., v. 17 (1987), p. 211–273. (Прекрасный путеводитель по одной из активно развивающихся областей.)

Semple J. G., Roth L. Introduction to algebraic geometry, Oxford. (Прекрасный старый учебник, содержащий много информации, но в нем постоянно ощущается недостаток строгости.)

Coolidge J. L. Treatise on algebraic plane curves, Oxford and Dover.

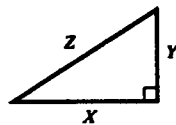
Глава 1

ПОИГРАЕМ С ПЛОСКИМИ КРИВЫМИ

§ 1. Плоские коники

Для мотивировки определения проективной плоскости займемся геометрией коник. Проективная геометрия впервые появляется на втором курсе в лекциях по геометрии. Напомню некоторые основные положения, делая упор на однородных координатах, но никак не затрагивая геометрию линейных подпространств и двойное отношение. Главная задача студента заключается в том, чтобы получить представление, как геометрические идеи (например, мысль о том, что «точки на бесконечности» соответствуют асимптотическим направлениям кривых) выражаются через координаты. Привлекательной чертой алгебраической геометрии является взаимодействие интуитивной геометрической картины (подсказывающей, чего следует ожидать) с точной формулировкой в координатах (позволяющей извлечь из интуиции пользу).

(1.1) **Пример параметризованной кривой.** Теорема Пифагора гласит, что в прямоугольном треугольнике



$X^2 + Y^2 = Z^2$, как, например, в треугольниках (3, 4, 5) и (5, 12, 13) (что было известно каждому древнему египтянину).

Как найти все целые решения этого уравнения? Оно однородно, и, следовательно, пары чисел $x = X/Z$, $y = Y/Z$ образуют окружность $C: (x^2 + y^2 = 1) \subset \mathbb{R}^2$, которая, как легко убедиться, может быть параметризована следующим образом:

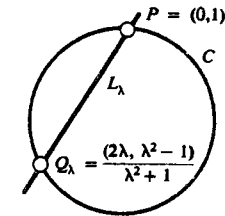
$$x = 2\lambda/(\lambda^2 + 1), \quad y = (\lambda^2 - 1)/(\lambda^2 + 1),$$

где $\lambda = x/(1 - y)$. Это и задает все решения:

$$X = 2lm, \quad Y = l^2 - m^2, \quad Z = l^2 + m^2,$$

где $l, m \in \mathbb{Z}$ взаимно просты. (Если и l и m нечетны, то все переменные следует разделить на 2.) Заметим, что из однородности уравнения вытекает, что если (X, Y, Z) — решение, то $(\lambda X, \lambda Y, \lambda Z)$ также является решением.

Возможно, эта параметризация уже известна читателю из школьной программы. Как бы то ни было, в ее справедливости легко убедиться. Однако если вы с ней не были знакомы, то можете легко ее получить с помощью простой геометрической конструкции, а именно линейным проектированием из данной точки:



Пусть $P = (0, 1) \in C$ и $\lambda \in \mathbb{Q}$ — произвольное рациональное число. Тогда прямая L_λ , имеющая угловой коэффициент $-\lambda$ и проходящая через точку P , пересекает C еще в одной точке Q_λ . Этот способ построения отображения с помощью линейного проектирования неоднократно встретится нам в дальнейшем.

(1.2) **Аналогичный пример.** $C: (2X^2 + Y^2 = 5Z^2)$. Тот же метод приводит к параметризации $\mathbb{R} \rightarrow C$, задаваемой формулами

$$x = \frac{2\sqrt{5}\lambda}{1 + 2\lambda^2}, \quad y = \frac{2\lambda^2 - 1}{1 + 2\lambda^2}.$$

Эта параметризация позволяет получить полную информацию о вещественных точках кривой C ; в вещественном случае между этим примером и предыдущим нет существенных различий. А как обстоит дело в случае рациональных коэффициентов?

Предложение. Если рациональные числа $a, b, c \in \mathbb{Q}$ удовлетворяют уравнению $2a^2 + b^2 = 5c^2$, то $(a, b, c) = (0, 0, 0)$.

Доказательство. Умножив (в случае необходимости) числа a, b и c на их общий знаменатель и разделив на их общий множитель, сведем задачу к случаю, когда a, b, c — целые числа, не все кратные 5. Кроме того, если $5|a$ и $5|b$, то $25|5c^2$, т. е. $5|c$, что противоречит сделанному предположению. Теперь, рассматривая значения

a и b по модулю 5, мы легко приходим к противоречию. Действительно, так как любой квадрат сравним по модулю 5 с 0, 1 или 4, то для сравнения по модулю 5 выражения $2a^2 + b^2$ имеются следующие возможности: $0 + 1$, $0 + 4$, $2 + 0$, $2 + 1$, $2 + 4$, $8 + 0$, $8 + 1$ или $8 + 4$. Однако ни одно из этих чисел не может быть представлено в виде $5c^2$. Ч.т.д.

Заметим, что приведенное рассуждение является чисто арифметическим.

(1.3) Коники в $\mathbb{R}^2$. Коникой в $\mathbb{R}^2$ называется плоская кривая, задаваемая квадратным уравнением:

$$q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

Все читатели заведомо знакомы с классификацией невырожденных коник:

(a) эллипс

(b) парабола

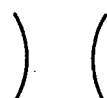
(c) гипербола



$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$



$$y = mx^2$$



$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

кроме них имеется еще ряд вырожденных случаев:

(d) изолированная точка, задаваемая уравнением $x^2 + y^2 = 0$;

(e, f, g) пустое множество, задаваемое одним из следующих трех уравнений: (e) $x^2 + y^2 = -1$, (f) $x^2 = -1$ или (g) $0 = 1$. Эти три уравнения различны, хотя в $\mathbb{R}^2$ они определяют одно и то же множество нулей. (Рассмотрите, например, множество их комплексных решений.)

(h) прямая $x = 0$;

(i) пара пересекающихся прямых $xy = 0$;

(j) параллельные прямые $x(x - 1) = 0$;

(k) «двойная прямая» $x^2 = 0$.

Последний случай:

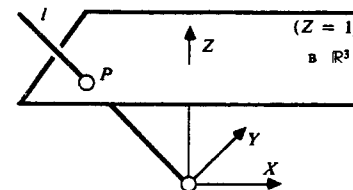
(l) плоскость, задаваемая уравнением $0 = 0$, его вы можете включать или не включать по своему усмотрению.

(1.4) Проективная плоскость. Определение «с потолка»:

$$\begin{aligned} \mathbb{P}_{\mathbb{R}}^2 &= \{\text{прямые в } \mathbb{R}^3, \text{ проходящие через начало координат}\} = \\ &= \{\text{отношения } X:Y:Z\} = \\ &= (\mathbb{R}^3 \setminus \{0\}) / \sim, \text{ где } (X, Y, Z) \sim (\lambda X, \lambda Y, \lambda Z), \\ &\text{если } \lambda \in \mathbb{R} \setminus \{0\}. \end{aligned}$$

(Искушенному читателю не составит труда перенести это определение со случая $\mathbb{R}^3$ на произвольное векторное пространство над любым полем и перейти от явных формул, записанных в выбранной системе координат, к бескоординатным формулировкам.)

Для того чтобы представить отношение $X:Y:Z$ для $Z \neq 0$, достаточно положить $x = X/Z$ и $y = Y/Z$. Этим мы упрощаем рассмотрения, так как исходное отношение задается теперь парой вещественных чисел. Другими словами, класс эквивалентности троек (X, Y, Z) по отношению $\sim$ имеет единственный представитель $(x, y, 1)$, третья координата которого равна 1. К сожалению, Z все-таки может обращаться в нуль, и в этом случае наш способ выбора представителя класса эквивалентности не годится. Приведенное рассуждение показывает, что $\mathbb{P}_{\mathbb{R}}^2$ содержит экземпляр пространства $\mathbb{R}^2$. Прямая общего положения в $\mathbb{R}^3$, проходящая через 0, не содержится в плоскости $(Z = 0)$ и, значит, пересекает плоскость $(Z = 1)$ в единственной точке, которая и представляет этот класс эквивалентности (см. рисунок).



$$\mathbb{R}^2 \hookrightarrow \mathbb{R}^3 \setminus \{0\} \rightarrow \mathbb{P}_{\mathbb{R}}^2 \text{ по формуле } (x, y) \mapsto (x, y, 1)$$

Прямые, лежащие в плоскости $(Z = 0)$, не пересекают плоскость $(Z = 1)$. Следовательно, они соответствуют не точкам из $\mathbb{R}^2$, а *асимптотическим направлениям* или пучкам параллельных прямых в $\mathbb{R}^2$. Таким образом, читатель может представлять себе, что $\mathbb{P}_{\mathbb{R}}^2$ состоит из плоскости $\mathbb{R}^2$, к которой добавлено по одной «точке на бесконечности» для каждого пучка параллельных прямых. При такой точке зрения выкладки следует проводить в $\mathbb{R}^2$, затем с помощью каких-нибудь «асимптотических» соображений постараться угадать, что происходит на бесконечности, и, наконец (в случае необходимости), доказать свою догадку с помощью однородных координат. Определение с помощью прямых в $\mathbb{R}^3$ придает всему более респектабельный вид, так как при таком определении все точки в $\mathbb{P}_{\mathbb{R}}^2$ равноправны.

Группы преобразований занимают в геометрии центральное положение. Свойства геометрической фигуры представляют интерес

лишь тогда, когда они инвариантны относительно соответствующего типа преобразований. *Аффинная* замена координат в $\mathbb{R}^2$ имеет вид $T(x) = Ax + B$, где $x = (x, y) \in \mathbb{R}^2$, A — обратимая 2×2 -матрица, а B — вектор сдвига. Если матрица A ортогональна, то преобразование T является *евклидовым*. Известно, что любая невырожденная коника приводится евклидовым преобразованием к одной из указанных выше форм (а)—(с). В качестве упражнения покажите, что произвольная коника приводится аффинным преобразованием к одной из форм (а)—(л).

Проективное преобразование проективной плоскости $\mathbb{P}^2_{\mathbb{R}}$ имеет вид $T(X) = MX$, где M — обратимая 3×3 -матрица. Легко определить действие этого преобразования на аффинном куске $\mathbb{R}^2 \subset \mathbb{P}^2_{\mathbb{R}}$. Оно совпадает с частично определенным преобразованием $\mathbb{R}^2 \rightarrow \mathbb{R}^2$, а именно с дробно-линейным преобразованием

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \left(A \begin{bmatrix} x \\ y \end{bmatrix} + B \right) / (cx + dy + e),$$

где

$$M = \begin{bmatrix} A & B \\ c & d & e \end{bmatrix}.$$

При $cx + dy + e = 0$ T , разумеется, не определено. Проективные преобразования могут показаться не слишком наглядными; однако они встречаются в реальной жизни. Так, две различные фотографии одного и того же (плоского) объекта связаны проективным преобразованием (см., например, рисунки в книге [Берже, 4.7.4]). Выпускник математической специальности, занимающийся работой по расшифровке фотографий со спутников (будь то в мирных целях для Министерства лесного хозяйства или в рамках открывающей большие перспективы для карьеры рейгановской политики стратегической оборонной инициативы), будет тратить большую часть своего времени, вычисляя проективные преобразования.

Проективные преобразования неявно используются на протяжении всей книги, что обычно маскируется словами «выбрав подходящим образом координаты, можно считать, что...».

(1.5) **Уравнение коники.** Неоднородный квадратный многочлен

$$q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$$

соответствует однородному квадратному многочлену

$$Q(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2.$$

Это соответствие можно воспринимать как способ преобразования

или как биекцию $q \leftrightarrow Q$, заданную формулами

$$q(x, y) = Q(X/Z, Y/Z, 1), \text{ где } x = X/Z, y = Y/Z,$$

и, в обратную сторону,

$$Q = Z^2 q(X/Z, Y/Z).$$

Коникой $C \subset \mathbb{P}^2$ называется кривая $C: (Q(X, Y, Z) = 0)$, где Q — однородный квадратный многочлен. Заметим, что соотношение $Q(X, Y, Z) = 0$ корректно определено на классах эквивалентности, так как $Q(\lambda X) = \lambda^2 Q(X)$ для любого $\lambda \in \mathbb{R}$. В качестве упражнения покажите, что ограничение проективной кривой C на аффинный кусок $\mathbb{R}^2$ совпадает с аффинной коникой, задаваемой условием $q = 0$.

«Бесконечная удаленная прямая» и асимптотические направления. Точки из $\mathbb{P}^2$, для которых $Z = 0$, соответствуют отношениям вида $(X:Y:0)$. Эти точки образуют «бесконечно удаленную прямую», являющуюся экземпляром проективной прямой $\mathbb{P}^1_{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ (так как отображение $(X:Y) \mapsto X/Y$ задает биекцию $\mathbb{P}^1_{\mathbb{R}} \rightarrow \mathbb{R} \cup \{\infty\}$).

По определению прямая L на $\mathbb{P}^2$ задается уравнением $aX + bY + cZ = 0$, и L проходит через точку $(X, Y, 0)$ тогда и только тогда, когда $aX + bY = 0$. В аффинных координатах та же прямая задается уравнением $ax + by + c = 0$, так что все прямые с одним и тем же отношением $a:b$ проходят через одну точку на бесконечности. Это явление описывается словами: «Параллельные прямые пересекаются на бесконечности».

Примеры. (а) Гипербола $(x^2/a^2 - y^2/b^2 = 1)$ в $\mathbb{R}^2$ соответствует в $\mathbb{P}^2_{\mathbb{R}}$ кривой $C: (X^2/a^2 - Y^2/b^2 = Z^2)$. Ясно, что это кривая пересекает прямую $(Z = 0)$ в двух точках $(a, \pm b, 0) \in \mathbb{P}^2_{\mathbb{R}}$, соответствующих очевидным образом асимптотам гиперболы.

Заметим, что аффинными координатами в аффинном куске $(X \neq 0)$ на $\mathbb{P}^2_{\mathbb{R}}$ являются $u = Y/X$, $v = Z/X$. Таким образом, в этом куске кривая C является эллипсом $(u^2/b^2 + v^2 = 1/a^2)$. (В упр. 1.7 читателю предлагается взглянуть на это глазами художника.)

(б) Парабола $(y = mx^2)$ в $\mathbb{R}^2$ соответствует в $\mathbb{P}^2_{\mathbb{R}}$ кривой $C: (YZ = mX^2)$; эта кривая пересекает прямую $(Z = 0)$ в единственной точке $(0, 1, 0)$. Значит, в $\mathbb{P}^2$ «две ветви параболы пересекаются на бесконечности». Заметим, что это утверждение интуитивно содержательно (может быть, вам это покажется неправдоподобным?). Однако прийти к нему, рассматривая ситуацию изнутри $\mathbb{R}^2$,

невозможно. Не исключено даже, что там это утверждение просто не имеет смысла.

(1.6) Классификация коник в $\mathbb{P}^2$. Пусть k — поле произвольной характеристики, отличной от 2. Напомним два результата из линейной алгебры квадратичных форм:

Предложение А. *Имеет место следующая естественная биекция:*

$$\left\{ \begin{array}{l} \text{однородные} \\ \text{квадратичные} \\ \text{многочлены} \end{array} \right\} = \left\{ \begin{array}{l} \text{квадратичные} \\ \text{формы} \\ k^3 \rightarrow k \end{array} \right\} \xleftrightarrow{\text{биекция}} \left\{ \begin{array}{l} \text{симметричные} \\ \text{билинейные} \\ \text{формы в } k^3 \end{array} \right\},$$

задаваемая формулой

$$aX^2 + 2bXY + cY^2 + 2dXZ + 2eYZ + fZ^2 \leftrightarrow \begin{bmatrix} a & b & d \\ b & c & e \\ d & e & f \end{bmatrix}.$$

Квадратичная форма невырождена, если невырождена соответствующая билинейная форма, т. е. невырождена ее матрица.

Теорема В. Пусть V — векторное пространство над k и $Q: V \rightarrow k$ — квадратичная форма. Тогда в V существует такой базис, что

$$Q = \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \dots + \varepsilon_n x_n^2,$$

где $\varepsilon_i \in k$.

[Это доказывается с помощью процесса ортогонализации Грама—Шмидта (если вам эти слова о чем-либо говорят).] Очевидно, что для $\lambda \in k \setminus \{0\}$ замена $x_i \mapsto \lambda x_i$ переводит ε_i в $\lambda^{-2} \varepsilon_i$.

Следствие. Любая коника в $\mathbb{P}_{\mathbb{R}}^2$ в подходящей системе координат приводится к одной из следующих форм:

- (α) невырожденная коника, $C: (X^2 + Y^2 - Z^2 = 0)$;
- (β) пустое множество, задаваемое уравнением $X^2 + Y + Z^2 = 0$;
- (γ) пара прямых, задаваемая уравнением $X^2 - Y^2 = 0$;
- (δ) точка $(0, 0, 1)$, задаваемая уравнением $X^2 + Y^2 = 0$;
- (ε) двойная прямая, задаваемая уравнением $X^2 = 0$.

В этот список можно по желанию включить и всю плоскость $\mathbb{P}_{\mathbb{R}}^2$, заданную уравнением $0 = 0$.

Доказательство. Любое вещественное число ε либо равно 0, либо является квадратом с точностью до знака. Следовательно, как

и в предыдущей теореме, нам достаточно рассмотреть только случай, когда коэффициенты многочлена Q равны $\varepsilon_i = 0, \pm 1$. Кроме того, так как нас интересует только множество точек ($Q = 0$), то Q можно умножать на -1 . Эти соображения сразу приводят к указанному списку. Ч. т. д.

По поводу этого следствия необходимо сделать два замечания. Во-первых, приведенный список намного короче списка из разд. (1.3); например, три невырожденных случая (эллипс, парабола, гипербола) из (1.3) соответствуют случаю (α), кроме того, случаи пар параллельных и пересекающихся прямых с проективной точки зрения также не различаются. Во-вторых, этот список получается из общих алгебраических соображений намного проще.

(1.7) Параметризация коники. Пусть C — невырожденная непустая коника на $\mathbb{P}_{\mathbb{R}}^2$. Тогда, согласно следствию (1.6), кривая C проективно эквивалентна кривой $(XZ = Y^2)$ (в новых координатах $(X + Z, Y, Z - X)$), т. е. кривой, параметризуемой отображением

$$\begin{aligned} \Phi: \mathbb{P}_{\mathbb{R}}^1 &\rightarrow C \subset \mathbb{P}_{\mathbb{R}}^2, \\ (U: V) &\mapsto (U^2: UV: V^2). \end{aligned}$$

Замечание 1. Обратное отображение $\Psi: C \rightarrow \mathbb{P}_{\mathbb{R}}^1$ задается соответствием $(X:Y:Z) \mapsto (X:Y) = (Y:Z)$. Отношение в левой части определено при $X \neq 0$, а отношение в правой части — при $Z \neq 0$. Согласно терминологии, которую мы введем позже, Φ и Ψ являются взаимно обратными изоморфизмами многообразий.

Замечание 2. На протяжении § 1, 2 молчаливо предполагается, что непустые невырожденные коники проективно эквивалентны кривой $(XZ = Y^2)$; над полем характеристики $\neq 2$ это обосновывается в упр. 1.5. (Читатель, интересующийся характеристикой 2, должен считать это определением невырожденности коники.)

(1.8) Однородные формы от двух переменных. Пусть $F(U, V)$ — ненулевой однородный многочлен степени d от переменных U и V с коэффициентами в заданном поле k (следуя традиции, будем для обозначения однородных многочленов использовать термин «форма»):

$$F(U, V) = a_d U^d + a_{d-1} U^{d-1} V + \dots + a_i U^i V^{d-i} + \dots + a_0 V^d.$$

Очевидно, что с F связан неоднородный многочлен от одной переменной

$$f(u) = a_d u^d + a_{d-1} u^{d-1} + \dots + a_i u^i + \dots + a_0.$$

Ясно, что для всех $\alpha \in k$

$$f(\alpha) = 0 \Leftrightarrow (u - \alpha)|f(u) \Leftrightarrow (U - \alpha V)|F(U, V) \Leftrightarrow F(\alpha, 1) = 0.$$

Значит, нули многочлена f соответствуют нулям формы F на $\mathbb{P}^1$, отличным от точки $(1, 0)$ (т. е. «точки $\alpha = \infty$ »). Что же означает наличие у F нуля на бесконечности?

$$F(1, 0) = 0 \Leftrightarrow a_d = 0 \Leftrightarrow \deg f < d.$$

Определим теперь кратность нуля многочлена F на $\mathbb{P}^1$ как:

(i) кратность нуля многочлена f в соответствующей точке $\alpha \in k$; или

(ii) $d - \deg f$, если точка $(1, 0)$ является нулем.

Таким образом кратность нуля многочлена F в точке $(\alpha, 1)$ — это наибольшая степень выражения $(U - \alpha V)$, на которую делится F , а для точки $(1, 0)$ — наибольшая степень V , на которую делится F .

Предложение. Пусть $F(U, V)$ — ненулевая форма степени d от переменных U, V . Тогда F имеет на $\mathbb{P}^1$ не более d нулей. Более того, если поле k алгебраически замкнуто, то F имеет на $\mathbb{P}^1$ ровно d нулей (при условии, что они подсчитываются с учетом определенной выше кратности).

Доказательство. Пусть m_∞ — кратность нуля многочлена F в точке $(1, 0)$. Тогда по определению величина $d - m_\infty$ — это степень неоднородного многочлена f , и утверждение сводится к общеизвестному факту, что многочлен f от одной переменной имеет не более $\deg f$ корней. Ч.т.д.

Заметим, что над алгебраически замкнутым полем многочлен F разлагается в произведение $F = \prod \lambda_i^{m_i}$ линейных форм $\lambda_i = a_i U + b_i V$. С этой точки зрения точка $(1, 0)$ соответствует форме $\lambda_\infty = V$ и ничем не отличается от всех остальных точек.

(1.9) Простые случаи теоремы Безу. Теорема Безу утверждает, что общее число точек пересечения двух плоских кривых C и D степеней $\deg C = m$ и $\deg D = n$ равно mn при условии, что

- (i) поле алгебраически замкнуто;
- (ii) точки пересечения подсчитываются с правильной кратностью;
- (iii) кривые рассматриваются на $\mathbb{P}^2$, чтобы правильно учитывать пересечение «на бесконечности».

Замкнутое доказательство см., например, в книге [Fulton, p. 112].

В этом разделе мы рассмотрим случай, когда одна из кривых является прямой или коникой.

Теорема. Пусть $L \subset \mathbb{P}_k^2$ — прямая (соответственно $C \subset \mathbb{P}_k^2$ — невырожденная коника) и $D \subset \mathbb{P}_k^2$ — кривая, определяемая условием $D: (G_d(X, Y, Z) = 0)$, где G — форма степени d от переменных X, Y, Z . Предположим, что $L \not\subset D$ (соответственно $C \not\subset D$); тогда $\# \{L \cap D\} \leq d$ (соответственно $\# \{C \cap D\} \leq 2d$).

В действительности имеется естественное определение кратности пересечения, при котором приведенное неравенство выполняется для «числа точек, подсчитанного с кратностями», а если k алгебраически замкнуто, то это неравенство превращается в равенство.

Доказательство. Прямая $L \subset \mathbb{P}_k^2$ задается уравнением $\lambda = 0$, где λ — линейная форма. Для наших целей удобно задать ее параметрически следующим образом:

$$X = a(U, V), \quad Y = b(U, V), \quad Z = c(U, V),$$

где a, b, c — линейные формы от U, V . Так, например, если $\lambda = \alpha X + \beta Y + \gamma Z$ и $\gamma \neq 0$, то L можно задать так:

$$X = U, \quad Y = V, \quad Z = -(\alpha/\gamma)U - (\beta/\gamma)V.$$

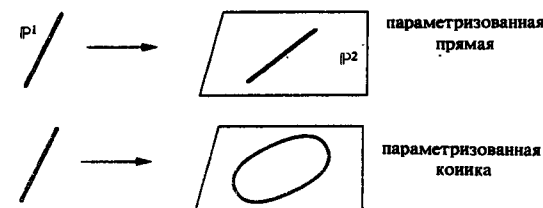
Аналогично, согласно (1.7), невырожденная коника может быть параметризована следующим образом:

$$X = a(U, V), \quad Y = b(U, V), \quad Z = c(U, V),$$

где a, b, c — квадратичные формы от переменных U и V . Это вытекает из того, что C проективно эквивалентна кривой $(XZ = Y^2)$, которая имеет следующую параметризацию: $(X, Y, Z) = (U^2, UV, V^2)$. Таким образом, C имеет вид

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = M \begin{bmatrix} U^2 \\ UV \\ V^2 \end{bmatrix},$$

где M — невырожденная 3×3 -матрица.



Теперь задача отыскания пересечений L (соответственно C) с D сводится к отысканию таких значений отношения $(U:V)$, что

$$F(U, V) = G_d(a(U, V), b(U, V), c(U, V)) = 0.$$

Так как F является формой степени d (соответственно $2d$) от переменных U, V , то искомым результатом вытекает из (1.8).

(1.10) Следствие. Если $P_1, \dots, P_5 \in \mathbb{P}_R^2$ — набор попарно различных точек, никакие 4 из которых не коллинеарны, то существует не более одной коники, проходящей через $P_1, \dots, P_5$.

Доказательство. Предположим противное. Пусть существуют такие коники C_1 и C_2 , $C_1 \neq C_2$, что

$$C_1 \cap C_2 \supset \{P_1, \dots, P_5\}.$$

Коника C_1 непустая, и, следовательно, если она невырождена, то, согласно (1.7), проективно эквивалентна параметризованной кривой

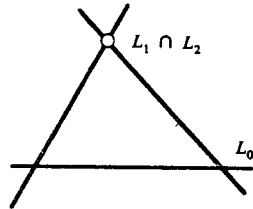
$$C_1 = \{(U^2, UV, V^2) | (U, V) \in \mathbb{P}^1\}.$$

В силу (1.9) $C_1 \subset C_2$. Пусть теперь $Q_2 = 0$ — уравнение кривой C_2 ; тогда для всех $(U, V) \in \mathbb{P}^1$ имеем $Q_2(U^2, UV, V^2) \equiv 0$, и легкие вычисления показывают (см. упр. 1.6), что Q_2 кратно $XZ - Y^2$, а это противоречит неравенству $C_1 \neq C_2$.

Предположим теперь, что C_1 вырождена. Снова воспользовавшись (1.6), убеждаемся, что она является либо парой прямых, либо одной прямой. Теперь легко показать, что

$$C_1 = L_0 \cup L_1, \quad C_2 = L_0 \cup L_2,$$

где L_1, L_2 — различные прямые. Следовательно, $C_1 \cap C_2 = L_0 \cup (L_1 \cap L_2)$:



Значит, 4 точки из набора $P_1, \dots, P_5$ лежат на L_0 , что вступает в противоречие с условием. Ч.т.д.

(1.11) Пространство всех коник. Пусть

$$S_2 = \left\{ \begin{array}{l} \text{квадратичные} \\ \text{формы на } \mathbb{R}^3 \end{array} \right\} = \left\{ \begin{array}{l} \text{симметричные} \\ 3 \times 3\text{-матрицы} \end{array} \right\} \cong \mathbb{R}^6.$$

Если $Q \in S_2$, то она имеет вид $Q = aX^2 + 2bXY + \dots + fZ^2$. Для точки $P_0 = (X_0, Y_0, Z_0) \in \mathbb{P}_R^2$ рассмотрим отношение $P_0 \in C: (Q = 0)$. Оно записывается следующим образом:

$$Q(X_0, Y_0, Z_0) = aX_0^2 + 2bX_0Y_0 + \dots + fZ_0^2 = 0,$$

и для фиксированной точки P_0 это уравнение линейно по $(a, b, \dots, f)$. Таким образом,

$$S_2(P_0) = \{Q \in S_2 | Q(P_0) = 0\} \cong \mathbb{R}^5 \subset S_2 = \mathbb{R}^6$$

является пятимерной гиперплоскостью. Аналогично набор точек $P_1, \dots, P_n \in \mathbb{P}_R^2$ задает

$$S_2(P_1, \dots, P_n) = \{Q \in S_2 | Q(P_i) = 0, \quad i = 1, \dots, n\};$$

возникает система из n линейных уравнений относительно 6 коэффициентов $(a, b, \dots, f)$ коники Q . В качестве следствия получаем такой результат:

Предложение. $\dim S_2(P_1, \dots, P_n) \geq 6 - n$.

Естественно предположить, что «для набора точек $P_1, \dots, P_n$ общего положения» неравенство превращается в равенство. Строгое утверждение таково.

Следствие. Если $n \leq 5$ и никакие 4 точки из набора $P_1, \dots, P_n$ не коллинеарны, то

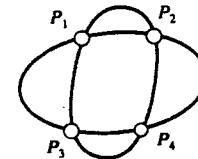
$$\dim S_2(P_1, \dots, P_n) = 6 - n.$$

Доказательство. Из следствия (1.10) вытекает, что при $n = 5$ $\dim S_2(P_1, \dots, P_5) \leq 1$, что и составляет требуемое утверждение для этого случая. Если $n \leq 4$, то можно добавить точки $P_{n+1}, \dots, P_5$, сохраняя условие неколлинеарности всех четверок. Так как каждая точка налагает не более одного линейного условия, то получаем

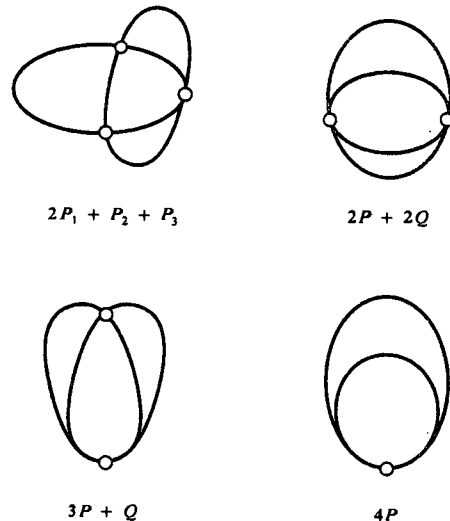
$$1 = \dim S_2(P_1, \dots, P_5) \geq \dim S_2(P_1, \dots, P_n) - (5 - n). \quad \text{Ч.т.д.}$$

Заметим, что произвольные 6 точек $P_1, \dots, P_6 \in \mathbb{P}_R^2$ могут и не лежать ни на какой конике.

(1.12) Пересечение двух коник. Как мы убедились ранее, две коники часто пересекаются в четырех точках:



И наоборот, согласно следствию (1.11), для заданных четырех точек $P_1, \dots, P_4$ при выполнении подходящих условий $S_2(P_1, \dots, P_4)$ является двумерным линейным пространством. Следовательно, выбрав в $S_2(P_1, \dots, P_4)$ базис Q_1, Q_2 , мы определим две коники C_1 и C_2 , такие, что $C_1 \cap C_2 = \{P_1, \dots, P_4\}$. Кроме того, имеется много разных конфигураций для кратных пересечений неособых коник:



(см. упр. 1.9 по поводу соответствующих уравнений).

(1.13) Вырождение коник в линейном пучке

Определение. Пучком коник называется семейство вида

$$C_{(\lambda, \mu)}: (\lambda Q_1 + \mu Q_2 = 0);$$

каждый элемент этого семейства является плоской кривой, линейно зависящей от параметров (λ, μ) . Отношение $(\lambda: \mu)$ следует представлять себе как точку на $\mathbb{P}^1$.

Из рассмотрения примеров становится ясно, что при некоторых значениях $(\lambda: \mu)$ коника $C_{(\lambda, \mu)}$ вырождается. Действительно, если рассмотреть детерминант $\det(Q)$ симметрической 3×3 -матрицы, соответствующей квадратичной форме Q , то легко заметить, что

$$C_{(\lambda, \mu)} \text{ вырождена} \Leftrightarrow \det(\lambda Q_1 + \mu Q_2) = 0.$$

Если Q_1 и Q_2 заданы симметрическими матрицами, то указанное условие приобретает следующий вид:

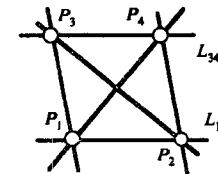
$$F(\lambda, \mu) = \det \left(\lambda \begin{bmatrix} a & b & d \\ b & c & e \\ d & e & f \end{bmatrix} + \mu \begin{bmatrix} a' & b' & d' \\ b' & c' & e' \\ d' & e' & f' \end{bmatrix} \right) = 0.$$

Отметим теперь, что $F(\lambda, \mu)$ — однородная кубическая форма от переменных λ, μ . Если в свою очередь применить к F предложение разд. (1.8), то получим следующее утверждение.

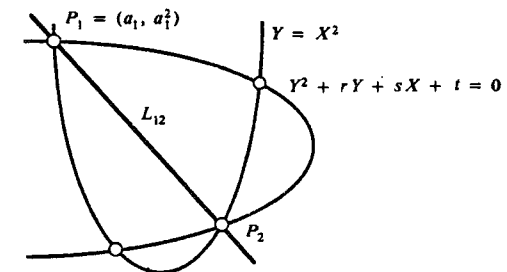
Предложение. Пусть $C_{(\lambda, \mu)}$ — пучок коник на $\mathbb{P}_k^2$, содержащий хотя бы одну невырожденную конику (т. е. $F(\lambda, \mu)$ не равна тождественно нулю); тогда он содержит не более трех вырожденных коник. В случае $k = \mathbb{R}$ этот пучок содержит по крайней мере одну вырожденную конику.

Доказательство. Кубическая форма имеет не более трех нулей, а в вещественном случае она имеет не менее одного нуля.

(1.14) **Пример.** Пусть $P_1, \dots, P_4$ — четыре точки в $\mathbb{P}_R^2$, никакие три из которых не коллинеарны. Тогда пучок $C_{(\lambda, \mu)}$ коник, проходящих через точки $P_1, \dots, P_4$, содержит три вырожденных элемента, а именно пары прямых $L_{12} + L_{34}$, $L_{13} + L_{24}$, $L_{14} + L_{23}$, где L_{ij} — прямая, проходящая через точки P_i и P_j :



Рассмотрим теперь пучок коник, порождаемый многочленами $Q_1 = Y^2 + rY + sX + t$ и $Q_2 = Y - X^2$, и попытаемся найти точки пересечения $P_1, \dots, P_4$.



Это можно сделать следующим образом:

(1) Найдем три отношения $(\lambda:\mu)$, для которых коники $C_{(\lambda,\mu)}$ вырождены. Согласно изложенному выше, это сводится к нахождению трех корней кубики

$$F(\lambda, \mu) = \det \left(\lambda \begin{bmatrix} 0 & 0 & s/2 \\ 0 & 1 & r/2 \\ s/2 & r/2 & t \end{bmatrix} + \mu \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1/2 \\ 0 & 1/2 & 0 \end{bmatrix} \right) =$$

$$= -\frac{1}{4}(s^2\lambda^3 + (4t - r^2)\lambda^2\mu - 2r\lambda\mu^2 - \mu^3).$$

(2) Разобьем две из вырожденных коник на пары прямых (что потребует решения двух квадратных уравнений).

(3) Определим четыре точки P_i как точки пересечения этих прямых.

Этот способ приводит к следующей геометрической интерпретации для редукции общей квартики в теории Галуа (см., например, [ван дер Варден. Алгебра. — М.: Наука, 1976, гл. 8, § 64]). Пусть k — поле и $f(X) = X^4 + rX^2 + sX + t \in k[X]$ — многочлен четвертой степени (квартика). Тогда две параболы C_1 и C_2 пересекаются в четырех точках $P_i = (a_i, a_i^2)$, где a_i — четыре корня многочлена f .

При этом прямая $L_{ij} = P_iP_j$ задается так:

$$L_{ij}: (Y = (a_i + a_j)X - a_ia_j),$$

а приводимая коника $L_{12} + L_{34}$ определяется уравнением

$$Y^2 + (a_1a_2 + a_3a_4)Y + (a_1 + a_2)(a_3 + a_4)X^2 + sX + t = 0,$$

или, что эквивалентно, соотношением $Q_1 - (a_1 + a_2)(a_3 + a_4)Q_2 = 0$. Следовательно, три значения отношения μ/λ , для которых коника $\lambda Q_1 + \mu Q_2$ распадается в пару прямых, таковы:

$$-(a_1 + a_2)(a_3 + a_4), -(a_1 + a_3)(a_2 + a_4), -(a_1 + a_4)(a_2 + a_3).$$

Кубическое уравнение, корнями которого являются указанные три значения, называется *присоединенной кубикой*, ассоциированной с квартикой. Она может быть вычислена через элементарные симметрические функции, однако это достаточно трудоемкое занятие. Описанный же геометрический метод приводит к довольно элегантному выводу для присоединенной кубики, требующему только вычисления детерминанта 3×3 -матрицы.

Эти рассуждения заимствованы из книги [Берже, 16.4.10 и 16.4.11.1].

Упражнения к § 1

1.1. Параметризуем конику $C: (x^2 + y^2 = 5)$ с помощью пучка прямых, проходящих через точку $(2, 1)$, и как следствие найдите все рациональные решения уравнения $x^2 + y^2 = 5$.

1.2. Пусть p — некоторое простое число. Поэкспериментируйте с разными p и угадайте необходимое и достаточное условие того, чтобы уравнение $x^2 + y^2 = p$ имело рациональные решения. Докажите свою догадку (указание приводится после упр. 1.9 — ручаюсь, что без него вам не справиться!).

1.3. Докажите утверждение из (1.3) о том, что любая коника в $\mathbb{R}^2$ с помощью аффинного преобразования приводится к одной из стандартных форм (а) — (л). (Указание. С помощью линейного преобразования $x \mapsto Ax$ приведите старший член $ax^2 + bxu + cy^2$ к одной из следующих форм: $\pm x^2 \pm y^2$, $\pm x^2$ или 0. После этого дополните получившееся выражение до полных квадратов по x и по y так, чтобы по возможности избавиться от линейной части.)

1.4. Проведите подробное сравнение аффинных коник из (1.3) с проективными кониками из (1.6).

1.5. Пусть k — произвольное поле, характеристика которого отлична от двух, а V — трехмерное векторное пространство. Пусть $Q: V \rightarrow k$ — невырожденная квадратичная форма на V . Покажите, что если ненулевой вектор $0 \neq e_1 \in V$ удовлетворяет условию $Q(e_1) = 0$, то существует такой базис e_1, e_2, e_3 пространства V , что $Q(x_1e_1 + x_2e_2 + x_3e_3) = x_1x_3 + ax_2^2$. (Указание. Рассмотрите симметрическую билинейную форму φ , ассоциированную с Q . Так как φ невырождена, то существует такой вектор e_2 , что $\varphi(e_1, e_2) = 1$. Теперь найдите подходящий вектор e_3 .)

Докажите, что непустая невырожденная коника $C \subset \mathbb{P}_k^2$ проективно эквивалентна кривой $(XZ = Y^2)$.

1.6. Пусть k — поле, содержащее не менее четырех элементов, и пусть $C: (XZ = Y^2) \subset \mathbb{P}_k^2$. Докажите, что если $Q(X, Y, Z)$ — квадратичная форма, обращающаяся на C в нуль, то $Q = \lambda(XZ - Y^2)$. (Указание. Если вы действительно не можете сделать это самостоятельно, воспользуйтесь рассуждениями из доказательства леммы (2.5).)

1.7. Рассмотрим в $\mathbb{R}^3$ две плоскости $A: (Z = 1)$ и $B: (X = 1)$. Прямая, проходящая через нуль и пересекающая плоскость A в точке $(x, y, 1)$, пересекает плоскость B в точке $(1, y/x, 1/x)$. Рассмотрим отображение $\varphi: A \rightarrow B$, определенное соотношением $(x, y) \mapsto (y' = y/x, z' = 1/x)$. Что представляет собой образ при отображении φ

(i) прямой $ax = y + b$; пучка параллельных прямых $ax = y + b$ (a фиксировано, b меняется);

(ii) окружностей $(x - 1)^2 + y^2 = c$ при переменном c (разберите 3 случая: $c > 1$, $c = 1$ и $c < 1$).

Постарайтесь представить себе результаты этого упражнения как изображение кривых, лежащих на плоскости $(Z = 1)$, которое нарисует на плоскости $(X = 1)$ художник, находящийся в точке 0. Что происходит в тех точках, где φ или φ^{-1} не определены?

1.8. Пусть $P_1, \dots, P_4$ — попарно различные точки на $\mathbb{P}^2$, никакие 3 из которых не коллинеарны. Докажите, что существует единственная система координат, в которой эти точки совпадают с точками $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ и $(1, 1, 1)$ соответственно. Найдите все коники, проходящие через $P_1, \dots, P_5$, где $P_5 = (a, b, c)$ — еще одна точка, и воспользуйтесь этим для того, чтобы получить новое доказательство следствия (1.10) и предложения (1.11).

1.9. В разд. (1.12) приведен набор различных вариантов пересечения пары коник. Выпишите уравнения, которые показывают, что каждый из этих вариантов действительно реализуется. Найдите все особые коники в соответствующих пучках. (Указание. Вы избежите многих неприятностей, воспользовавшись симметрией и подходящей системой координат.)

Указание к упр. 1.2. Из элементарной теории чисел известно, что -1 является квадратичным вычетом по модулю p тогда и только тогда, когда $p = 2$ или $p \equiv 1 \pmod{4}$.

1.10. (Детерминант Сильвестра.) Пусть k — алгебраически замкнутое поле, и пусть заданы, как и в разд. (1.8), квадратичная и кубическая формы от переменных U и V :

$$q(U, V) = a_0 U^2 + a_1 UV + a_2 V^2,$$

$$c(U, V) = b_0 U^3 + b_1 U^2 V + b_2 UV^2 + b_3 V^3.$$

Докажите, что q и c имеют общий корень $(\eta : \tau) \in \mathbb{P}^1$ тогда и только тогда, когда

$$\det \begin{bmatrix} a_0 & a_1 & a_2 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & b_3 & 0 \\ 0 & b_0 & b_1 & b_2 & b_3 \end{bmatrix} = 0.$$

(Указание. Покажите, что если q и c имеют общий корень, то 5 элементов

$$U^2 q, UVq, V^2 q, Uc \text{ и } Vc$$

не порождают все пятимерное векторное пространство форм четвертой степени и, следовательно, линейно зависимы. И наоборот, воспользуйтесь единственностью разложения на множители в кольце многочленов $k[U, V]$ для получения информации о соотношениях вида $Aq = Bc$, где A и B — формы от переменных (U, V) , $\deg A = 2$, $\deg B = 1$.)

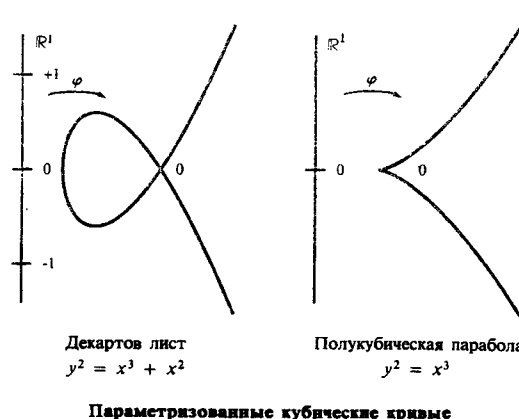
1.11. Обобщите результаты упр. 1.10 на случай двух форм от переменных U, V произвольных степеней n и m .

§ 2. Кубики и групповой закон

(2.1) Примеры параметризованных кубик. Так же как коники, могут быть параметризованы и некоторые плоские кубики:

Декартов лист (нодальная кубика). $C: (y^2 = x^3 + x^2) \subset \mathbb{R}^2$ является образом отображения $\varphi: \mathbb{R}^1 \rightarrow \mathbb{R}^2$, заданного формулой $t \mapsto (t^2 - 1, t^3 - t)$ (проверьте и убедитесь);

Полукубическая парабола (каспидальная кубика). $C: (y^2 = x^3) \subset \mathbb{R}^2$ является образом отображения $\varphi: \mathbb{R}^1 \rightarrow \mathbb{R}^2$, заданного формулой $t \mapsto (t^2, t^3)$.



Потратьте некоторое время на изучение особенностей кривой-образа и отображения φ . Эти примеры будут часто встречаться в дальнейшем, поэтому поизучайте их уравнения [см. упр. 2.1—2.2].

(2.2) Кривая $(y^2 = x(x-1)(x-\lambda))$ не имеет рациональной параметризации. Параметризуемые кривые обладают замечательными свойствами. Например, если мы решаем диофантову задачу, то можно надеяться получить, как и в разд. (1.1), способ описания всех рациональных точек. Найденная в (1.1) параметризация имела вид $x = f(t)$, $y = g(t)$, где f и g — рациональные функции, т. е. отношения двух многочленов.

Теорема. Пусть k — поле, характеристика которого не равна 2, а $\lambda \in k$, $\lambda \neq 0, 1$. Пусть $f, g \in k(t)$ — такие рациональные функции, что

$$f^2 = g(g-1)(g-\lambda). \quad (*)$$

Тогда $f, g \in k$.

Это утверждение эквивалентно тому, что не существует отличного от константы отображения $\mathbb{R}^1 \rightarrow C: (y^2 = x(x-1)(x-\lambda))$, задаваемого рациональными функциями. Это обстоятельство отражает свойство сильной «жесткости» алгебраических многообразий.

Доказательство этой теоремы состоит из арифметических вычислений в поле $k(t)$ и использует тот факт, что $k(t)$ — поле частных кольца $k[t]$, являющегося областью с однозначным разложением на множители. Само доказательство достаточно длинное, и поэтому читатель должен либо его детально разобрать, либо сразу

перейти к разд. (2.4). В упр. 2.12 приводится очень похожий пример доказательства несуществования, основанного на арифметике над $\mathbb{Q}$.

Доказательство. Используя тот факт, что $k[t]$ — область с однозначным разложением на множители, представим f и g в виде

$$f = r/s, \text{ где } r, s \in k[t] \text{ и взаимно просты,}$$

$$g = p/q, \text{ где } p, q \in k[t] \text{ и взаимно просты.}$$

После приведения к общему знаменателю (*) принимает вид

$$r^2 q^3 = s^2 p(p - q)(p - \lambda q).$$

Далее, так как r и s взаимно просты, то сомножитель s^2 , стоящий в правой части, должен делить q^3 ; аналогично, так как p и q взаимно просты, то сомножитель q^3 , стоящий в левой части, должен делить s^2 . Итак, $s^2 | q^3$ и $q^3 | s^2$, а значит, $s^2 = aq^3$, где $a \in k$ (a является единицей в кольце $k[t]$ и, следовательно, лежит в k).

Тогда $aq = (s/q)^2$ является квадратом в $k[t]$. Кроме того,

$$r^2 = ap(p - q)(p - \lambda q).$$

Из разложения в произведение простых сомножителей вытекает теперь, что существуют такие ненулевые константы $b, c, d \in k$, что $br, c(p - q), d(p - \lambda q)$ являются квадратами в $k[t]$. Если нам удастся доказать, что p и q — константы, то из сказанного выше будет следовать, что r и s — также константы, и теорема будет доказана. Чтобы убедиться, что p и q — константы, рассмотрим алгебраическое замыкание K поля k . Тогда $p, q \in K[t]$ удовлетворяют условиям следующей леммы.

(2.3) Лемма. Пусть K — алгебраически замкнутое поле, а p и $q \in K[t]$ — взаимно простые элементы. Предположим, что четыре различные линейные комбинации (т. е. $\lambda p + \mu q$ для четырех различных отношений $(\lambda:\mu) \in \mathbb{P}_K^1$) являются квадратами в $K[t]$; тогда $p, q \in K$.

Доказательство (метод бесконечного спуска Ферма). Заметим, что и посылка и утверждение леммы не меняются при замене p, q на

$$p' = ap + bq, \quad q' = cp + dq,$$

где $a, b, c, d \in K$ и $ad - bc \neq 0$. Следовательно, мы можем считать, что заданными квадратами являются

$$p, p - q, p - \lambda q, q.$$

Имеем $p = u^2, q = v^2$, где $u, v \in K[t]$ взаимно просты и

$$\max\{\deg u, \deg v\} < \max\{\deg p, \deg q\}.$$

Предположим от противного, что $\max\{\deg p, \deg q\}$ положителен и является минимальным на множестве всех пар p, q , удовлетворяющих условиям леммы. Тогда справедливы два следующих равенства:

$$p - q = u^2 - v^2 = (u - v)(u + v),$$

$$p - \lambda q = u^2 - \lambda v^2 = (u - \mu v)(u + \mu v)$$

(где $\mu = \sqrt{\lambda}$) являются квадратами в $K[t]$, а в силу взаимной простоты u и v квадратами будут также $u - v, u + v, u - \mu v, u + \mu v$, что противоречит минимальности $\max\{\deg p, \deg q\}$. Ч.т.д.

(2.4) Линейные системы. Обозначим через S_d пространство всех форм степени d от переменных X, Y, Z . (Напомним, что форма — это просто однородный многочлен.) Каждый элемент $F \in S_d$ единственным образом представляется в виде

$$F = \sum a_{ijk} X^i Y^j Z^k, \quad a_{ijk} \in k,$$

где сумма берется по всем $i, j, k \geq 0$, таким, что $i + j + k = d$.

Это, разумеется, означает, что S_d является векторным k -пространством с базисом

$$\begin{aligned} & Z^d, \\ & Z^{d-1}X, Z^{d-1}Y, \\ & \dots \dots \\ & X^{d-1}Z, X^{d-2}YZ, \dots, Y^{d-1}Z, \\ & X^d, X^{d-1}Y, X^{d-2}Y^2, \dots, Y^d \end{aligned}$$

и, в частности, что $\dim S_d = \binom{d+2}{2}$. Для набора точек $P_1, \dots, P_n \in \mathbb{P}^2$ положим

$$S_d(P_1, \dots, P_n) = \{F \in S_d \mid F(P_i) = 0, i = 1, \dots, n\} \subset S_d.$$

Каждое из условий $F(P_i) = 0$ (точнее $F(X_i, Y_i, Z_i) = 0$, где $P_i = (X_i:Y_i:Z_i)$) задает на F одно линейное соотношение. Таким образом, $S_d(P_1, \dots, P_n)$ является векторным пространством размерности не менее $\binom{d+2}{2} - n$.

(2.5) Лемма. Предположим, что k — бесконечное поле, и пусть $F \in S_d$.

(i) Пусть $L \subset \mathbb{P}_k^2$ — прямая. Если $F \equiv 0$ на L , то F делится в кольце $k[X, Y, Z]$ на определяющий многочлен прямой L . Это означает, что $F = H \cdot F'$, где $H = 0$ — уравнение L , а $F' \in S_{d-1}$.

(ii) Пусть $C \subset \mathbb{P}_k^2$ — непустая невырожденная коника. Если $F \equiv 0$ на C , то F делится в кольце $k[X, Y, Z]$ на определяющий многочлен коники C . Это означает, что $F = QF'$, где $Q = 0$ — уравнение коники C , а $F' \in S_{d-2}$.

Если это утверждение кажется вам очевидным, то можете считать, что у вас хорошая интуиция. Вы угадали частный случай Nullstellensatz. Теперь докажете его самостоятельно и переходите к разд. (2.6).

Доказательство. (i) Выбрав подходящие координаты, мы можем считать, что $H = X$. Тогда для любого $F \in S_d$ существует единственное представление вида $F = X \cdot F'_{d-1} + G(Y, Z)$. Чтобы его получить, достаточно сгруппировать все одночлены, содержащие X , в первое слагаемое, а то, что осталось, будет многочленом только от Y и Z . Имеет место следующая цепочка эквивалентностей: $F \equiv 0$ на $L \Leftrightarrow G \equiv 0$ на $L \Leftrightarrow G(Y, Z) = 0$. Последняя эквивалентность справедлива в силу (1.8). А именно, если $G(Y, Z) \neq 0$, то он имеет не более d нулей на $\mathbb{P}_k^1$, тогда как если k бесконечно, то $\mathbb{P}_k^1$ также бесконечно.

(ii) Выбрав подходящие координаты, добьемся, чтобы $Q = XZ - Y^2$. Покажем теперь, что для любого $F \in S_d$ существует единственное представление вида $F = Q \cdot F'_{d-2} + A(X, Z) + YB(X, Z)$. А именно, если в многочлене F заменить всюду Y^2 на $XZ - Q$, то результат подстановки будет иметь по Y степень ≤ 1 , т. е. будет иметь вид $A(X, Z) + YB(X, Z)$. Коника C является параметризованной коникой (см. разд. (1.7)) с параметризацией $X = U^2$, $Y = UV$, $Z = V^2$. Таким образом,

$$F \equiv 0 \text{ на } C \Leftrightarrow A(U^2, V^2) + UVB(U^2, V^2) \equiv 0 \text{ на } C \Leftrightarrow \\ \Leftrightarrow A(U^2, V^2) + UVB(U^2, V^2) = 0 \in k[U, V] \Leftrightarrow A(X, Z) = B(X, Z) = 0.$$

Последняя эквивалентность вытекает из раздельного рассмотрения членов четной и нечетной степени формы $A(U^2, V^2) + UVB(U^2, V^2)$. Ч.т.д.

В упр. 2.2 рассматриваются аналогичные «явные» случаи Nullstellensatz.

Следствие. Пусть $L: (H = 0) \subset \mathbb{P}_k^2$ — прямая (соответственно $C: (Q = 0) \subset \mathbb{P}_k^2$ — невырожденная коника). Предположим, что на $\mathbb{P}_k^2$ зафиксирован набор точек $P_1, \dots, P_n$, и рассмотрим пространство $S_d(P_1, \dots, P_n)$ для некоторого фиксированного d . Тогда

(i) если $P_1, \dots, P_a \in L$, $P_{a+1}, \dots, P_n \notin L$ и $a > d$, то

$$S_d(P_1, \dots, P_n) = H \cdot S_{d-1}(P_{a+1}, \dots, P_n);$$

(ii) если $P_1, \dots, P_a \in C$, $P_{a+1}, \dots, P_n \notin C$ и $a > 2d$, то

$$S_d(P_1, \dots, P_n) = Q \cdot S_{d-2}(P_{a+1}, \dots, P_n).$$

Доказательство. (i) Если F — однородный многочлен степени d и кривая $D: (F = 0)$ пересекает L в точках $P_1, \dots, P_a$, где $a > d$, то в силу (1.9) получаем, что $L \subset D$. Тогда по доказанной лемме $F = H \cdot F'$. Далее, так как $P_{a+1}, \dots, P_n \notin L$, то очевидно, что $F' \in S_{d-1}(P_{a+1}, \dots, P_n)$. (ii) То же самое рассуждение проходит и во втором случае. Ч.т.д.

(2.6) Предложение. Пусть k — бесконечное поле, а $P_1, \dots, P_8 \in \mathbb{P}_k^2$ — набор различных точек. Предположим, что никакие 4 точки из $P_1, \dots, P_8$ не коллинеарны и никакие 7 из них не лежат на невырожденной конике. Тогда

$$\dim S_3(P_1, \dots, P_8) = 2.$$

Доказательство. Будем для краткости говорить, что набор точек является конкониическим, если все точки этого набора лежат на невырожденной конике. Доказательство предложения (2.6) распадается на несколько случаев.

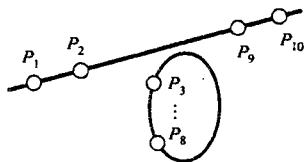
Основной случай. Никакие 3 точки не коллинеарны и никакие 6 не конкониичны. Это случай «общего положения».

Предположим противное. Пусть $\dim S_3(P_1, \dots, P_8) \geq 3$, и пусть P_9 и P_{10} — несовпадающие точки на прямой $L = P_1P_2$. Тогда

$$\dim S_3(P_1, \dots, P_{10}) \geq \dim S_3(P_1, \dots, P_8) - 2 \geq 1.$$

Таким образом, существует $0 \neq F \in S_3(P_1, \dots, P_{10})$. Согласно следствию (2.5), $F = H \cdot Q$, где $Q \in S_2(P_3, \dots, P_8)$. Получаем следующее противоречие с предположением: если Q невырожденна, то 6 точек

$P_3, \dots, P_8$ являются конконическими, а если Q — пара прямых или двойная прямая, то по крайней мере 3 из них коллинеарны.



Первый вырожденный случай. Пусть $P_1, P_2, P_3 \in L$ коллинеарны и $L: (H=0)$. Пусть P_9 — четвертая точка на прямой L . Тогда в силу следствия из разд. (2.5)

$$S_3(P_1, \dots, P_9) = H \cdot S_2(P_4, \dots, P_8).$$

Кроме того, так как никакие четыре из точек $P_4, \dots, P_8$ не коллинеарны, то в силу следствия (1.11) $\dim S_2(P_4, \dots, P_8) = 1$ и, значит, $\dim S_3(P_1, \dots, P_9) = 1$, откуда вытекает, что $\dim S_3(P_1, \dots, P_8) \leq 2$.

Второй вырожденный случай. Предположим, что $P_1, \dots, P_6 \in C$ — конконический набор, где $C: (Q=0)$ — невырожденная коника. Тогда если $P_9 \in C$ — точка, отличная от $P_1, \dots, P_6$, то опять в силу следствия из разд. (2.5) получаем

$$S_3(P_1, \dots, P_9) = Q \cdot S_1(P_7, P_8);$$

прямая $L = P_7P_8$ определена однозначно, так что $S_3(P_1, \dots, P_9)$ — одномерное пространство, порожденное QH . Следовательно, $\dim S_3(P_1, \dots, P_8) \leq 2$. Ч.т.д.

(2.7) Следствие. Пусть C_1, C_2 — две кубические кривые, пересечение которых состоит из 9 различных точек, $C_1 \cap C_2 = \{P_1, \dots, P_9\}$. Тогда кубика D , проходящая через точки $P_1, \dots, P_8$, проходит также и через P_9 .

Доказательство. Если какие-нибудь четыре точки из набора $P_1, \dots, P_8$ лежат на одной прямой L , то C_1 и C_2 пересекают L не менее чем в четырех точках и, значит, содержат ее, что противоречит предположению относительно пересечения $C_1 \cap C_2$. По тем же причинам никакие 7 из указанных точек не могут быть конконическими. Таким образом, в рассматриваемом случае выполнены условия предложения (2.6), откуда следует, что

$$\dim S_3(P_1, \dots, P_8) = 2;$$

это означает, что многочлены F_1 и F_2 , задающие кривые C_1 и C_2 , образуют базис пространства $S_3(P_1, \dots, P_8)$. Следовательно, D задается уравнением $G=0$, где $G = \lambda F_1 + \mu F_2$. Далее, так как F_1 и F_2 обращаются в точке P_9 в нуль, то G также равно нулю. Ч.т.д.

(2.8) Групповой закон на плоской кубике. Пусть $k \subset \mathbb{C}$ — некоторое подполе в $\mathbb{C}$, а $F \in k[X, Y, Z]$ — кубическая форма, определяющая (непустую) плоскую кривую $C: (F=0) \subset \mathbb{P}_k^2$. Предположим, что F удовлетворяет следующим двум условиям:

(a) F неприводима (а значит, C не содержит ни прямой, ни коники);

(b) для любой точки $P \in C$ существует единственная прямая $L \subset \mathbb{P}_k^2$, такая, что P — кратный нуль функции $F|_L$.

Заметим, что геометрический смысл условия (b) заключается в том, что C должна быть неособой и что прямая L , о которой идет речь, является касательной к C ($L = T_P C$) (см. упр. 2.3). Это наблюдение послужит нам в § 6 мотивировкой общего определения неособости и касательных пространств к многообразию.

Зафиксируем произвольную точку $O \in C$ и выполним следующее построение.

Построение. (i) Для $A \in C$ обозначим через $\bar{A}$ третью точку пересечения C с прямой OA .

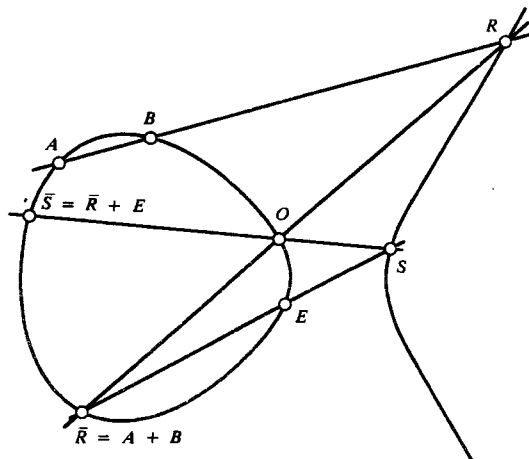
(ii) Для $A, B \in C$ обозначим через R третью точку пересечения прямой AB с C и определим сумму $A + B$ формулой $A + B = \bar{R}$ (см. рисунок на следующей странице).

Теорема. Описанная конструкция задает на C структуру абелевой группы, нулем (нейтральным элементом) которой является точка O .

Доказательство. Здесь суть дела составляет проверка ассоциативности. Мы начнем с простых наблюдений.

(I) Покажем, что операции сложения и взятия обратного элемента корректно определены. Если $P, Q \in C$ — любые две точки, то либо $P \neq Q$ и прямая $L = PQ \subset \mathbb{P}_k^2$ однозначно определена, либо $P = Q$ и тогда в силу предположения (b) существует единственная прямая $L \subset \mathbb{P}_k^2$, такая, что P — кратный нуль функции $F|_L$. В обоих случаях $F|_L$ является кубической формой от двух переменных, имеющей два заданных нуля с координатами в k . Тем самым она разлагается в произведение трех линейных множителей. Следовательно, во всех без исключения случаях определена третья точка пе-

ресекация R и ее координаты принадлежат k . Отметим, что разрешены все вырожденные случаи $P = Q$, $Q = R$, $P = R$ или $P = Q = R$. Алгебраически они соответствуют тому, что $F|_L$ имеет кратные корни, а геометрически — касательным и точкам перегиба.



Кубическая кривая и групповой закон на ней

(II) Проверка того, что заданная точка O является нейтральным элементом, выполняется автоматически: так как точки $O, A, \bar{A}$ коллинеарны, то при построении суммы $O + A$ мы с помощью прямой $L = OA$ получаем третью точку пересечения $\bar{A}$, а затем с помощью той же прямой $L = O\bar{A}$ возвращаемся к исходной точке A .

(III) Проверку равенства $A + B = B + A$ можно, пожалуй, оставить читателю.

(IV) Чтобы найти обратный элемент, мы аналогично п. (i) построения определим точку $\bar{O}$. Точнее, пусть L — прямая, такая, что $F|_L$ имеет в точке O кратный нуль, и определим $\bar{O}$ как третью точку пересечения L с кривой C . Легко убедиться, что для любой точки $A \in C$ третья точка пересечения прямой $\bar{O}A$ с C является обратным элементом к A .

(2.9) Теперь я докажу ассоциативность изучаемой операции для «достаточно общих» точек. Предположим, что на кривой C заданы три точки A , B и E . Тогда при построении суммы $(A + B) + E = \bar{S}$ нам понадобятся следующие четыре прямые (см. предыдущий рисунок):

$$L_1: ABR, \quad L_2: ROR\bar{R}, \quad L_3: E\bar{R}S, \quad L_4: SO\bar{S}.$$

При построении суммы $(B + E) + A = \overline{T}$ необходимы следующие четыре прямые:

$$M_1: BEO, M_2: OOO, M_3: AOT \text{ и } M_4: TOT$$

Нужно доказать, что $\overline{S} = \overline{T}$, для чего, очевидно, достаточно доказать, что $S = T$. Чтобы убедиться в этом, рассмотрим две кубики:

$$D_1 = L_1 + M_2 + L_3 \text{ и } D_2 = M_1 + L_2 + M_3.$$

Тогда по построению получаем

$$C \cap D_1 = \{A, B, E, O, R, \bar{R}, Q, \bar{Q}, S\},$$

И

$$C \cap D_2 = \{A, B, E, O, R, \bar{R}, Q, \bar{Q}, T\}.$$

Если теперь 9 точек $A, B, E, O, R, \bar{R}, Q, \bar{Q}, S$ попарно различны, то кубики C и D_1 удовлетворяют условиям следствия (2.7). Значит, D_2 должна проходить через точку S , что возможно лишь при $S = T$.

Чтобы закончить наше рассуждение, можно воспользоваться разными методами. Наиболее последовательный из них заключается в полном описании случая кратных пересечений двух кривых (грубо говоря, в терминах «идеалов пересечений»); утверждением, соответствующим следствию (2.7), является лемма М. Нётера (см. [Fulton, p. 120, 124]).

(2.10) Я набросаю схему одного варианта доказательства «по непрерывности», в котором используется то, что $k \subset \mathbb{C}$. Для произвольной кривой C обозначим через $C_{\mathbb{C}} \subset \mathbb{P}_{\mathbb{C}}^2$ ее комплексификацию, т. е. множество отношений $(X:Y:Z)$ комплексных чисел, удовлетворяющих тому же уравнению $F(X, Y, Z) = 0$. Если ассоциативность имеет место для всех $A, B, E \in C_{\mathbb{C}}$, то, очевидно, она выполняется и для всех точек кривой C . Поэтому можно считать, что $k = \mathbb{C}$.

Заинтересованному читателю не составит труда доказать следующие два утверждения (см. упр. 2.8).

Лемма. (i) $A + B$ — непрерывная функция от A и B ;

(ii) для любых трех точек $A, B, E \in C$ существуют три точки $A', B', E' \in C$, расположенные в произвольно малых окрестностях точек A, B, E соответственно и такие, что построенные по ним 9 точек $A', B', E', O, R, \bar{R}, Q, \bar{Q}, S$ попарно различны.

Групповой закон — это отображение $\varphi: C \times C \rightarrow C$, заданное формулой $(A, B) \mapsto A + B$. В силу утверждения (i) леммы отображе-

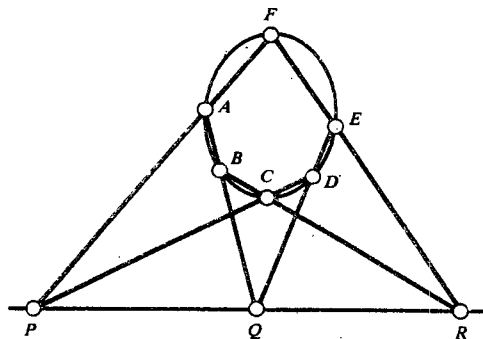
ние φ непрерывно и, значит, тем же свойством обладают следующие два отображения (приношу извинение за громоздкость):

$$f = \varphi \circ (\sigma \times \text{id}_C) \text{ и } g = \varphi \circ (\text{id}_C \times \varphi): C \times C \times C \rightarrow C,$$

заданные формулами $(A, B, E) \mapsto (A + B) + E$ и $A + (B + E)$. Кроме того, из (ii) вытекает, что подмножество $U \subset C \times C \times C$ тех троек (A, B, E) , для которых 9 точек, участвующих в построении, различны, является плотным. Таким образом, из приведенного рассуждения следует, что на множестве U отображения f и g совпадают, а так как они непрерывны, то совпадают всюду. Ч.т.д.

Замечание. Доказательство по непрерывности в том виде, в котором оно приведено, использует топологию поля C и поэтому не является чисто алгебраическим. В действительности, как мы установим позднее (см. (4.14)), групповой закон φ является морфизмом многообразий $\varphi: C \times C \rightarrow C$, и оставшейся части доказательства можно также придать чисто алгебраическую форму. А именно, подмножество в $C \times C \times C$, для которого упомянутые 9 точек различны, открыто и плотно в топологии Зарисского, а два морфизма, совпадающие на открытом плотном множестве, совпадают всюду. (Я надеюсь, что это замечание создаст у читателя некоторое представление о том, что его ожидает в остальной части курса. Если читатель сочтет его неубедительным, то он вправе его пока проигнорировать.)

(2.11) Теорема Паскаля (таинственная гексаграмма).



На чертеже изображен шестиугольник $ABCDEF$, лежащий в $\mathbb{P}_k^2$, пары противоположных сторон которого продолжены до пересечения в точках P, Q, R . Предположим, что все 9 точек и 6 прямых

на чертеже различны; тогда

A, B, C, D, E, F конконичны $\Leftrightarrow P, Q, R$ коллинеарны.

Эта знаменитая теорема — аналогичное применение следствия (2.7) и приведена здесь только для того, чтобы доставить читателю удовольствие. Конечно, у нее имеются и другие доказательства (см. любой учебник по геометрии, например, [Берже, 16.2.10 и 16.8.3-5]).

Доказательство. Рассмотрим две тройки прямых

$$L_1: PAF, L_2: QDE, L_3: RCB$$

и

$$M_1: PCD, M_2: QBA, M_3: REF,$$

изображенных на чертеже. Пусть кривая C_1 равна $L_1 + L_2 + L_3$, а кривая C_2 равна $M_1 + M_2 + M_3$. Теперь все подготовлено для применения следствия (2.7), так как очевидно, что C_1 и C_2 — кубики, удовлетворяющие условию

$$C_1 \cap C_2 = \{A, B, C, D, E, F, P, Q, R\}.$$

Предположим, что точки P, Q, R коллинеарны и $L = PQR$ — прямая. Пусть Γ — коника, проходящая через A, B, C, D, E (ее существование и единственность вытекают из предложения (1.11)). Тогда по построению $L + \Gamma$ — кубика, проходящая через 8 точек A, B, C, D, E, P, Q, R . Значит, в силу следствия (2.7) она должна содержать точку F . По предположению $F \notin L$, поэтому обязательно $F \in \Gamma$, что приводит к конконичности указанных шести точек.

Чтобы доказать обратное утверждение, предположим, что точки A, B, C, D, E, F лежат на конике Γ , и пусть $L = PQ$. Тогда $L + \Gamma$ — кубика, проходящая через точки A, B, C, D, E, F, P, Q . Поэтому в силу следствия (2.7) она должна проходить и через точку R . Далее, R не может лежать на конике Γ (так как в противном случае Γ является парой прямых и некоторые из 6 прямых на чертеже должны совпасть). Таким образом $R \in L$, т. е. точки P, Q, R коллинеарны. Ч.т.д.

(2.12) Перегиб, нормальная форма. Каждая кубика в $\mathbb{P}_{\mathbb{R}}^2$ или $\mathbb{P}_{\mathbb{C}}^2$ приводится к нормальной форме

$$C: (Y^2 Z = X^3 + aXZ^2 + bZ^3), \quad (**)$$

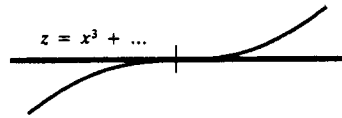
или, в аффинной записи,

$$y^2 = x^3 + ax + b.$$

Рассмотрим такую кривую C . Где она пересекает бесконечно удаленную прямую $L: (Z = 0)$? Это легко вычислить: надо подставить $Z = 0$ в определяющий многочлен $F = -Y^2Z + X^3 + aXZ^2 + bZ^3$ и получить $F|_L = X^3$. Это означает, что $F|_L$ имеет в точке $P = (0, 1, 0)$ трехкратный нуль. Чтобы понять, какой это имеет геометрический смысл, положим $Y = 1$ и запишем уравнение в аффинном куске, содержащем точку $(0, 1, 0)$, с координатами (x, z) :

$$z = x^3 + axz^2 + bz^3.$$

Эта кривая с большой точностью аппроксимируется кривой $z = x^3$:



При таком поведении кривой C говорят, что она имеет в точке $(0, 1, 0)$ *перегиб*. Более общим образом, точка перегиба P кривой C определяется условием, что существует прямая $L \subset \mathbb{P}_k^2$, такая, что $F|_L$ имеет нуль кратности ≥ 3 в точке P (см. упр. 2.9). В действительности в силу (2.8 (b)) необходимо, чтобы $L = T_P C$ и чтобы кратность равнялась 3 в силу (1.9). Нетрудно переписать это условие через первые и вторые производные определяющего многочлена. Например, если определяющее уравнение имеет вид $y = f(x)$, то условие наличия перегиба есть просто $d^2 f/dx^2(P) = 0$. На чертеже это соответствует кривой, у которой «выпуклость вверх» меняется на «выпуклость вниз». Имеется общий критерий того, что плоская кривая имеет точку перегиба, в терминах *гессиана*; см., например, [Fulton, p. 116] или упр. 7.3 (iii).

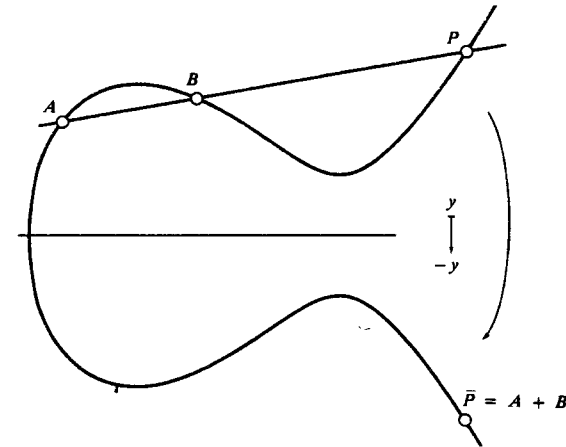
Можно показать (см. упр. 2.10), что верно и обратное утверждение: если плоская кубика C имеет точку перегиба, то ее уравнение приводится к нормальной форме (**), как выше.

(2.13) Упрощенный групповой закон. Нормальная форма (**) особенно удобна для описания группового закона. Возьмем точку перегиба $O = (0, 1, 0)$ в качестве нейтрального элемента. При этом групповой закон особенно упрощается по следующим причинам:

(а) $C = \{O\} \cup C_0: (y^2 = x^3 + ax + b)$, где C_0 — аффинная кривая. Это позволяет рассматривать C как аффинную кривую, лишь время от времени вспоминая о находящейся на бесконечности точке O — нуле группового закона.

(б) Прямые, проходящие через O и являющиеся основными компонентами (см. (2.8 (i))) при определении группового закона, зада-

ются в однородных координатах уравнением $X = \lambda Z$, а в аффинных координатах — уравнением $x = \lambda$. Любая такая прямая пересекает кривую C в точках $(\lambda, \pm \sqrt{\lambda^3 + a\lambda + b})$ и на бесконечности. Следовательно, если $P = (x, y)$, то точка $\bar{P}$, определяемая согласно (2.8 (i)), имеет координаты $(x, -y)$. Таким образом, преобразование $P \mapsto \bar{P}$ является естественной симметрией $(x, y) \mapsto (x, -y)$ кривой C_0 :



(с) Процедура взятия обратного элемента для группового закона 2.8 (IV) использует точку $\bar{O}$, которая строится как третья точка пересечения единственной прямой L , такой, что $F|_L$ имеет в точке O кратный нуль. В нашем же случае эта прямая совпадает с бесконечно удаленной прямой $L: (Z = 0)$ и $L \cap C = 3O$. Таким образом, $\bar{O} = O$, и взятие обратного элемента упрощается до $-P = \bar{P}$.

Теперь я в состоянии переформулировать групповой закон в виде упрощенного варианта теоремы (2.8).

Теорема. Пусть кубическая кривая C приведена к нормальной форме (**). Тогда на C существует единственный групповой закон, такой, что точка $O = (0, 1, 0)$ является нейтральным элементом, взятие обратного имеет вид $(x, y) \mapsto (x, -y)$ и для всех $P, Q, R \in C$

$$P + Q + R = O \Leftrightarrow P, Q, R \text{ коллинеарны.}$$

Упражнения к § 2

2.1. Пусть $C: (y^2 = x^3 + x^2) \subset \mathbb{R}^2$. Покажите, что любая прямая, проходящая через точку $(0, 0)$, пересекает C еще в одной точке, и получите в качестве следствия рассмотренную в разд. (2.1) параметризацию кривой C . Прделайте то же самое для $(y^2 = x^3)$ и $(x^3 = y^3 - y^4)$.

2.2. Пусть $\varphi: \mathbb{R}^1 \rightarrow \mathbb{R}^2$ — отображение $t \mapsto (t^2, t^3)$. Докажите непосредственно, что любой многочлен $f \in \mathbb{R}[X, Y]$, обращающийся в нуль на образе $C = \varphi(\mathbb{R}^1)$, делится на $Y^2 - X^3$. (Указание. Воспользуйтесь методом доказательства леммы (2.5).) Определите, каким свойством должно обладать поле k для того, чтобы сформулированный результат был верен для отображения $\varphi: k \rightarrow k^2$, заданного приведенной формулой.

Проделайте то же самое для отображения $t \mapsto (t^2 - 1, t^3 - t)$.

2.3. Пусть $C: (f = 0) \subset k^2$ и $P = (a, b) \in C$. Предположим, что $\partial f / \partial x(P) \neq 0$. Докажите, что прямая

$$L: (\partial f / \partial x(P) \cdot (X - a) + \partial f / \partial y(P) \cdot (Y - b) = 0)$$

является касательной к кривой C в точке P , т. е. единственной прямой L на плоскости k^2 , для которой $f|_L$ имеет в точке P кратный корень (этот вопрос подробно разбирается в разд. (6.1)).

2.4. Пусть $C: (y^2 = x^3 + 4x)$ — кривая, на которой мы рассматриваем упрощенный групповой закон (2.13). Покажите, что касательная прямая к C в точке $P = (2, 4)$ проходит через точку $(0, 0)$, и выведите отсюда, что P — точка порядка 4 относительно группового закона.

2.5. Пусть $C: (y^2 = x^3 + ax + b) \subset \mathbb{R}^2$ — неособая кубика. Найдите все точки порядка 2 относительно группового закона и выясните, какую группу они образуют (придется рассмотреть два разных случая).

Теперь поясните в геометрических терминах, как бы вы стали искать на C все точки порядка 4.

2.6. Пусть $C: (y^2 = x^3 + ax + b) \subset \mathbb{R}^2$. Напишите программу для ЭВМ, которая изображает часть кривой C и выполняет групповую операцию, т. е. запрашивает координаты точек A и B , затем рисует соответствующие прямые и выдает координаты точки $A + B$ (работайте с вещественными переменными).

2.7. Пусть $C: (y^2 = x^3 + ax + b) \subset k^2$, $A = (x_1, y_1)$ и $B = (x_2, y_2)$. Покажите, как задать координаты точки $A + B$ в виде рациональных функций от x_1, y_1, x_2, y_2 . (Указание. Если $F(X)$ — многочлен третьей степени и вам известно два его корня, то, зная лишь один из коэффициентов F , можно найти и третий корень. Ответ на этот вопрос не является единственным, так как рациональные функции имеют много правильных представлений. Один из возможных ответов приводится в разд. (4.14).)

2.8. С помощью уравнения касательной прямой к кривой C в точке A найдите формулу для $2A$ относительно группового закона на C и проверьте, что она получается в пределе из соответствующей формулы для $A + B$ при B , стремящемся к A . (Указание. Воспользуйтесь упр. 2.7, а в случае необходимости обратитесь к разд. (4.14).)

2.9. Пусть x, z — координаты на плоскости k^2 и $f \in k[x, z]$. Запишем f в виде

$$f = a + bx + cz + dx^2 + exz + fz^2 + \dots$$

Задайте в терминах коэффициентов $a, b, c, \dots$ условия, которые должны выполняться, чтобы

(i) $P = (0, 0) \in C: (f = 0)$;

(ii) касательная прямая к C в точке P совпадала с $(z = 0)$;

(iii) P являлась точкой перегиба кривой C , а касательная прямая в точке P совпадала с $(z = 0)$.

(Напомним, что, согласно (2.12), $P \in C$ является точкой перегиба, если определена касательная прямая L и $f|_L$ имеет в точке P корень кратности, не меньшей 3.)

2.10. Пусть $C \subset \mathbb{P}_k^2$ — плоская кубика, и предположим, что $P \in C$ — точка перегиба. Докажите, что с помощью подходящей замены координат на $\mathbb{P}_k^2$ можно привести

C к нормальной форме $(Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3)$. (Указание. Выберите координаты так, чтобы P совпала с $(0, 1, 0)$, а касательная прямая в точке перегиба совпала с $(Z = 0)$. Тогда, согласно результатам предыдущего упражнения, в локальных координатах (x, z) Y войдет в единственный квадратичный по нему член Y^2Z , а остальные будут линейными по Y . Покажите, что от линейных по Y членов можно избавиться путем дополнения до полного квадрата.)

2.11. (Групповой закон на полукубической параболе.) Рассмотрим кривую $C: (z = x^3) \subset k^2$. Она является образом при биективном отображении $\varphi: k \rightarrow C$, а именно при $t \mapsto (t, t^3)$. Поэтому она наследует групповой закон аддитивной группы k . Докажите, что это единственный групповой закон на C , для которого точка $(0, 0)$ является нейтральным элементом и

$$P + Q + R = 0 \Leftrightarrow P, Q, R \text{ коллинеарны}$$

для всех $P, Q, R \in C$. (Указание. Вам поможет следующее тождество:

$$\det \begin{bmatrix} 1 & a & a^3 \\ 1 & b & b^3 \\ 1 & c & c^3 \end{bmatrix} = (a - b)(b - c)(c - a)(a + b + c).$$

С точки зрения проективной геометрии C является кривой $(Y^2Z = X^3)$, т. е. нашей старой знакомой, имеющей в начале координат касп, а в точке $(0, 1, 0)$ — перегиб. А суть дела заключается в том, что обычная конструкция определяет групповой закон на дополнении к особой точке.

2.12. (Задача поставлена Леонардо Пизанским по прозвищу Фибоначчи около 1220 г.) Докажите, что для целых чисел $u, v \in \mathbb{Z}$

$$u^2 + v^2 \text{ и } u^2 - v^2 \text{ являются квадратами} \Rightarrow v = 0.$$

Указание (принадлежит П. де Ферма, см. Cassels J. W. S., Journal of London Math. Soc. 41 (1966), p. 207):

Шаг 1. Сведите задачу к решению системы

$$x^2 = u^2 + v^2, \quad y^2 = u^2 - v^2, \quad (*)$$

где x, y, u, v являются попарно взаимно простыми.

Шаг 2. Рассмотрите остатки по модулю 4 и установите, что x, y, u должны быть нечетными, а v — четным.

Шаг 3. Покажите, что 4 пары сомножителей в левых частях приведенных ниже выражений не могут иметь общего множителя, не являющегося степенью 2:

$$\begin{aligned} (x - u)(x + u) &= v^2, \\ (u - y)(u + y) &= v^2, \\ (x - y)(x + y) &= 2v^2, \\ (2u - x - y)(2u + x + y) &= (x - y)^2. \end{aligned} \quad (**)$$

Шаг 4. Заменяя в случае необходимости u на $-u$, можно считать, что $4 \nmid x - y$. Рассмотрите теперь четность сомножителей левых частей соотношений (**) и докажете, что

$$x - u = 2v_1^2, \quad u - y = 2u_1^2, \quad x - y = 2x_1^2 \text{ и } 2u - x - y = 2y_1^2,$$

где $u_1, v_1, x_1, y_1 \in \mathbb{Z}$.

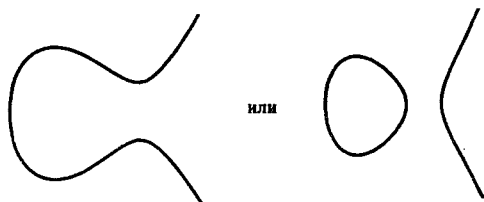
Шаг 5. Покажите, что u_1, v_1, x_1, y_1 является другим решением (*), для которого $v_1 < v$, и с помощью «бесконечного спуска» получите противоречие.

Сравните это рассуждение с доказательством в (2.2), которое проще только тем, что не приходится заботиться о двойках.

Добавление к гл. 1

Кривые и их род

(2.14) **Топология неособой кубики.** Легко видеть, что неособая плоская кубика $C: (y^2 = x^3 + ax + b) \subset \mathbb{P}_{\mathbb{R}}^2$ имеет один из следующих двух видов:



Таким образом, топологически C является либо одной окружностью, либо объединением двух окружностей (разумеется, если учитывать одну точку на бесконечности). Чтобы изучить этот вопрос над $\mathbb{C}$, воспользуемся другой нормальной формой

$$C: (y^2 = x(x-1)(x-\lambda)) \cup \{\infty\}.$$

Какова же топология $C \subset \mathbb{P}_{\mathbb{C}}^2$? Ответ — это тор:

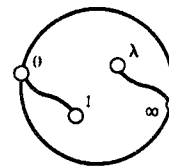


Идея доказательства заключается в том, чтобы рассмотреть отображение

$$\pi: C \rightarrow \mathbb{P}_{\mathbb{C}}^1, \text{ заданное формулами } (X, Y, Z) \mapsto (X, Z) \text{ и } \infty \mapsto (1, 0).$$

В аффинных координатах оно имеет вид $(x, y) \mapsto x$, т. е. является двулистным накрытием, соответствующим ветвям графика функции $y = \pm \sqrt{x(x-1)(x-\lambda)}$. Всем известно, что $\mathbb{P}_{\mathbb{C}}^1$ гомеоморфна римановой сфере S^2 (гомеоморфизм устанавливается с помощью

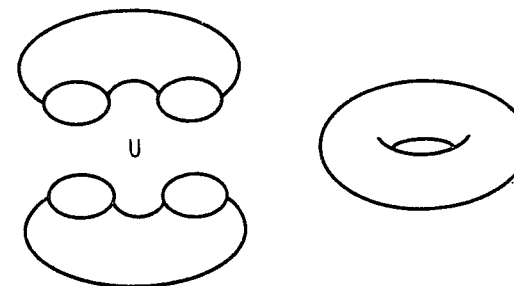
стереографической проекции). Рассмотрим на $\mathbb{P}_{\mathbb{C}}^1$ «функцию» $y(x) = \pm \sqrt{x(x-1)(x-\lambda)}$. Она двузначна вне точек $\{0, 1, \lambda, \infty\}$:



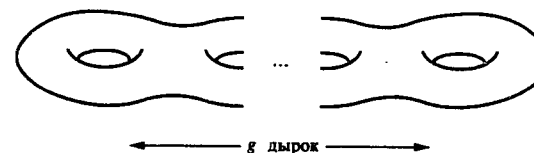
Разрежем $\mathbb{P}_{\mathbb{C}}^1$ вдоль двух путей 01 и $\lambda\infty$. Двулистное накрытие распадется на 2 куска, на каждом из которых функция y однозначна. Таким образом,



(штриховка показывает, как соединяются два куска при склеивании). Чтобы понять, что происходит, раскроем разрезы:



(2.15) **Обсуждение понятия рода.** Неособая проективная кривая C имеет над $\mathbb{C}$ единственный топологический инвариант, а именно род $g = g(C)$:



Например, аффинная кривая $C: (y^2 = f_{2g+1}(x) = \prod_i (x - a_i)) \subset \mathbb{C}^2$,

Топология

 C гомеоморфна:

фундаментальная группа:

Алгебраическая/комплексно-аналитическая геометрия

вложения, явные описания:

автоморфизмы:

модули:

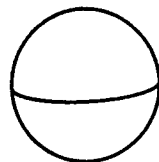
Дифференциальная геометрия

существует естественный класс римановых метрик постоянной кривизны:

Диофантовы задачи

если $k = \mathbb{Q}$ или k — числовое поле, т. е. $[k : \mathbb{Q}] < \infty$ то:

$g = 0$



одинсвязна

$$C \cong \mathbb{P}_C^1 \\ \cong C_2 \subset \mathbb{P}_C^2$$

3-мерная группа проективных преобразований

отсутствуют

постоянная положительная кривизна

$$C_k = \emptyset \text{ или } \mathbb{P}_k^1$$

$g = 1$



$$\pi_1 = \mathbb{Z} \oplus \mathbb{Z}$$

$$C \cong C_3 \subset \mathbb{P}_C^2 \\ \cong \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$$

сдвиги, определяемые групповым законом $\times$ конечная группа1 модуль (двойное отношение или j -инвариант)

нулевая кривизна (т. е. плоская)

 C_k — конечно порожденная абелева группа (теорема Морделла—Вейля)

$g \geq 2$

похожа на свободную группу с $2g$ образующимине имеют простого описания, но, например, почти все кривые рода 3 изоморфны неособым кривым $C_4 \subset \mathbb{P}_C^2$

конечная группа

 $3g - 3$ модулей

постоянная отрицательная кривизна

 C_k — конечное множество (теорема Фальтингса, гипотеза Морделла)

где f_{2g+1} — многочлен от x степени $2g+1$ с попарно различными корнями a_i , может быть соотнесена с римановой поверхностью $\sqrt{f}$ в точности так же, как в разд. (2.14), и может рассматриваться как двулистное накрытие римановой сферы $\mathbb{P}_{\mathbb{C}}^1$, разветвленное в $2g+1$ точках a_i и точке ∞ . То же рассуждение показывает, что род этой кривой равен g . В качестве другого примера укажем, что род неособой плоской кривой $C_d \subset \mathbb{P}_{\mathbb{C}}^2$ степени d задается формулой

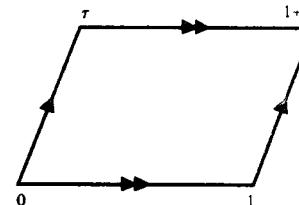
$$g = g(C_d) = \binom{d-1}{2}.$$

(2.16) Реклама. Комплексные кривые (= компактные римановы поверхности) встречаются в огромном числе математических задач от диофантовой арифметики, теории функций комплексной переменной и топологии в малых размерностях до уравнений математической физики. Поэтому спешите купить комплексную кривую сегодня же.

Свойства кривой в необыкновенно высокой степени определяют ее родом, а в особенности одной из трех возможностей $g=0$, $g=1$ или $g \geq 2$. Наиболее примечательные аспекты этого разбиения на три класса приведены в таблице на стр. 50—51. Эти сведения входят в обязательный минимум знаний каждого математика.

В качестве неполного решения диофантовой задачи, приведенной в разд. (1.1)—(1.2), а затем еще раз в (2.1), укажем, что кривая может быть параметризована рациональными функциями тогда и только тогда, когда $g=0$. При рассмотрении конкретного поля может оказаться, что данная кривая рода 0 совсем не имеет k -значных точек (например, коника из (1.2)), но если у нее есть хотя бы одна точка, то ее можно параметризовать над k так, чтобы ее k -значные точки находились в биективном соответствии с $\mathbb{P}_k^1$. Любая кривая рода 1 изоморфна кубике, подобной той, которая была описана выше, и на k -значных точках определен групповой закон (конечно, при условии, что это множество непусто, так как не существует такого объекта, как пустая группа. Если k — числовое поле, например, $k = \mathbb{Q}$, то k -значные точки образуют абелеву группу, которая является конечно порожденной (теорема Морделла—Вейля). Что же касается кривой, род которой ≥ 2 , то в настоящее время известно, что число ее k -значных точек конечно. Это — знаменитая теорема, доказанная Фальтингсом в 1983 г., за которую он удостоился в 1986 г. Филдсовской премии. Таким образом, например, для любого $n \geq 4$ кривая Ферма $x^n + y^n = 1$ содержит не более конечного числа рациональных точек.

Над $\mathbb{C}$ кривая C рода 1 топологически является тором, и на ней определена групповая операция, так что с аналитической точки зрения она представляется в виде $C \cong \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$:



Изоморфизм между этим факторпространством и плоской кривой $C_3 \subset \mathbb{P}_{\mathbb{C}}^2$ задается голоморфным отображением $\varphi: \mathbb{C} \rightarrow C_3$, т. е. своего рода «параметризацией» кривой C_3 , однако φ не выражается через рациональные функции (в силу (2.2)) и является бесконечнолистным накрытием. Именно теория двоякопериодических функций комплексной переменной явилась одной из вершин анализа 19-го века ($\wp$ -функция Вейерштрасса, θ -функция Римана).

Другим важным обстоятельством является то, что различные периоды τ , как правило, соответствуют разным кривым, т. е. все они гомеоморфны стандартному тору $S^1 \times S^1$, но не изоморфны как алгебраические или комплексно-аналитические кривые. Период τ является *модулем*, т. е. комплексным параметром, управляющим изменением комплексной структуры на заданном топологическом многообразии $S^1 \times S^1$.

Читателю, желающему больше узнать о кривых, можно порекомендовать книгу [Mamford D. Curves and their Jacobians], первая часть которой написана достаточно неформально, или книгу [Клеменс].

§ 3. Аффинные многообразия и Nullstellensatz

Большую часть первой половины этого параграфа составляет материал по коммутативной алгебре. Отметим, что здесь и далее термин *кольцо* обозначает коммутативное кольцо с единицей. Так как коммутативная алгебра не является основным предметом этой книги, то ниже я постараюсь, чтобы излишние детали нас не тормозили.

(3.1) Предложение-определение. Следующие условия в кольце A эквивалентны:

- (i) Каждый идеал $I \subset A$ конечно порожден, т. е. для каждого идеала $I \subset A$ существуют такие $f_1, \dots, f_k \in I$, что $I = (f_1, \dots, f_k)$.
 (ii) Условие обрыва возрастающих цепей: каждая возрастающая цепь

$$I_1 \subset \dots \subset I_m \subset \dots$$

идеалов кольца A стабилизируется, т. е. начиная с некоторого места, $I_N = I_{N+1} = \dots$.

- (iii) Каждое непустое множество идеалов в кольце A имеет максимальный элемент.

Если выполнены эти условия, то кольцо называется нётеровым.

Доказательство. (i) $\Rightarrow$ (ii). Рассмотрим цепочку $I_1 \subset \dots \subset I_m \subset \dots$ и положим $I = \bigcup I_m$. Очевидно, что I также является идеалом. Если $I = (f_1, \dots, f_k)$, то каждый из элементов f_i принадлежит $I_{m(i)}$ для некоторого $m(i)$. Взяв $m = \max(m(i))$, получим, что $I = I_m$, и цепочка стабилизируется, начиная с члена I_m .

Импликация (ii) $\Rightarrow$ (iii) очевидна. (На самом деле в доказательстве используется аксиома выбора.)

(iii) $\Rightarrow$ (i). Пусть I — произвольный идеал. Положим $\Phi = \{J \subset I \mid J \text{ — конечно порожденный идеал}\}$. Согласно свойству (iii), Φ имеет максимальный элемент, который мы обозначим через J_0 . Но тогда $J_0 = I$, поскольку в противном случае для любого $f \in I \setminus J_0$ идеал $J_0 + Af$ также является конечно порожденным и строго содержит J_0 . Ч.т.д.

Для тренировки докажите, что $\mathbb{Z}$ и $k[x]$ являются нётеровыми кольцами.

(3.2) Предложение. (i) Пусть A — нётерово кольцо, а I — некоторый идеал в A . Тогда факторкольцо $B = A/I$ является нётеровым.

(ii) Пусть A — нётерова область целостности, $A \subset K$ — ее поле частных, а $S \subset A$ — некоторое подмножество, не содержащее нуля. Положим

$$B = A[S^{-1}] = \{a/b \in K \mid a \in A, b \in S\} \text{ или является произведением элементов из } S\}.$$

Тогда B также является нётеровым.

Доказательство сводится к следующему упражнению: опишите в обоих случаях идеалы в кольце B через идеалы в кольце A . (Некоторые указания см. в упр. 3.4).

(3.3) Теорема (Гильберта о базисе). Если A — нётерово кольцо, то кольцо $A[X]$ также нётерово.

Доказательство. Пусть J — некоторый идеал в $A[X]$. Докажем, что J конечно порожден. Определим идеал J_n старших коэффициентов многочленов n -й степени, принадлежащих идеалу J , следующим образом:

$$J_n = \{a \in A \mid \exists f = aX^n + b_{n-1}X^{n-1} + \dots + b_0 \in J\}.$$

Тогда J_n является идеалом в A и такие идеалы вложены друг в друга, т. е. $J_n \subset J_{n+1}$. (Докажите это, пожалуйста, самостоятельно.) Используя свойство (ii) стабилизации возрастающих цепей, получаем, что существует номер N , такой, что

$$J_N = J_{N+1} = \dots$$

Теперь систему образующих идеала J можно построить следующим образом. Пусть $a_{i1}, \dots, a_{im(i)}$ для $i \leq N$ — образующие идеала J_i . Обозначим (как и в определении J_i) для каждого a_{ik} через $f_{ik} = a_{ik}X^i + \dots \in J$ многочлен i -й степени из J , старший коэффициент которого равен a_{ik} .

Покажем, что множество

$$\{f_{ik} \mid i = 0, \dots, N, k = 1, \dots, m(i)\}$$

порождает J . Рассмотрим принадлежащий J многочлен g степени m . Его старший член равен bX^m , где $b \in J_m$. Тогда в силу свойств идеала J_m имеем $b = \sum c_{m'k} a_{m'k}$ (здесь $m = m'$, если $m \leq N$, в противном случае $m' = N$). Рассмотрим теперь $g_1 = g - X^{m-m'} \cdot \sum c_{m'k} f_{m'k}$. Коэффициент при члене степени m равен нулю по построению, и, таким образом, $\deg g_1 \leq \deg g - 1$. Следовательно, по предположению индукции g записывается в виде комбинации f_{ik} , которые, таким образом, порождают J . Ч.т.д.

Следствие. Если k — поле, то любая конечно порожденная k -алгебра является нётеровой.

Любая конечно порожденная k -алгебра является кольцом вида $A = k[a_1, \dots, a_n]$. Значит, A порождается (как кольцо) полем k и элементами $a_1, \dots, a_n$. Очевидно, что любое такое кольцо изоморфно факторкольцу кольца многочленов, $A \cong k[X_1, \dots, X_n]/I$. Поле является нётеровым кольцом, и индукцией, использующей теорему (3.3), легко показать, что $k[X_1, \dots, X_n]$ — нётерово кольцо. Следовательно, его факторкольцо является нётеровым в силу (3.2(ii)). Ч.т.д.

(3.4) Соответствие V . Пусть k — произвольное поле, а $A = k[X_1, \dots, X_n]$.

Следуя странному обыкновению алгебраических геометров¹⁾, обозначим через $\mathbb{A}_k^n = k^n$ n -мерное аффинное пространство над полем k . Для данного многочлена $f(X_1, \dots, X_n) \in A$ и точки $P = (a_1, \dots, a_n) \in \mathbb{A}_k^n$ будем рассматривать элемент $f(a_1, \dots, a_n) \in k$ как «значение функции f в точке P ».

Определим соответствие

$$\{\text{идеалы } J \subset A\} \xrightarrow{V} \{\text{подмножества } X \subset \mathbb{A}_k^n\}$$

следующим образом:

$$J \mapsto V(J) = \{P \in \mathbb{A}_k^n \mid f(P) = 0 \text{ для всех } f \in J\}.$$

Определение. Подмножество $X \subset \mathbb{A}_k^n$ называется *алгебраическим множеством*, если $X = V(I)$ для некоторого I . (Это — то же самое, что (алгебраическое) многообразие, но последний термин желательно зарезервировать.) Заметим, что в силу следствия (3.3) идеал I

¹⁾ $\mathbb{A}^n$ — алгебраическое многообразие, в то время как k^n — это всего лишь множество точек. Читатель может при желании считать это чистым педантизмом (см. разд. (4.6), а также (8.3)).

конечно порожден. Если $I = (f_1, \dots, f_r)$, то очевидно, что

$$V(I) = \{P \in \mathbb{A}_k^n \mid f_i(P) = 0 \text{ для всех } i = 1, \dots, r\},$$

т. е. алгебраическое множество — это просто совокупность точек, удовлетворяющих конечному числу полиномиальных уравнений.

Если $I = (f)$ — главный идеал, то мы будем использовать обозначение $V(f)$ для $V(I)$ (это разумеется, то же самое, что $V: (f=0)$ в обозначениях § 1 и 2).

(3.5) Предложение-определение. Соответствие V обладает следующими формальными свойствами:

- (i) $V(0) = \mathbb{A}_k^n$; $V(A) = \emptyset$;
- (ii) $I \subset J \Rightarrow V(I) \supset V(J)$;
- (iii) $V(I_1 \cap I_2) = V(I_1) \cup V(I_2)$;
- (iv) $V\left(\sum_{\lambda \in \mathbb{Z}} I_\lambda\right) = \bigcap_{\lambda \in \mathbb{Z}} V(I_\lambda)$.

Таким образом, алгебраические подмножества в $\mathbb{A}_k^n$ являются замкнутыми множествами в некоторой топологии на $\mathbb{A}_k^n$, называемой топологией Зарисского.

Сформулированные свойства очевидны, за исключением включения $\subset$ в (iii). Для его доказательства предположим, что $P \notin V(I_1) \cup V(I_2)$; тогда существуют такие $f \in I_1$ и $g \in I_2$, что $f(P) \neq 0$ и $g(P) \neq 0$. Таким образом, $fg \in I_1 \cap I_2$, но $fg(P) \neq 0$. Следовательно, $P \notin V(I_1 \cap I_2)$. Ч.т.д.

Топология Зарисского на $\mathbb{A}_k^n$ индуцирует топологию на любом алгебраическом множестве $X \subset \mathbb{A}_k^n$. Замкнутыми подмножествами в X являются алгебраические подмножества.

Важно отметить, что топология Зарисского на алгебраическом многообразии является очень слабой и сильно отличается от привычной топологии метрических пространств, таких, как $\mathbb{R}^n$. Например, замкнутое по Зарисскому подмножество в $\mathbb{A}_k^1$ либо совпадает с $\mathbb{A}_k^1$, либо конечно (описание топологии Зарисского на $\mathbb{A}_k^2$ см. в упр. 3.12). Если $k = \mathbb{R}$ или $k = \mathbb{C}$, то замкнутые по Зарисскому множества замкнуты и в обычной топологии, так как многочлены являются непрерывными функциями. В действительности они являются очень специальными открытыми или замкнутыми подмножествами. Так, например, непустое открытое по Зарисскому подмножество в $\mathbb{R}^n$ является дополнением к подмногообразию и тем самым автоматически плотно в $\mathbb{R}^n$.

Топология Зарисского может вызвать затруднение у некоторых студентов. Так как она употребляется только как удобный язык и

ее содержательный аспект незначителен, это трудности скорее психологического, чем технического характера.

(3.6) Соответствие I . Определим некоторый вариант соответствия, обратного к соответствию V ,

$$\{\text{идеалы } J \subset A\} \xleftarrow{I} \{\text{подмножества } X \subset \mathbb{A}_k^n\}$$

формулой

$$I(X) = \{f \in A \mid f(P) = 0 \text{ для всех } P \in X\} \leftarrow X,$$

т. е. подмножество X отображается в идеал функций, обращающихся на X в нуль.

Предложение. (а) $X \subset Y \Rightarrow I(X) \supset I(Y)$;

(б) для любого подмножества $X \subset \mathbb{A}_k^n$ имеем $X \subset V(I(X))$; равенство выполняется тогда и только тогда, когда X — алгебраическое множество.

(с) для любого $J \subset A$ имеем $J \subset I(V(J))$ (последнее включение может быть строгим).

Доказательство. Пункт (а) тривиален. Включения в пп. (б) и (с) являются тавтологиями. А именно, так как $I(X)$ определяется как множество функций, обращающихся в нуль во всех точках, принадлежащих X , то для любой точки из X все функции из $I(X)$ обращаются в ней в нуль. «Конечно, это совершенно неоспоримо; я и сам так, Пятачок, думаю».

Оставшаяся часть п. (б) доказывается легко. Если $X = V(I(X))$, то X является алгебраическим множеством, так как оно есть множество нулей некоторого идеала. И обратно, если $X = V(I_0)$ является алгебраическим множеством, то $I(X)$ по крайней мере содержит I_0 , так что $V(I(X)) \subset V(I_0) = X$.

Есть две различные причины, по которым включение $J \subset I(V(J))$ в п. (с) может оказаться строгим. Их важно разобрать, так как они подсказывают правильную формулировку Nullstellensatz.

Пример 1. Предположим, что поле k не является алгебраически замкнутым, и пусть $f \in k[X]$ — нетривиальный (отличный от константы) многочлен, не имеющий корней в поле k . Рассмотрим идеал $J = (f) \subset k[X]$. Тогда $J \neq k[X]$, так как $1 \notin J$. Но

$$V(J) = \{P \in \mathbb{A}_k^1 \mid f(P) = 0\} = \emptyset.$$

Следовательно, $I(V(J)) = k[X]$ (так как любая функция обращается в нуль во всех точках пустого множества).

Значит, если рассматриваемое поле не является алгебраически замкнутым, то у нас может не оказаться нужного количества нулей. Вот довольно подходящий пример: многочлен $X^2 + Y^2$ в $\mathbb{R}^2$, который определяет единственную точку $P = (0, 0)$, т. е. $V(X^2 + Y^2) = \{P\}$. Однако существует много многочленов, не кратных $X^2 + Y^2$, которые также обращаются в нуль на $\{P\}$, и на самом деле $I(P) = (X, Y)$.

Пример 2. Для любого $f \in k[X_1, \dots, X_n]$ и $a \geq 2$ многочлен f^a определяет ту же совокупность точек, что и f , т. е. $f^a(P) = 0 \Leftrightarrow f(P) = 0$. Поэтому $V(f^a) = V(f)$ и $f \in I(V(f^a))$, но, как правило, $f \notin (f^a)$. Это видно уже на примере $\mathbb{R}^2$: в § 1 упоминалась «двойная прямая», определяемая уравнением $X^2 = 0$. Единственный смысл, который можно этому придать, заключается в том, что следует считать прямую ($X = 0$) двукратной. Но сама прямая как множество точек не подозревает ни о какой кратности.

(3.7) Неприводимые алгебраические множества. Алгебраическое множество $X \subset \mathbb{A}_k^n$ называется *неприводимым*, если не существует его представления

$$X = X_1 \cup X_2, \quad X_1, X_2 \subsetneq X$$

в виде объединения двух собственных алгебраических подмножеств. Например, алгебраическое подмножество $V(xy) \subset \mathbb{A}_k^2$ состоит из двух координатных осей. Очевидно, что оно представляется в виде объединения $V(x)$ и $V(y)$ и, следовательно, приводимо.

Предложение. (а) Если $X \subset \mathbb{A}_k^n$ — алгебраическое множество, а $I(X)$ — соответствующий идеал, то

X неприводимо тогда и только тогда, когда идеал $I(X)$ прост;

(б) любое алгебраическое множество имеет (единственное) разложение вида

$$X = X_1 \cup \dots \cup X_r, \quad (*)$$

где X_i неприводимы и $X_i \not\subset X_j$ для $i \neq j$.

Подмножества X_i в формуле (*) называются *неприводимыми компонентами* множества X .

Доказательство. (а) В действительности я докажу, что X приводимо $\Leftrightarrow I(X)$ не прост.

($\Rightarrow$) Предположим, что $X = X_1 \cup X_2$, где X_1, X_2 — собственные алгебраические подмножества множества X . Условие, что X_1 является собственным подмножеством в X , означает, что существует $f_1 \in I(X_1) \setminus I(X)$. Аналогично, из того, что X_2 — собственное подмножество в X , следует существование $f_2 \in I(X_2) \setminus I(X)$. Произведение $f_1 f_2$ обращается в нуль во всех точках множества X , т. е. $f_1 f_2 \in I(X)$. Следовательно, $I(X)$ не прост.

($\Leftarrow$) Предположим, что $I(X)$ не прост, тогда существуют $f_1, f_2 \notin I(X)$, такие, что $f_1 f_2 \in I(X)$. Пусть $I_1 = (I(X), f_1)$ и $V(I_1) = X_1$; тогда X_1 строго содержится в X и является его алгебраическим подмножеством. Аналогично, положив $I_2 = (I(X), f_2)$ и $V(I_2) = X_2$, получим, что X_2 строго содержится в X . Но $X \subset X_1 \cup X_2$, ибо для всех $P \in X$ из $f_1 f_2(P) = 0$ следует, что либо $f_1(P) = 0$, либо $f_2(P) = 0$.

(b) Прежде всего докажем следующее утверждение: алгебраические подмножества в $\mathbb{A}_k^n$ удовлетворяют условию обрыва убывающих цепей, т. е. произвольная цепочка

$$X_1 \supset X_2 \supset \dots \supset X_n \supset \dots$$

стабилизируется на некотором месте $X_N = X_{N+1} = \dots$. Это вытекает из стабилизации возрастающей цепи идеалов

$$I(X_1) \subset I(X_2) \subset \dots \subset I(X_n) \subset \dots$$

Таким образом, в точности, как в предложении (3.1), получаем, что

любое непустое множество Φ алгебраических подмножеств (!)

в $\mathbb{A}_k^n$ имеет минимальный элемент.

Для доказательства (b) выберем теперь в качестве Φ множество алгебраических подмножеств в $\mathbb{A}_k^n$, не имеющих разложения (*). Если $\Phi = \emptyset$, то п. (b) доказан. С другой стороны, если $\Phi \neq \emptyset$, то в силу утверждения (!) существует минимальный элемент $X \in \Phi$, что сразу приводит к одному из следующих двух противоречий. Если X неприводимо, то $X \notin \Phi$ — противоречие. Если X приводимо, то $X = X_1 \cup X_2$, где X_1, X_2 строго содержатся в X , и $X_1, X_2 \notin \Phi$ в силу минимальности $X \in \Phi$. Итак, каждое из X_1, X_2 обладает разложением (*) в объединение неприводимых компонент; взяв объединение этих объединений, получим разложение (*) для X , а значит, $X \notin \Phi$. Это противоречие доказывает, что $\Phi = \emptyset$; тем самым решается вопрос о существовании из п. (b). Доказательство единственности является легким упражнением (см. упр. 3.8). Ч.т.д.

Приведенное доказательство п. (b) является типичным образцом рассуждения алгебраистов. Будучи логически безупречным, оно по-

что полностью затемняет существо дела. В действительности суть состоит в том, что если X не является неприводимым, то оно разлагается в объединение $X = X_1 \cup X_2$. То же самое имеет место для X_1, X_2 и т. д. В конце концов мы должны добраться до неприводимых алгебраических множеств, так как иначе возникала бы бесконечная убывающая цепочка.

(3.8) Теперь я перейду к формулировке и доказательству Nullstellensatz. Любое ее доказательство обязательно содержит некоторую внутреннюю трудность, и я предпочитаю разбить его на 2 части. Сначала сформулирую без доказательства одно утверждение из коммутативной алгебры, которое будет доказано в (3.15) ниже (в действительности некоторые части этого доказательства будут иметь явно геометрический смысл).

Трудный факт. Пусть k — (бесконечное) поле и $A = k[a_1, \dots, a_n]$ — конечно порожденная k -алгебра. Тогда

$$A \text{ — поле} \Rightarrow A \text{ алгебраично над } k.$$

Для того чтобы хотя бы приблизительно дать представление о том, почему это утверждение верно, заметим, что если $t \in A$ трансцендентно над k , то $k[t]$ является кольцом многочленов и, таким образом, *содержит бесконечно много простых элементов* (согласно рассуждению Евклида). Следовательно, расширение $k \subset k(t)$ не является конечно порожденным как k -алгебра, так как среди знаменателей конечного числа элементов $p_i/q_i \in k(t)$ может содержаться только конечное число простых.

(3.9) **Определение.** Пусть I — идеал в кольце A ; его *радикалом* называется

$$\text{rad } I = \sqrt{I} = \{f \in A \mid f^n \in I \text{ для некоторого } n\}.$$

$\text{rad } I$ является идеалом, так как из того, что $f, g \in \text{rad } I$, вытекает, что $f^n, g^m \in I$ для некоторых n и m . Следовательно,

$$(f + g)^r = \sum \binom{r}{a} f^a g^{r-a} \in I, \text{ если } r \geq n + m - 1.$$

Идеал I называется *радикальным*, если $I = \text{rad } I$.

Заметим, что простой идеал радикален. Нетрудно показать, что для области с однозначным разложением на множители, такой, как $k[X_1, \dots, X_n]$, радикал $\text{rad } I$ главного идеала вида $I = (f)$, где $f = \prod f_i^{n_i}$ (разложение в произведение степеней различных простых сомножителей) равен (f_{rad}) , где $f_{\text{rad}} = \prod f_i$.

(3.10) Nullstellensatz (теорема Гильберта о нулях). Пусть k — алгебраически замкнутое поле. Тогда

(а) Любой максимальный идеал кольца многочленов $A = k[X_1, \dots, X_n]$ имеет вид $m_P = (X_1 - a_1, \dots, X_n - a_n)$ для некоторой точки $P = (a_1, \dots, a_n) \in \mathbb{A}_k^n$, т. е. совпадает с идеалом $I(P)$ всех функций, обращающихся в точке P в нуль.

(б) Пусть $J \subset A$ — некоторый идеал, отличный от A ; тогда $V(J) \neq \emptyset$.

(с) Для любого $J \subset A$

$$I(V(J)) = \text{rad } J.$$

Основное содержание теоремы заключено в п. (б), утверждающем, что если идеал J отличен от всего кольца $k[X_1, \dots, X_n]$, то он имеет в $\mathbb{A}_k^n$ нули. Заметим, что утверждение п. (б) абсолютно неверно над алгебраически незамкнутым полем k , так как если $f \in k[X]$ — многочлен, отличный от константы, то порождаемый им идеал не совпадает со всем кольцом $k[X]$, однако вполне может оказаться, что $V(f) = \emptyset \subset \mathbb{A}_k^1$. Название теоремы (Nullstelle = нуль многочлена + Satz = теорема) должно помочь вам запомнить ее содержание. (Советую вам придерживаться немецкого названия, если вы не желаете прослыть невеждами¹⁾.)

Следствие. Соответствия V и I

$$\begin{array}{ccc} \{\text{идеалы } I \subset A\} & \xleftrightarrow{V, I} & \{\text{подмножества } X \subset \mathbb{A}_k^n\} \\ \cup & & \cup \\ \text{индуцируют биекции} & & \\ \{\text{радикальные идеалы}\} & \leftrightarrow & \{\text{алгебраические подмножества}\} \\ \cup & & \cup \\ \text{и} & & \\ \{\text{простые идеалы}\} & \leftrightarrow & \{\text{неприводимые алгебраические подмножества}\}. \end{array}$$

Справедливость этого утверждения следует из того, что в силу (3.6(б)) для любого алгебраического подмножества X имеем $V(I(X)) = X$, и того, что в силу (3.10 (с)) для любого радикального идеала J $I(V(J)) = J$.

¹⁾ Этот совет автора относится, разумеется, к англоязычному читателю, для которого такая терминология почти традиционна, но мы сочли возможным последовать ему и в русском переводе. — Прим. перев.

Доказательство Nullstellensatz (использующее (3.8)).

(а) Пусть $m \subset k[X_1, \dots, X_n]$ — максимальный идеал. Обозначим через K кольцо $k[X_1, \dots, X_n]/m$, а через φ — композицию естественных отображений $\varphi: k[X_1, \dots, X_n] \rightarrow K$. Тогда K является полем (так как идеал m максимален) и конечно порождено как k -алгебра (так как оно порождается образами элементов X_i). Поэтому в силу (3.8) $\varphi: k \rightarrow K$ является алгебраическим расширением полей. Но k алгебраически замкнуто, следовательно, φ — изоморфизм.

Для всех i элемент $X_i \in k[X_1, \dots, X_n]$ отображается в некоторый элемент $b_i \in K$. Поэтому, если положить $a_i = \varphi^{-1}(b_i)$, то получим $X_i - a_i \in \text{Ker } \varphi = m$. Следовательно, существуют $a_1, \dots, a_n \in k$, такие, что $(X_1 - a_1, \dots, X_n - a_n) \subset m$. С другой стороны, очевидно, что в левой части стоит максимальный идеал, так что $(X_1 - a_1, \dots, X_n - a_n) = m$, и это доказывает (а).

Импликация (а) $\Rightarrow$ (б) доказывается просто. Если $J \neq A = k[X_1, \dots, X_n]$, то существует такой максимальный идеал m кольца A , что $J \subset m$ (существование m легко получить из условия обрыва возрастающих цепей). Согласно (а), идеал m имеет вид $m = (X_1 - a_1, \dots, X_n - a_n)$. Тогда условие $J \subset m$ означает попросту, что $f(P) = 0$ для всех $f \in J$, где $P = (a_1, \dots, a_n)$. Следовательно, $P \in V(J)$.

Доказательство импликации (б) $\Rightarrow$ (с) основано на следующем хитром трюке. Пусть $J \subset k[X_1, \dots, X_n]$ — любой идеал и $f \in k[X_1, \dots, X_n]$. Введем дополнительную переменную Y и рассмотрим новый идеал

$$J_1 = (J, fY - 1) \subset k[X_1, \dots, X_n, Y],$$

порожденный идеалом J и $fY - 1$. Грубо говоря, $V(J_1)$ является многообразием, состоящим из тех $P \in V(J)$, для которых $f(P) \neq 0$. Точнее, точка $Q \in V(J_1) \subset \mathbb{A}_k^{n+1}$ является набором из $n + 1$ чисел $Q = (a_1, \dots, a_n, b)$, таких, что

$$g(a_1, \dots, a_n) = 0 \text{ для всех } g \in J, \text{ т. е. } P = (a_1, \dots, a_n) \in V(J),$$

и

$$f(P) \cdot b = 1, \text{ т. е. } f(P) \neq 0 \text{ и } b = f(P)^{-1}.$$

Предположим теперь, что $f(P) = 0$ для всех $P \in V(J)$. Тогда из только что сделанного замечания вытекает, что $V(J_1) = \emptyset$. Теперь из (б) следует, что $1 \in J_1$, т. е. существует разложение

$$1 = \sum g_i f_i + g_0(fY - 1) \in k[X_1, \dots, X_n, Y], \quad (**)$$

где $f_i \in J$, а $g_0, g_i \in k[X_1, \dots, X_n, Y]$.

Рассмотрим, каким образом входит Y в правую часть формулы (**). Кроме множителя во втором члене, явно содержащего Y , он может входить во все g_i . Предположим, что Y^N — наибольшая из степеней Y , входящих в g_0 и все g_i . Если умножить обе части формулы (**) на f^N , то получится соотношение вида

$$f^N = \sum G_i(X_1, \dots, X_n, fY)f_i + G_0(X_1, \dots, X_n, fY)(fY - 1), (***)$$

где G_i — это просто $f^N g_i$, записанные как многочлены от переменных $X_1, \dots, X_n$ и fY .

(***) есть не что иное, как равенство двух многочленов в кольце $k[X_1, \dots, X_n, Y]$, приведя которое по модулю $fY - 1$ получим

$$f^N = \sum h_i(X_1, \dots, X_n)f_i \in k[X_1, \dots, X_n, Y]/(fY - 1).$$

Обе части этого уравнения являются элементами кольца $k[X_1, \dots, X_n]$. Так как естественный гомоморфизм $k[X_1, \dots, X_n] \hookrightarrow k[X_1, \dots, X_n, Y]/(fY - 1)$ инъективен (он является просто включением $k[X_1, \dots, X_n]$ в $k[X_1, \dots, X_n][f^{-1}]$ (как подкольца в его поле частных)), то

$$f^N = \sum h_i(X_1, \dots, X_n)f_i \in k[X_1, \dots, X_n],$$

т. е. $f^N \in J$ для некоторого N . Ч. т. д.

Замечание. В некоторых учебниках доказательство сокращается благодаря тому, что (**) объявляется тождеством. Тем самым оно остается справедливым при подстановке $Y = f^{-1}$. Это, безусловно, верно, но я предпочел привести более детальное доказательство.

(3.11) **Примеры.** (а) Гиперповерхности. Простейшим примером многообразия является гиперповерхность $V(f): (f = 0) \subset \mathbb{A}_k^n$. Если k алгебраически замкнуто, то имеет место очевидное соответствие между неприводимыми элементами $f \in k[X_1, \dots, X_n]$ и неприводимыми гиперповерхностями. А именно, из Nullstellensatz следует, что два различных неприводимых многочлена f_1 и f_2 (не кратные друг другу) определяют различные гиперповерхности $V(f_1)$ и $V(f_2)$. Это совсем неочевидно (и, например, неверно над $\mathbb{R}$), хотя и может быть доказано без использования Nullstellensatz с помощью *теории исключений* — намного более явного метода, в котором явственно ощущается колорит XIX века (см. упр. 3.13).

(б) За исключением случая гиперповерхностей, большинство алгебраических многообразий задаются «кучей» уравнений. Вопреки интуиции обычно для задания идеала $I(X)$ требуется много образу-

ющих (намного больше коразмерности X). Я приведу пример кривой $C \subset \mathbb{A}_k^3$, для задания идеала $I(C)$ которой требуется 3 образующих. Предположим, что k — бесконечное поле. Рассмотрим сначала идеал $J = (uw - v^2, u^3 - vw)$. Он не прост, так как

$$J \ni w(uw - v^2) - v(u^3 - vw) = u(w^2 - u^2v),$$

но $u, w^2 - u^2v \notin J$. Поэтому

$$V(J) = V(J, u) \cup V(J, w^2 - u^2v).$$

Очевидно, что $V(J, u)$ — это прямая ($u = v = 0$). Утверждается, что другая компонента $C = V(J, w^2 - u^2v)$ является неприводимой кривой. Действительно, C задается системой

$$uw = v^2, \quad u^3 = vw, \quad w^2 = u^2v.$$

Я утверждаю, что $C \subset \mathbb{A}^3$ является образом отображения $\varphi: \mathbb{A}^1 \rightarrow C \subset \mathbb{A}^3$, заданного формулой $t \mapsto (t^3, t^4, t^5)$. Чтобы убедиться в этом, следует заметить, что если $u \neq 0$, то $v, w \neq 0$. Положим $t = v/u$; тогда $t = w/v$ и $t^2 = (v/u)(w/v) = w/u$. Следовательно, $v = w^2/u^2 = t^4$, $u = v/(v/u) = t^4/t = t^3$ и $w = tv = t^5$.

Значит, C неприводима, так как если $C = X_1 \cup X_2$, где $X_i \subset C$, и $f_i(u, v, w) \in I(X_i)$, то для всех t один из $f_i(t^3, t^4, t^5)$ обязательно обращается в нуль. Так как ненулевой многочлен имеет не более конечного числа нулей, то один из f_1 и f_2 должен тождественно равняться нулю, а значит, $f_i \in I(C)$.

Этот пример есть образец изящного мономиального задания. Вообще же угадать неприводимые компоненты многообразия довольно трудно, а еще сложнее доказать их неприводимость. Аналогичный пример приводится в упр. 3.11.

(3.12) **Конечные алгебры.** Перейдем теперь к доказательству (3.8). Пусть $A \subset B$ — кольца. Как обычно, B называется *конечно порожденным над A* (или конечно порожденным как A -алгебра), если существует конечное число элементов $b_1, \dots, b_n$, таких, что $B = A[b_1, \dots, b_n]$, т. е. если B как кольцо конечно порождено кольцом A и элементами $b_1, \dots, b_n$.

Сравните это определение со следующим: B — *конечная A -алгебра*, если существует конечное число элементов $b_1, \dots, b_n$, таких, что $B = Ab_1 + \dots + Ab_n$, т. е. B — конечно порождена как A -модуль. Здесь имеется существенное различие между порождаемостью как кольца (когда допускаются любые полиномиальные выражения от b_i) и порождаемостью как модуля (когда b_i могут входить лишь линейно). Например, $k[X]$ является конечно порожденной k -алгеб-

рой (она порождается одним элементом X), но не является конечной k -алгеброй (так как ее размерность как k -векторного пространства бесконечна).

Предложение. (i) Пусть $A \subset B \subset C$ — кольца. Тогда, если B — конечная A -алгебра и C — конечная B -алгебра, то C — конечная A -алгебра.

(ii) Если $A \subset B$ — конечная A -алгебра и $x \in B$, то x удовлетворяет нормированному уравнению над A , т. е. существует соотношение

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0, \text{ где } a_i \in A$$

(обратите внимание, что старший коэффициент равен 1).

(iii) И наоборот, если x удовлетворяет нормированному уравнению над A , то $B = A[x]$ — конечная A -алгебра.

Доказательство. Пункты (i) и (iii) являются простыми упражнениями (ср. с аналогичными результатами для расширений полей). Для доказательства (ii) воспользуемся довольно неочевидным «детерминантным трюком» (который не является моим изобретением). Предположим, что $B = \sum A b_i$. Тогда $x b_i \in B$ для всех i , т. е. существуют константы $a_{ij} \in A$, такие, что

$$x b_i = \sum_j a_{ij} b_j.$$

Перепишем это условие в виде

$$\sum_j (x \delta_{ij} - a_{ij}) b_j = 0.$$

где δ_{ij} — единичная матрица. Пусть теперь M — матрица вида

$$M_{ij} = (x \delta_{ij} - a_{ij}),$$

а $\Delta = \det M$. Из стандартных утверждений линейной алгебры вытекает, что

$$M \mathbf{b} = 0,$$

где $\mathbf{b}$ — вектор-столбец с элементами $(b_1, \dots, b_n)$. Следовательно,

$$0 = (M^{\text{adj}}) M \mathbf{b} = \Delta \mathbf{b},$$

(где M^{adj} — присоединенная матрица). Поэтому $\Delta b_i = 0$ для всех i . При этом, так как $1_B \in B$ является линейной комбинацией b_i , то $\Delta = \Delta \cdot 1_B = 0$, что и дает нам, наконец, искомое соотношение

$\det(x \delta_{ij} - a_{ij}) = 0$. Очевидно, что оно задается нормированным многочленом относительно переменной x с коэффициентами из A . Ч. т. д.

(3.13) Нётерова нормализация.

Теорема (лемма о нормализации Э. Нётер). Пусть k — бесконечное поле, а $A = k[a_1, \dots, a_n]$ — конечно порожденная k -алгебра. Тогда существуют $m \leq n$ и $y_1, \dots, y_m \in A$, такие, что

- (i) $y_1, \dots, y_m$ алгебраически независимы над k ;
- (ii) A — конечная $k[y_1, \dots, y_m]$ -алгебра.

(i) означает, как обычно, что не существует нетривиального полиномиального соотношения, которому удовлетворяли бы y_i . Алгебраист выразит эту мысль так: естественное (сюрьеक्टивное) отображение $k[Y_1, \dots, Y_m] \rightarrow k[y_1, \dots, y_m] \subset A$ является инъективным.)

Утверждается, что, как и можно было ожидать, расширение колец может быть построено в два этапа: сначала добавляются алгебраически независимые элементы, а затем «производится алгебраическое расширение». Впрочем, (ii) намного точнее, так как в нем утверждается, что каждый элемент кольца A не просто алгебраичен над $k[y_1, \dots, y_m]$, но удовлетворяет нормированному (т. е. со старшим коэффициентом 1) уравнению над этим кольцом.

Доказательство. Пусть I — ядро естественной сюрьекции

$$I = \ker \{k[X_1, \dots, X_n] \rightarrow k[a_1, \dots, a_n] = A\}.$$

Предположим, что $0 \neq f \in I$. Идея доказательства заключается в том, чтобы заменить $X_1, \dots, X_{n-1}$ на некоторые $X'_1, \dots, X'_{n-1}$ так, чтобы преобразовать f в нормированное уравнение относительно переменной a_n над кольцом $A' = k[a'_1, \dots, a'_{n-1}]$. Запишем

$$\begin{aligned} a'_1 &= a_1 - \alpha_1 a_n, \\ &\dots \dots \dots \\ a'_{n-1} &= a_{n-1} - \alpha_{n-1} a_n. \end{aligned}$$

(где α_i являются неизвестными пока элементами поля k). Тогда

$$0 = f(a'_1 + \alpha_1 a_n, \dots, a'_{n-1} + \alpha_{n-1} a_n, a_n).$$

Утверждение. При подходящем выборе элементов $\alpha_1, \dots, \alpha_{n-1} \in k$ многочлен

$$f(X'_1 + \alpha_1 X_n, \dots, X'_{n-1} + \alpha_{n-1} X_n, X_n)$$

является нормированным относительно переменной X_n .

Используя это утверждение, будем доказывать теорему индукцией по n . Если $I = 0$, то доказывать нечего, так как $a_1, \dots, a_n$ алгебраически независимы. В противном случае возьмем $0 \neq f \in I$; пусть $\alpha_1, \dots, \alpha_{n-1}$ удовлетворяют условиям сформулированного утверждения. Тогда f задает нормированное соотношение относительно переменной a_n с коэффициентами из $A' = k[a'_1, \dots, a'_{n-1}]$. В силу предположения индукции существуют $y_1, \dots, y_m \in A'$, такие, что

(1) $y_1, \dots, y_m$ алгебраически независимы над k ;

(2) A' — конечная $k[y_1, \dots, y_m]$ -алгебра.

Тогда $A = A'[a_n]$ конечна над A' (в силу (3.12(iii))). Следовательно, согласно (3.12 (i)), A конечна над $k[y_1, \dots, y_m]$, что и доказывает теорему.

Осталось только доказать утверждение. Пусть $d = \deg f$; запишем

$$f = F_d + G,$$

где F_d — однородный многочлен степени d и $\deg G \leq d-1$. Тогда

$$\begin{aligned} f(X_1, \dots, X_{n-1}, X_n) &= f(X'_1 + \alpha_1 X_n, \dots, X'_{n-1} + \alpha_{n-1} X_n, X_n) = \\ &= F_d(\alpha_1, \dots, \alpha_{n-1}, 1) \cdot X_n^d + \\ &+ (\text{члены, содержащие } X_n \text{ в степенях } \leq d-1). \end{aligned}$$

Если теперь $F_d(\alpha_1, \dots, \alpha_{n-1}, 1) \neq 0$, то все сделано. Так как F_d — ненулевой многочлен, то нетрудно проверить, что нужное условие выполняется для «почти всех» значений $\alpha_1, \dots, \alpha_{n-1}$ (доказательство этого обсуждается в упр. 3.13). Ч.т.д.

(3.14) Замечания. (I) В действительности из доказательства (3.13) следует, что в качестве $y_1, \dots, y_m$ можно выбрать m общих линейных форм от $a_1, \dots, a_n$. Чтобы оценить важность теоремы (3.13), положим $I = \ker \{K[X_1, \dots, X_n] \rightarrow k[a_1, \dots, a_n] = A\}$, и предположим для простоты, что I прост. Рассмотрим $V = V(I) \subset \mathbb{A}_k^n$. Пусть $\pi: \mathbb{A}_k^n \rightarrow \mathbb{A}_k^m$ — линейное проектирование на подпространство с координатами $y_1, \dots, y_m$ и $p = \pi|_V: V \rightarrow \mathbb{A}_k^m$. Можно показать, что из условий (i) и (ii) в (3.13) вытекает, что прообраз $p^{-1}(P)$ каждой точки $P \in \mathbb{A}_k^m$ является непустым конечным множеством (см. упр. 3.16).

(II) Доказательство (3.13) имеет также простую геометрическую интерпретацию. А именно, набор из $n-1$ линейных форм от n переменных определяет линейную проекцию $\pi: \mathbb{A}_k^n \rightarrow \mathbb{A}_k^{n-1}$. Слои проекции π образуют $(n-1)$ -мерное семейство параллельных прямых. Нетрудно показать, что фиксированный многочлен $f \in I$ задает нормированное уравнение по последней переменной X_n тогда и только тогда, когда эти параллельные прямые не являются асимптотами

многообразия ($f = 0$). В терминах проективной геометрии это означает, что точка на бесконечности $(0, \alpha_1, \dots, \alpha_{n-1}, 1) \in \mathbb{P}_k^{n-1}$, определяющая параллельное проектирование, не лежит в проективном замыкании поверхности ($f = 0$).

(III) Приведенное выше доказательство не проходит в случае конечного поля (см. упр. 3.14). Однако сама теорема верна без каких бы то ни было ограничений на k (см. [Mumford, Introduction, р. 4] или [Атья, Макдональд (7.9)]).

(3.15) Доказательство (3.8). Пусть $A = k[a_1, \dots, a_n]$ — конечно порожденная k -алгебра. Предположим, что $y_1, \dots, y_m \in A$ такие же, как в (3.13), а $B = k[y_1, \dots, y_m]$. Тогда A — конечная B -алгебра, и по условию она является полем. Если бы было известно, что B — поле, то из этого мгновенно вытекало бы, что $m = 0$. Это означало бы, что A — конечная k -алгебра, т. е. конечное расширение поля k , и утверждение было бы доказано. Поэтому нам осталось доказать следующее предложение.

Лемма. Если A — поле и $B \subset A$ — такое подкольцо, что A — конечная B -алгебра, то B — поле.

Доказательство. Для любого $0 \neq b \in B$ в A существует обратный элемент $b^{-1} \in A$. Далее, в силу (3.12 (ii)) из условия конечности следует, что b^{-1} удовлетворяет нормированному уравнению над B , т. е. существует соотношение

$$b^{-n} + a_{n-1}b^{-(n-1)} + \dots + a_1b^{-1} + a_0 = 0, \text{ где } a_i \in B.$$

Умножив его на b^{n-1} , получим

$$b^{-1} = -(a_{n-1} + a_{n-2}b + \dots + a_0b^{n-1}) \in B.$$

Следовательно, B — поле. Это рассуждение доказывает (3.8) и завершает доказательство Nullstellensatz.

(3.16) Для того чтобы все наши рассуждения проходили в характеристике p , полезно сделать следующее небольшое уточнение. Оно понадобится нам в дальнейшем только один раз, и читатель не знакомый с понятием сепарабельности из теории Галуа, может не тратить времени и переходить к разд. (3.17).

Добавление. Если в предположениях (3.13) поле k является, кроме того, алгебраически замкнутым, а кольцо A — областью целостности, поле частных которой обозначается через K , то элементы

$y_1, \dots, y_m \in A$ можно, как и выше, выбрать так, чтобы помимо условий (i), (ii) выполнялось

(iii) $k(y_1, \dots, y_m) \subset K$ — сепарабельное расширение.

Доказательство. Если поле k имеет характеристику 0, то любое его расширение сепарабельно. Поэтому будем считать, что k имеет характеристику p . Так как A — область целостности, то идеал I прост. Следовательно, если $I \neq 0$, то он содержит неприводимый элемент f . Для каждого i имеет место следующая альтернатива: либо f сепарабелен по X_i , либо $f \in k[X_1, \dots, X_i^p, \dots, X_n]$.

Утверждение. Если f несепарабелен по всем X_i , то $f = g^p$ для некоторого g , что противоречит неприводимости f .

Согласно предположению, f имеет вид

$$f = F(X_1^p, \dots, X_n^p), \text{ где } F \in k[X_1, \dots, X_n].$$

Если это так, то пусть $g \in k[X_1, \dots, X_n]$ — многочлен, получаемый взятием корня p -й степени из каждого коэффициента F . Тогда, применив нужное количество раз тождество $(a + b)^p = a^p + b^p$ в характеристике p , получим, что $f = g^p$.

Следовательно, любой неприводимый многочлен f сепарабелен по крайней мере относительно одного из X_i , для определенности относительно X_n . Далее, проводя в точности такие же рассуждения, как и выше, получим, что

$$f(X'_1 + \alpha_1 X_n, \dots, X'_{n-1} + \alpha_{n-1} X_n, X_n)$$

дает нормированное сепарабельное соотношение на a_n над кольцом $A' = k[a'_1, \dots, a'_{n-1}]$. Искомый результат доказывается с помощью такого же индуктивного рассуждения, в котором на этот раз используется то обстоятельство, что композиция сепарабельных расширений полей сепарабельна. Ч.т.д.

(3.17) Редукция к случаю гиперповерхности. Напомним следующий результат теории Галуа.

Теорема о примитивном элементе. Пусть K — бесконечное поле и $K \subset L$ — конечное сепарабельное расширение. Тогда существует такой $x \in L$, что $L = K(x)$. Более того, если L порождается над полем K элементами $z_1, \dots, z_k$, то x можно выбрать в виде линейной комбинации $\sum_i \alpha_i z_i$.

(Это непосредственно вытекает из основной теоремы теории Галуа. Действительно, если $K \subset M$ является нормальным замыканием L над K , то $K \subset M$ — конечное расширение Галуа рассматриваемого поля. Таким образом, в силу основной теоремы между K и M существует только конечное число промежуточных расширений. Промежуточные подполя между K и L образуют конечный набор $\{K_j\}$ K -векторных подпространств в L . Значит, можно выбрать $x \in L$, который не лежит ни в одном из них. Если даны $z_1, \dots, z_k$, не принадлежащие ни одному из K_i одновременно, то x может быть выбран в виде K -линейной комбинации z_i . Тогда $K(x) = L$.)

Следствие. При выполнении условий леммы Нётер о нормализации (3.13) существуют $y_1, \dots, y_{m+1} \in A$, удовлетворяющие заключению теоремы (3.13) и, кроме того, условию, что поле частных K кольца A порождается над k элементами $y_1, \dots, y_{m+1}$.

Доказательство. В силу (3.16) мы можем считать, что K — сепарабельное расширение поля $k(y_1, \dots, y_m)$. Если $A = k[x_1, \dots, x_n]$, то x_i , разумеется, порождают K как расширение поля $k(y_1, \dots, y_m)$, так что подходящая линейная комбинация y_{m+1} элементов x_i с коэффициентами из $k[y_1, \dots, y_m]$ порождает искомое расширение. Приведя все к общему знаменателю, можно выбрать y_{m+1} в виде линейной комбинации x_i с коэффициентами из $k[y_1, \dots, y_m]$, т. е. принадлежащим кольцу A . Ч.т.д.

Алгебраический смысл доказанного заключается в том, что расширение $k \subset K$, которое само по себе не обязано быть чисто трансцендентным, может быть получено как композиция чисто трансцендентного расширения $k \subset k(y_1, \dots, y_m) = K_0$ и примитивного алгебраического расширения $K_0 \subset K = K_0(y_{m+1})$. Другими словами, $K = k(y_1, \dots, y_{m+1})$, а между образующими имеется единственное алгебраическое соотношение. Геометрическое значение этого результата станет ясным в (5.10).

Упражнения к § 3

3.1. Область целостности называется областью главных идеалов, если каждый идеал I из A является главным, т. е. имеет вид $I = (a)$. Найдите прямое доказательство того, что идеалы в области главных идеалов удовлетворяют условию обрыва возрастающих цепей.

3.2. Покажите, что область целостности A является областью с однозначным разложением на множители тогда и только тогда, когда каждая возрастающая цепочка главных идеалов стабилизируется и каждый неприводимый элемент кольца A прост.

3.3. (i) Докажите следующую лемму Гаусса. Если A — область с однозначным разложением на множители и $f, g \in A[X]$ — многочлены с коэффициентами из A , то простой элемент из A , являющийся общим делителем коэффициентов произведения fg , является общим делителем либо коэффициентов f , либо коэффициентов g .

(ii) В начальном курсе общей алгебры доказывается, что если K — поле, то $K[X]$ — область с однозначным разложением на множители. Докажите индукцией по n , что $k[X_1, \dots, X_n]$ является областью с однозначным разложением на множители. Для этого сравните разложение в $k[X_1, \dots, X_n]$ с разложением в $k(X_1, \dots, X_{n-1})[X_n]$, пользуясь для приведения к общему знаменателю леммой Гаусса.

3.4. Докажите предложение (3.2 (ii)). Пусть A — область целостности. K — ее поле частных и $0 \neq S \subset A$ — некоторое подмножество. Положим

$$B = A[S^{-1}] = \{a/b \in K \mid a \in A \text{ и } b = 1 \text{ или является произведением элементов из } S\}.$$

Докажите, что идеал I из B полностью определяется своим пересечением с A , и установите, что из нётеровости A следует нётеровость B .

3.5. Пусть $J = (XY, XZ, YZ) \subset k[X, Y, Z]$. Найдите $V(J) \subset \mathbb{A}^3$. Является ли оно неприводимым? Верно ли, что $J = I(V(J))$? Докажите, что J не может быть порожден двумя элементами. Пусть теперь $J' = (XY, (X - Y)Z)$. Найдите $V(J')$ и вычислите $\text{rad } J'$.

3.6. Пусть $J = (X^2 + Y^2 - 1, Y - 1)$. Найдите $f \in I(V(J)) \setminus J$.

3.7. Пусть $J = (X^2 + Y^2 + Z^2, XY + XZ + YZ)$. Найдите $V(J)$ и $I(V(J))$.

3.8. Докажите, что неприводимые компоненты алгебраического множества определены однозначно (что было сформулировано без доказательства в (3.7(b))). Это

означает, что если $V = \bigcup_{i \in I} V_i = \bigcup_{j \in J} W_j$ — два несократимых разложения множества V в объединение неприводимых компонент (т. е. $V_i \not\subset V_{i'}$ для $i \neq i'$), то V_i получаются из W_j перенумерацией.

3.9. Пусть $f = X^2 - Y^2$ и $g = X^3 + XY^2 - Y^3 - X^2Y - X + Y$. Найдите неприводимые компоненты множества $V(f, g) \subset \mathbb{A}_C^2$.

3.10. Пусть $J = (uw - v^2, w^3 - u^5)$. Покажите, что $V(J)$ имеет две неприводимые компоненты, одной из которых является кривая C из (3.11(b)).

Докажите, что ту же кривую C можно задать двумя уравнениями $uw = v^2$ и $u^5 - 2u^2vw + w^3 = 0$. Здесь дело в том, что второе уравнение, ограниченное на квадратичный конус ($uw = v^2$), становится похожим на полный квадрат.

3.11. Пусть $f = v^2 - uw$, $g = u^4 - vw$, $h = w^2 - u^3v$. Опишите многообразие $V(f, g, h) \subset \mathbb{A}^3$ так, как это делалось в духе (3.11(b)). Выясните, имеют ли $V(f, g)$, $V(f, h)$ и $V(g, h)$ другие интересные компоненты?

3.12. (i) Докажите, что над любым полем k алгебраическое подмножество в $\mathbb{A}_k^1$ либо конечно, либо совпадает с $\mathbb{A}_k^1$. Выведите отсюда, что топология Зарисского является кофинитивной топологией.

(ii) Пусть k — произвольное поле и $f, g \in k[X, Y]$ — неприводимые элементы, не кратные друг другу. Докажите, что $V(f, g)$ конечно. (Указание. Обозначьте через K поле $k(X)$. Докажите сначала, что f и g не имеют общих делителей в области главных идеалов $K[Y]$. Выведите отсюда, что существуют такие $p, q \in K[Y]$, что $pf + qg = 1$. Далее, приводя p и q к общему знаменателю, покажите, что существуют $h \in k[X]$ и $a, b \in k[X, Y]$, такие, что $h = af + bg$. Сделайте из этого вывод, что имеется лишь конечное число допустимых значений для X -координаты точек из $V(f, g)$.)

(iii) Докажите, что любое алгебраическое множество $V \subset \mathbb{A}_k^2$ является объединением конечного числа точек и кривых.

3.13. (a) Пусть k — бесконечное поле и $f \in k[X_1, \dots, X_n]$. Предположим, что f — не константа, т. е. $f \notin k$. Покажите, что $V(f) \neq \mathbb{A}_k^n$. (Указание. Предположите, что в f входит переменная X_n и рассмотрите разложение $f = \sum a_i(X_1, \dots, X_{n-1})X_n^i$. Воспользуйтесь теперь индукцией по n .)

(b) Предположим, что поле k алгебраически замкнуто, а f такой же, как и в п. (a). Пусть f имеет по переменной X_n степень m и $a_m(X_1, \dots, X_{n-1})X_n^m$ является его старшим членом. Покажите, что если $a_m \neq 0$, то существует конечное непустое множество точек из $V(f)$, соответствующих каждому набору значений $(X_1, \dots, X_{n-1})$. Выведите отсюда, в частности, что если $n \geq 2$, то $V(f)$ бесконечно.

(c) Объединяя результаты п. (b) и упр. 3.12 (iii), докажите, что если k — алгебраически замкнутое поле, то различные неприводимые многочлены $f \in k[X, Y]$ определяют различные гиперповерхности в $\mathbb{A}_k^2$ (ср. с п. (a) разд. 3.11).

(d) Обобщите результат п. (c) на случай $\mathbb{A}_k^n$.

3.14. Приведите пример, показывающий, что доказательство леммы Нётер о нормализации, приведенное в (3.13), не проходит для конечного поля k . (Указание. Найдите многочлен $f(X, Y)$, для которого $F_d(\alpha, 1) = \alpha^d - \alpha$, так что $F_d(\alpha, 1) = 0$ для всех $\alpha \in k$.)

3.15. Пусть A — кольцо и $A \subset B$ — конечная A -алгебра. Докажите, что если m — максимальный идеал в A , то $mB \neq B$. (Указание. Предположим противное, а именно что $B = mB$. Тогда если $B = \sum Ab_i$, то $b_i = \sum a_{ij}b_j$ для всех i , где $a_{ij} \in m$. Докажите теперь, что

$$\Delta = \det(\delta_{ij} - a_{ij}) = 0,$$

и получите, что $1_B \in m$. Противоречие. (См. также [Атья, Макдональд, предл. 2.4 и след. 2.5].)

3.16. Пусть $A = k[a_1, \dots, a_n]$ удовлетворяет посылкам леммы Нётер о нормализации (3.13). Положим $I = \ker \{k[X_1, \dots, X_n] \rightarrow k[a_1, \dots, a_n] = A\}$ и рассмотрим $V = V(I)$ в $\mathbb{A}_k^n$. Предположим для простоты, что I прост.

Пусть $Y_1, \dots, Y_m$ — общие линейные формы от $X_1, \dots, X_m$. Обозначим через $\pi: \mathbb{A}_k^n \rightarrow \mathbb{A}_k^m$ линейную проекцию, определенную формами $Y_1, \dots, Y_m$, и положим $p = \pi|_V: V \rightarrow \mathbb{A}_k^m$. Докажите, что из (3.13(i)) и (3.13(ii)) вытекает, что прообраз $p^{-1}(P)$ любой точки $P \in \mathbb{A}_k^m$ является конечным множеством, которое непусто, если k алгебраически замкнуто. (Указание. I содержит нормированные соотношения над $k[Y_1, \dots, Y_m]$ относительно всех X_i . Из этого легко вытекает условие конечности. Для доказательства непустоты воспользуйтесь упр. 3.15, чтобы получить, что для любой точки $P = (b_1, \dots, b_m) \in \mathbb{A}_k^m$ идеал $J_P = I + (Y_1 - b_1, \dots, Y_m - b_m)$ не совпадает с $k[X_1, \dots, X_m]$. Затем примените утверждение о непустоте из Nullstellensatz.)

§ 4. Функции на многообразиях

В этом параграфе я работаю с фиксированным полем k . Начиная с (4.8(II)) и далее поле k будет предполагаться алгебраически замкнутым. Читатель, который будет считать, что $k = \mathbb{C}$, потеряет немного, а психологически, возможно, будет легче. В некоторых случаях для упрощения обозначений поле k не указывается.

(4.1) **Полиномиальные функции.** Пусть $V \subset \mathbb{A}_k^n$ — алгебраическое множество, а $I(V)$ — его идеал. Тогда факторкольцо $k[V] = k[X_1, \dots, X_n]/I(V)$ естественным образом отождествляется с кольцом функций на V . Точнее, определим *полиномиальную функцию* на V как отображение $f: V \rightarrow k$ вида $P \mapsto F(P)$, где $F \in k[X_1, \dots, X_n]$. Это означает, что f является ограничением отображения $F: \mathbb{A}^n \rightarrow k$, заданного многочленом. Согласно определению $I(V)$, два элемента $F, G \in k[X_1, \dots, X_n]$ определяют одну и ту же функцию на V тогда и только тогда, когда

$$F(P) - G(P) = 0 \text{ для всех } P \in V,$$

т. е. тогда и только тогда, когда $F - G \in I(V)$. Определим *координатное кольцо* $k[V]$ следующим образом:

$$\begin{aligned} k[V] &= \{f: V \rightarrow k \mid f \text{ — полиномиальная функция}\} \cong \\ &\cong k[X_1, \dots, X_n]/I(V). \end{aligned}$$

Оно является наименьшим из колец функций на V , содержащих координатные функции X_i (наряду с полем k), так что в этом случае традиционное название достаточно естественно.

(4.2) $k[V]$ и алгебраические подмножества в V . Алгебраическое множество $X \subset \mathbb{A}^n$ содержится в V тогда и только тогда, когда $I(X) \supset I(V)$. С другой стороны, идеалы кольца $k[X_1, \dots, X_n]$, содержащие $I(V)$, находятся в очевидном биективном соответствии с идеалами в $k[X_1, \dots, X_n]/I(V)$. (Поразмышляйте, не торопясь, если вам это не кажется очевидным. Действительно, идеал J , такой, что $I(V) \subset J \subset k[X_1, \dots, X_n]$, соответствует идеалу $J/I(V)$. И обратно, идеал J_0 в $k[X_1, \dots, X_n]/I(V)$ соответствует своему прообразу в $k[X_1, \dots, X_n]$.)

Поэтому следующие соответствия I и V :

$$\{\text{идеалы } I \subset k[V]\} \xrightarrow{V} \{\text{подмножества } X \subset V\},$$

заданное формулой

$$I \mapsto V(I) = \{P \in V \mid f(P) = 0 \text{ для всех } f \in I\},$$

и

$$\{\text{идеалы } J \subset k[V]\} \xleftarrow{I} \{\text{подмножества } X \subset V\},$$

заданное формулой

$$I(X) = \{f \in k[V] \mid f(P) = 0 \text{ для всех } P \in X\} \leftarrow X,$$

определяются так же, как в § 3, и имеют аналогичные свойства.

В частности, алгебраическое множество V снабжено топологией Зарисского, замкнутыми множествами которой являются алгебраические подмножества (разумеется, эта топология индуцирована на V как на подпространстве топологией Зарисского на $\mathbb{A}^n$).

Предложение. Пусть $V \subset \mathbb{A}^n$ — алгебраическое подмножество. Следующие условия эквивалентны:

- (i) V неприводимо;
- (ii) для любых двух открытых подмножеств $\emptyset \neq U_1, U_2 \subset V$ имеем $U_1 \cap U_2 \neq \emptyset$;
- (iii) любое непустое открытое подмножество $U \subset V$ является плотным.

Все эти утверждения вполне тривиальны. Неприводимость V означает, что V не может быть представлено в виде объединения двух собственных замкнутых подмножеств, а (ii) является просто переформулировкой этого замечания в терминах дополнений, так как

$$U_1 \cap U_2 = \emptyset \Leftrightarrow V = (V \setminus U_1) \cup (V \setminus U_2).$$

Подмножество топологического пространства является плотным тогда и только тогда, когда оно пересекается с любым открытым множеством, так что (iii) — это просто переформулировка (ii).

(4.3) **Полиномиальные отображения.** Пусть $V \subset \mathbb{A}^n$ и $W \subset \mathbb{A}^m$ — алгебраические множества. Обозначим через $X_1, \dots, X_n$ и $Y_1, \dots, Y_m$ координаты на $\mathbb{A}^n$ и $\mathbb{A}^m$ соответственно.

Определение. Отображение $f: V \rightarrow W$ называется *полиномиальным*, если существует набор из m таких многочленов $F_1, \dots, F_m \in k[X_1, \dots, X_n]$, что для всех $P \in V$

$$f(P) = (F_1(P), \dots, F_m(P)) \in \mathbb{A}_k^m.$$

Это определение является очевидным обобщением приведенного выше понятия полиномиальной функции.

Утверждение. Отображение $f: V \rightarrow W$ является полиномиальным тогда и только тогда, когда для всех j композиция отображений $f_j = Y_j \circ f$ полиномиальна:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \subset \mathbb{A}_k^m \\ & \searrow f_j & \downarrow Y_j \\ & & k \end{array} \quad (j\text{-я координатная функция})$$

Это очевидно. Действительно, пусть f задано набором $F_1, \dots, F_m$; тогда композиция имеет вид $P \mapsto F_j(P)$ и является, очевидно, полиномиальной функцией. Обратно, если $f_j \in k[V]$ для всех j , то при любом выборе $F_j \in k[X_1, \dots, X_n]$, таких, что $f_j = F_j \bmod I(V)$, получается представление f в виде полиномиального отображения, заданного набором $(F_1, \dots, F_m)$.

В свете этого утверждения отображение f может быть записано в виде $f = (f_1, \dots, f_m)$.

Композиция полиномиальных отображений определяется очевидным образом. Если $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ и $U \subset \mathbb{A}^l$ — алгебраические множества, а $f: V \rightarrow W$ и $g: W \rightarrow U$ — полиномиальные отображения, то $g \circ f: V \rightarrow U$ также полиномиально; действительно, если f задано многочленами $F_1, \dots, F_m \in k[X_1, \dots, X_n]$, а g задано многочленами $G_1, \dots, G_l \in k[Y_1, \dots, Y_m]$, то $g \circ f$ задается многочленами

$$G_1(F_1, \dots, F_m), \dots, G_l(F_1, \dots, F_m) \in k[X_1, \dots, X_n].$$

Определение. Полиномиальное отображение $f: V \rightarrow W$ алгебраических множеств называется *изоморфизмом*, если существует полиномиальное отображение $g: W \rightarrow V$, такое, что $f \circ g = g \circ f = \text{id}$.

Мы уже приводили несколько примеров полиномиальных отображений. Так, отображения параметризации $\mathbb{R}^1 \rightarrow C \subset \mathbb{R}^2$ из (2.1), задаваемые формулами $t \mapsto (t^2, t^3)$ или $t \mapsto (t^2 - 1, t^3 - t)$, а также отображение $k \rightarrow C \subset \mathbb{A}_k^3$ из (3.11(b)), заданное формулой $t \mapsto (t^3, t^4, t^5)$, явно имеют требуемый вид. Кроме этого при обсуждении нормализации Нётер рассматривалось алгебраическое множество $V \subset \mathbb{A}_k^n$ и общая проекция $p: V \rightarrow \mathbb{A}_k^m$, определенная m «достаточно общими» линейными формами $Y_1, \dots, Y_m$. Так как Y_i являются линейными формами от координат $X_i \in \mathbb{A}_k^n$, то это отображение полиномиально.

С другой стороны, параметризация окружности из разд. (1.1) задается рациональными функциями, а не полиномиальными, так как в знаменателе стоит выражение $(\lambda^2 + 1)$. По той же причине не годится также и обратное отображение $(X, Y) \mapsto t = Y/X$ любой из особых кубик $C \subset \mathbb{R}^2$ на $\mathbb{R}^1$ (точнее, не годится *данная запись*).

(4.4) Полиномиальные отображения и $k[V]$

Теорема. Пусть, как и выше, $V \subset \mathbb{A}_k^n$ и $W \subset \mathbb{A}_k^m$ — алгебраические множества.

(I) Полиномиальное отображение $f: V \rightarrow W$ индуцирует гомоморфизм колец $f^*: k[W] \rightarrow k[V]$, определяемый взятием композиции функций. А именно если $g \in k[W]$ — полиномиальная функция, то $f^*(g) = g \circ f$ также полиномиальна и $g \mapsto g \circ f$ определяет гомоморфизм колец и в действительности даже гомоморфизм k -алгебр $f^*: k[W] \rightarrow k[V]$. (Заметим, что это отображение действует в сторону, обратную f .)

(II) И обратно, любой гомоморфизм k -алгебр $\Phi: k[W] \rightarrow k[V]$ имеет вид $\Phi = f^*$ для некоторого однозначно определенного полиномиального отображения $f: V \rightarrow W$.

Таким образом, (I) и (II) показывают, что отображение

$$\left\{ \begin{array}{l} \text{полиномиальные} \\ \text{отображения } f: V \rightarrow W \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \text{гомоморфизмы } k\text{-алгебр} \\ \Phi: k[W] \rightarrow k[V] \end{array} \right\},$$

заданное формулой $f \mapsto f^*$, является биекцией.

(III) Если $f: V \rightarrow W$ и $g: W \rightarrow U$ — полиномиальные отображения, то два кольцевых гомоморфизма $(g \circ f)^* = f^* \circ g^*: k[U] \rightarrow k[V]$ совпадают.

Доказательство. (I) В силу того, что говорилось в (4.3), $f^*(g)$ является полиномиальным отображением $V \rightarrow k$ и, следовательно, $f^*(g) \in k[V]$. Очевидно, что $f^*(a) = a$ для всех $a \in k$ (так как k рассматривается как множество постоянных функций на V, W). И наконец, тот факт, что f^* — кольцевой гомоморфизм, получается автоматически, так как и $k[W]$ и $k[V]$ являются кольцами функций. (Кольцевая структура определяется поточечно; так, например, для $g_1, g_2 \in k[W]$ сумма $g_1 + g_2$ определяется как функция на W , такая, что $(g_1 + g_2)(P) = g_1(P) + g_2(P)$ для всех $P \in W$. Следовательно, $f^*(g_1 + g_2)(Q) = (g_1 + g_2)(f(Q)) = g_1(f(Q)) + g_2(f(Q)) = f^*g_1(Q) + f^*g_2(Q)$. Надеюсь, что никто не станет читать этой ерунды?)

(II) просто означает, что композиция отображений ассоциативна.

(II) Доказательство этого пункта более замысловатое, хотя его содержательная нагрузка ничуть не выше, чем у прочих пунктов. Для всех $i = 1, \dots, m$ обозначим через $y_i \in k[W]$ i -ю координатную функцию на W ; значит,

$$k[W] = k[y_1, \dots, y_m] = k[Y_1, \dots, Y_m]/I(W).$$

Таким образом, задано отображение $\Phi: k[W] \rightarrow k[V]$ и можно определить $f_i \in k[V]$ формулой $f_i = \Phi(y_i)$.

Рассмотрим отображение $f: V \rightarrow \mathbb{A}_k^m$, определенное набором функций $f(P) = (f_1(P), \dots, f_m(P))$. Оно полиномиально, так как $f_i \in k[V]$. Более того, можно утверждать, что f отображает V в W , т. е. $f(V) \subset W$. В самом деле, предположим, что $G \in I(W) \subset k[Y_1, \dots, Y_m]$; тогда

$$G(y_1, \dots, y_m) = 0 \in k[W],$$

где левая часть означает, что в полиномиальное выражение G подставлены элементы y_i кольца. Следовательно, $\Phi(G(y_1, \dots, y_m)) = 0 \in k[V]$, и так как Φ — гомоморфизм k -алгебр, то

$$k[V] \ni 0 = \Phi(G(y_1, \dots, y_m)) = G(\Phi(y_1), \dots, \Phi(y_m)) = G(f_1, \dots, f_m).$$

f_i — функции на V , и $G(f_1, \dots, f_m) \in k[V]$ является по определению функцией вида $P \mapsto G(f_1(P), \dots, f_m(P))$. Этим доказано, что для точки $P \in V$ и произвольного $G \in I(W)$ координаты $(f_1(P), \dots, f_m(P))$ точки $f(P)$ удовлетворяют соотношению $G(f_1(P), \dots, f_m(P)) = 0$. Поскольку W — подмножество в $\mathbb{A}_k^m$, определяемое тем, что $G \in I(W)$ обращаются на нем в нуль, получаем что $f(P) \in W$. Это доказывает, что рассматриваемое отображение f является полиномиальным отображением $V \rightarrow W$. Чтобы убедиться, что два гомоморфизма $f^*, \Phi: k[W] \rightarrow k[V]$ k -алгебр совпадают, достаточно проверить, что они совпадают на образующих, т. е. $f^*(y_i) = \Phi(y_i)$. Несложный анализ способа построения f (в начале доказательства п. (ii) выше) показывает, что это действительно так. Совершенно аналогичное рассуждение устанавливает, что отображение f однозначно определяется условием $f^*(y_i) = \Phi(y_i)$. Ч.т.д.

(4.5) Следствие. Полиномиальное отображение $f: V \rightarrow W$ является изоморфизмом тогда и только тогда, когда $f^*: k[W] \rightarrow k[V]$ — изоморфизм.

Пример. Над бесконечным полем k полиномиальное отображение

$$\varphi: \mathbb{A}_k^1 \rightarrow C: (Y^2 = X^3) \subset \mathbb{A}_k^2,$$

заданное формулой $T \mapsto (T^2, T^3)$, не является изоморфизмом, так как в этом случае гомоморфизм

$$\varphi^*: k[C] = k[X, Y]/(Y^2 - X^3) \rightarrow k[T]$$

задается формулой $X \mapsto T^2, Y \mapsto T^3$. Образ φ^* является k -алгеброй, порожденной T^2 и T^3 , а $k[T^2, T^3]$ строго содержится в $k[T]$ (Пожалуйста, убедитесь, что вам понятно, почему T^2 и T^3 не порождают $k[T]$. Тут я вам помочь не берусь.)

Заметим, что φ биективно и, следовательно, имеет вполне хорошее обратное отображение $\psi: C \rightarrow \mathbb{A}_k^1$, задаваемое формулой $(X, Y) \mapsto 0$ при $X = Y = 0$ и $(X, Y) \mapsto Y/X$ в остальных случаях. Почему же в таком случае φ не является изоморфизмом? Дело в том, что на C имеется меньше полиномиальных функций, чем на $\mathbb{A}^1$. На самом деле вы могли бы догадаться об этом и сами, так как в кольце $k[\mathbb{A}^1] = k[T]$ есть полиномиальная функция с ненулевой производной в точке 0. Создается ощущение, что φ «сплюсчивает касательные векторы в точке 0».

(4.6) Аффинные многообразия. Пусть k — поле. Аффинным многообразием я буду называть неприводимое алгебраическое подмножество $V \subset \mathbb{A}_k^n$, определенное с точностью до изоморфизма.

Теорема (4.4) означает, что координатное кольцо $k[V]$ является инвариантом многообразия V с точностью до изоморфизма. Это позволяет нам дать определение многообразия, в котором меньше используется объемлющее пространство $\mathbb{A}_k^n$. Наше желание добиться такого определения вызвано довольно смутными причинами, и с практической стороны читатель не много потеряет, если проигнорирует его. В дальнейшем аффинное многообразие будет пониматься в указанном выше смысле (переходите к п. (4.7)).

Определение. Аффинным многообразием над полем k называется подмножество V вместе с кольцом $k[V]$ k -значных функций $f: V \rightarrow k$, такие, что

- (i) $k[V]$ — конечно порожденная k -алгебра;
- (ii) при некотором выборе образующих $x_1, \dots, x_n$ в кольце $k[V]$ отображение

$$V \rightarrow \mathbb{A}_k^n,$$

заданное формулой

$$P \mapsto (x_1(P), \dots, x_n(P)),$$

определяет вложение V как неприводимого алгебраического множества.

(4.7) Поле функций. Пусть V — аффинное многообразие. Тогда координатное кольцо $k[V]$ многообразия V — это область целостности, элементами которой являются k -значные функции на V .

Определение. Полем функций $k(V)$ многообразия V называется поле частных $k(V) = \text{Quot}(k[V])$ кольца $k[V]$. Элемент $f \in k(V)$ на-

зывается *рациональной функцией* на V . Заметим, что $f \in k(V)$ является по определению отношением $f = g/h$, где $g, h \in k[V]$ и $h \neq 0$.

Априори из-за нулей функции h f не является функцией на V . Тем не менее f корректно определена в точке $P \in V$, если $h(P) \neq 0$, так что она является по крайней мере «частично определенной» функцией. Сейчас мы введем терминологию, подкрепляющую это понятие.

Определение. Пусть $f \in k(V)$ и $P \in V$. Скажем, что f *регулярна* в точке P или что P принадлежит *области определения* функции f , если существует представление $f = g/h$, где $g, h \in k[V]$ и $h(P) \neq 0$.

Важное обстоятельство, которое следует иметь в виду, заключается в том, что, как правило, $k[V]$ не является областью с однозначным разложением на множители, т. е. для $f \in k(V)$ могут существовать принципиально разные представления $f = g/h$ (см., например, упр. 4.9). Через

$$\text{dom} f = \{P \in V \mid f \text{ регулярна в точке } P\}$$

обозначим *область определения* функции f и запишем

$$\mathcal{O}_{V,P} = \{f \in k(V) \mid f \text{ регулярна в точке } P\} = k[V][\{h^{-1} \mid h(P) \neq 0\}].$$

Тогда $\mathcal{O}_{V,P} \subset k(V)$ является подкольцом, называемым *локальным кольцом* многообразия V в точке P .

(4.8) **Теорема.** (I) $\text{dom} f$ является открытым и плотным в топологии Зарисского множеством.

Предположим, что k алгебраически замкнуто; тогда

$$(II) \quad \text{dom} f = V \Leftrightarrow f \in k[V];$$

(т. е. полиномиальная функция — это регулярная рациональная функция). Более того, для любого $h \in k[V]$ положим

$$V_h = V \setminus V(h) = \{P \in V \mid h(P) \neq 0\};$$

тогда

$$(III) \quad \text{dom} f \supset V_h \Leftrightarrow f \in k[V][h^{-1}].$$

Доказательство. Определим идеал знаменателей функции $f \in k[V]$ соотношением

$$\begin{aligned} D_f &= \{h \in k[V] \mid hf \in k[V]\} \subset k[V] = \\ &= \{h \in k[V] \mid \text{существует представление } f = g/h, \text{ где } g \in k[V] \cup \{0\}\}. \end{aligned}$$

Из первой строки очевидно, что D_f является идеалом в $k[V]$. Тогда автоматически получаем, что

$$V \setminus \text{dom} f = \{P \in V \mid h(P) = 0 \text{ для всех } h \in D_f\} = V(D_f),$$

так что $V \setminus \text{dom} f$ является алгебраическим множеством в V . Следовательно, $\text{dom} f = V \setminus V(D_f)$ — дополнение к замкнутому множеству, и, таким образом, оно открыто в топологии Зарисского. Очевидно, что $\text{dom} f$ непусто и, значит, в силу упр. 4.2 плотно.

Далее, используя п. (b) из Nullstellensatz получим

$$\text{dom} f = V \Leftrightarrow V(D_f) = \emptyset \Leftrightarrow 1 \in D_f, \text{ т. е. } f \in k[V].$$

И, наконец,

$$\text{dom} f \supset V_h \Leftrightarrow h \text{ обращается в нуль на } V(D_f)$$

и в силу п. (c) из Nullstellensatz

$$\Leftrightarrow h^n \in D_f \text{ для некоторого } n, \text{ т. е. } f = g/h^n \in k[V][h^{-1}]. \text{ Ч.т.д.}$$

(4.9) **Рациональные отображения.** Пусть V — аффинное многообразие.

Определение. Рациональным отображением $f: V \rightarrow \mathbb{A}_k^n$ называется частично определенное отображение, заданное рациональными функциями $f_1, \dots, f_n$, т. е.

$$f(P) = (f_1(P), \dots, f_n(P)) \text{ для всех } P \in \bigcap \text{dom} f_i.$$

По определению $\text{dom} f = \bigcap \text{dom} f_i$. Как и ранее, f называется *регулярным* в точке $P \in V$ тогда и только тогда, когда $P \in \text{dom} f$. Рациональное отображение $V \rightarrow W$ двух аффинных многообразий $V \subset \mathbb{A}^n$ и $W \subset \mathbb{A}^m$ определяется как рациональное отображение $f: V \rightarrow \mathbb{A}^m$, такое, что $f(\text{dom} f) \subset W$.

Два примера рациональных отображений были описаны в конце разд. (4.3).

(4.10) **Композиция рациональных отображений.** Композиция $g \circ f$ рациональных отображений $f: V \rightarrow W$ и $g: W \rightarrow U$ может быть не определена. Эта трудность вызвана тем, что рациональное отображение не является настоящим отображением; в естественном и очевидном смысле композиция определена на множестве $\text{dom} f \cap \bigcap f_i^{-1}(\text{dom} g)$, которое вполне может оказаться пустым (см. упр. 4.10).

Эта же проблема возникает и при алгебраической трактовке. А именно, пусть f задано набором $f_1, \dots, f_m \in k(V)$, так что

$$f: V \rightarrow W \subset \mathbb{A}^m$$

по формуле

$$P \mapsto (f_1(P), \dots, f_m(P)),$$

где $P \in \bigcap \text{dom } f_i$. Любая функция $g \in k[W]$ имеет вид $g = G \bmod I(W)$ для некоторого $G \in k[Y_1, \dots, Y_m]$, и композиция $g \circ f = G(f_1, \dots, f_m)$ корректно определена в $k(V)$. Таким образом, так же как в разд. (4.4), имеет место гомоморфизм k -алгебр

$$f^*: k[W] \rightarrow k(V),$$

соответствующий функции f . Однако если $h \in k[W]$ лежит в ядре отображения f^* , то выражению $f^*(g/h)$ нельзя придать никакого смысла, т. е. f^* не может быть продолжено до гомоморфизма полей $k(W) \rightarrow k(V)$.

Определение. Отображение $f: V \rightarrow W$ называется *доминантным*, если $f(\text{dom } f)$ плотно в W в топологии Зарисского.

Геометрически это означает, что для любого рационального отображения $g: W \rightarrow U$ прообраз $f^{-1}(\text{dom } g) \subset \text{dom } f$ является открытым плотным множеством в топологии Зарисского, так что композиция $g \circ f$ определена на открытом плотном подмножестве в V и является частично определенным отображением $V \rightarrow U$.

С алгебраической точки зрения

$$f \text{ доминантно} \Leftrightarrow f^*: k[W] \rightarrow k[V] \text{ инъективно.}$$

Для заданного $g \in k[W]$ получаем, что

$$g \in \ker f^* \Leftrightarrow f(\text{dom } f) \subset V(g),$$

т. е. f^* не является инъективным тогда и только тогда, когда $f(\text{dom } f)$ содержится в собственном алгебраическом подмножестве многообразия W .

Очевидно, что композиция $g \circ f$ рациональных отображений f и g определена, если f доминантно. В этом случае $g \circ f$ является рациональным отображением с компонентами $f^*(g_i)$. Заметим, что область определения $g \circ f$, очевидно, содержит $f^{-1}(\text{dom } g) \cap \text{dom } f$, но вполне может быть больше (см. упр. 4.6).

(4.11) Теорема. (I) Доминантное рациональное отображение $f: V \rightarrow W$ определяет гомоморфизм полей $f^*: k(W) \rightarrow k(V)$.

(II) Обратно, k -гомоморфизм $\Phi: k(W) \rightarrow k(V)$ индуцируется однозначно определенным доминантным рациональным отображением $f: V \rightarrow W$.

(III) Если f и g доминантны, то $(g \circ f)^* = f^* \circ g^*$.

Доказательство получается небольшим изменением рассуждения из (4.4).

(4.12) Морфизмы из открытого подмножества аффинного многообразия. Пусть V и W — аффинные многообразия, а $U \subset V$ — открытое подмножество.

Определение. Морфизмом $f: U \rightarrow W$ называется рациональное отображение $f: V \rightarrow W$, такое, что $U \subset \text{dom } f$, т. е. f регулярно во всех точках $P \in U$.

Если $U_1 \subset V$ и $U_2 \subset W$ — открытые множества, то морфизм $f: U_1 \rightarrow U_2$ — это просто морфизм $f: U_1 \rightarrow W$, такой, что $f(U_1) \subset U_2$. *Изоморфизмом* называется морфизм, имеющий двусторонний обратный морфизм.

Заметим, что если V и W — аффинные многообразия, то по п. (II) теоремы (4.8)

$$\{\text{морфизмы } f: V \rightarrow W\} = \{\text{полиномиальные отображения } f: V \rightarrow W\};$$

Левая часть этого соотношения содержит рациональные объекты, подчиненные условиям регулярности, в то время как правая часть определяется более непосредственно через многочлены.

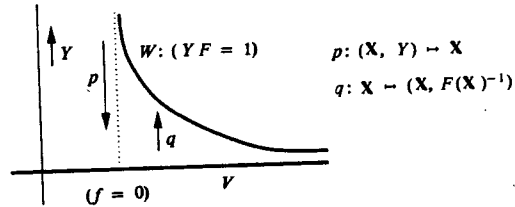
Пример. Параметризация полукубической параболы $\mathbb{A}^1 \rightarrow C: (Y^2 = X^3)$ из разд. (2.1) индуцирует изоморфизм $\mathbb{A}^1 \setminus \{0\} \cong C \setminus \{(0, 0)\}$ (детали см. в упр. 4.5).

(4.13) Стандартные открытые подмножества. Пусть V — аффинное многообразие. Для $f \in k[V]$ обозначим через V_f открытое множество $V_f = V \setminus V(f) = \{P \in V \mid f(P) \neq 0\}$. Такие V_f называются *стандартными открытыми множествами* в V .

Предложение. V_f изоморфно аффинному многообразию, и

$$k[V_f] = k[V][f^{-1}].$$

Доказательство. Идея заключается в рассмотрении графика функции f^{-1} . Аналогичный прием использовался при доказательстве импликации (b) $\Rightarrow$ (c) в Nullstellensatz (3.10).



Пусть $J = I(V) \subset k[X_1, \dots, X_n]$. Выберем $F \in k[X_1, \dots, X_n]$ так, что $f = F \bmod I(V)$. Положим теперь $I = (J, YF - 1) \subset k[X_1, \dots, X_n, Y]$ и

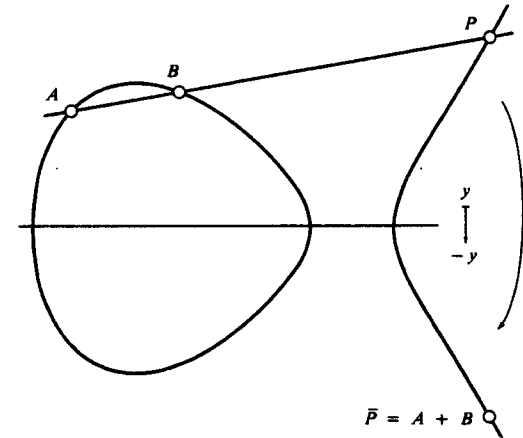
$$V(I) = W \subset \mathbb{A}^{n+1}.$$

Легко проверить, что отображения, изображенные на диаграмме, являются взаимно обратными морфизмами многообразий W и V_f . Утверждение о координатном кольце содержится в теореме (4.8). Ч.т.д.

Стандартные открытые множества V_f важны тем, что они образуют базис топологии Зарисского на V . А именно, каждое открытое множество $U \subset V$ является объединением множеств V_f (так как любое замкнутое подмножество имеет вид $V(I) = \bigcap_{f \in I} V(f)$ для

некоторого идеала). Таким образом, смысл сформулированного результата состоит в том, что каждое открытое множество $U \in V$ есть объединение открытых множеств V_f , которые являются аффинными многообразиями.

(4.14) Пример. В § 2 я обсуждал групповой закон $(A, B) \mapsto A + B$ на плоской неособой (проективной) кубике $C \subset \mathbb{P}^2$. Пусть $C_0: (y^2 = x^3 + ax + b)$ — неособая аффинная кубика (см стр. 85). Я покажу сейчас, что групповой закон определяет рациональное отображение $\varphi: C_0 \times C_0 \rightarrow C_0$ и что φ является морфизмом там, где ему положено быть. Хотя я не буду на этом останавливаться, замечу, что то же рассуждение может быть использовано, чтобы получить другое доказательство «по непрерывности» ассоциативности группового закона, которое пригодно для любого поля (см. обсуждения в разд. (2.10)).



Нетрудно убедиться (см. упр. 2.7), что если $A = (x, y)$, $B = (x', y')$ и $x \neq x'$, то, обозначив через u отношение $(y - y')/(x - x')$, можно определить координаты третьей точки пересечения $P = (x'', y'')$ следующим образом:

$$x'' = f(x, y, x', y') = u^2 - (x + x'),$$

$$y'' = g(x, y, x', y') = u^3 + xu + y'.$$

Так как x'' и y'' являются рациональными функциями координат (x, y) , (x', y') , то это означает, что $\varphi: C_0 \times C_0 \rightarrow C_0$ является рациональным отображением. Из явного вида формул следует, что при $x \neq x'$ отображение φ является морфизмом, так как в этом случае знаменатель u не обращается в нуль. Пусть теперь $x = x'$ и $y = -y'$; тогда координаты x'' и y'' должны обращаться в бесконечность, и это соответствует тому, что прямая AB пересекает проективную кривую C в точке $O = (0, 1, 0)$ на бесконечности. Если же $x = x'$ и $y = y' \neq 0$, то и в этом случае точка $P = (x'', y'')$ должна быть корректно определена. Я утверждаю, что f и g в таких точках на $C_0 \times C_0$ являются регулярными функциями. Чтобы убедиться в этом, заметим, что из

$$y^2 = x^3 + ax + b \text{ и } y'^2 = x'^3 + ax' + b$$

вытекает, что $y^2 - y'^2 = x^3 - x'^3 + a(x - x')$;

следовательно, для рациональных функций на $C_0 \times C_0$ имеет место тождество

$$u = (y - y')/(x - x') = (x^2 + xx' + x'^2 + a)/(y + y').$$

Из вида знаменателя следует, что u (а также f и g) регулярна при $y \neq -y'$.

Следствием наших выкладок является такое утверждение: групповой закон $\varphi: C_0 \times C \rightarrow C_0$ является морфизмом в точке $(A, B) \in C_0 \times C_0$ при условии, что $A + B \neq 0$.

Упражнения к § 4

4.1. Проверьте, что утверждения § 4 по (4.8 (I)) включительно выполняются над любым полем k . Продумайте, в частности, что они означают для конечного поля. Приведите контрпример к (4.8 (II)), если поле k не является алгебраически замкнутым.

4.2. Пусть $\varphi: \mathbb{A}^1 \rightarrow \mathbb{A}^3$ — полиномиальное отображение, заданное формулой $X \mapsto (X, X^2, X^3)$. Докажите, что образ отображения φ является алгебраическим подмножеством $C \subset \mathbb{A}^3$ и что $\varphi: \mathbb{A}^1 \rightarrow C$ — изоморфизм. Попробуйте получить обобщения.

4.3. Пусть $\varphi_n: \mathbb{A}^1 \rightarrow \mathbb{A}^2$ — полиномиальное отображение, заданное формулой $X \mapsto (X^2, X^n)$. Докажите, что если n четно, то образ φ_n изоморфен $\mathbb{A}^1$ и φ_n является двулистным накрытием вне 0. Покажите, что если n нечетно, то φ_n — биекция, и задайте рациональное отображение, обратное к φ_n .

4.4. Докажите, что морфизм $\varphi: X \rightarrow Y$ двух аффинных многообразий является изоморфизмом между X и подмногообразием $\varphi(X) \subset Y$ тогда и только тогда, когда индуцированное отображение $\Phi: k[Y] \rightarrow k[X]$ сюръективно.

4.5. Пусть $C: (Y^2 = X^3) \subset \mathbb{A}^2$. Тогда

(а) параметризация $f: \mathbb{A}^1 \rightarrow C$, заданная формулой (T^2, T^3) , является полиномиальным отображением;

(б) f имеет рациональное обратное отображение $g: C \rightarrow \mathbb{A}^1$, определяемое формулой $(X, Y) \mapsto Y/X$;

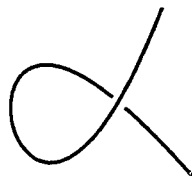
(с) $\text{dom } g = C \setminus \{(0, 0)\}$;

(д) f и g задают взаимно обратные изоморфизмы $\mathbb{A}^1 \setminus \{0\} \cong C \setminus \{(0, 0)\}$.

4.6. (i) Покажите, что область определения отображения $g \circ f$ может быть строго большей, чем $\text{dom } f \cap f^{-1}(\text{dom } g)$. (Указание. Это может произойти, если g и f являются взаимно обратными рациональными отображениями. Попробуйте рассмотреть f и g из упр. 4.5).

(ii) Большинство курсов анализа функций нескольких переменных содержат такие примеры, как функция $f(x, y) = xy/(x^2 + y^2)$. Объясните, как получается, что функция f , ограниченная на любую гладкую кривую, проходящую через $(0, 0)$, является гладкой, а как функция двух переменных она даже не непрерывна.

4.7. Пусть $C: (Y^2 = X^3 + X^2) \subset \mathbb{A}^2$. Уже знакомая нам параметризация кривой $\varphi: \mathbb{A}^1 \rightarrow C$ задается полиномиальным отображением $T \mapsto (T^2 - 1, T^3 - T)$, но она не является изоморфизмом (а почему?). Определите, является ли изоморфизмом ограничение $\varphi': \mathbb{A}^1 \setminus \{1\} \rightarrow C$.



4.8. Пусть $C: (Y^2 = X^4 + X^3) \subset \mathbb{A}^2$. Покажите, что отображение $(X, Y) \mapsto X/Y$ определяет рациональное отображение $\varphi: C \rightarrow \mathbb{A}^1$, и его обратным является полиномиальное отображение $\varphi: \mathbb{A}^1 \rightarrow C$, параметризующее C . Докажите, что φ ограничивается до изоморфизма

$$\mathbb{A}^1 \setminus \{3 \text{ точки}\} \cong C \setminus \{(0, 0)\}.$$

4.9. Пусть $V: (XT = YZ) \subset \mathbb{A}^4$. Объясните, почему $k[V]$ не является областью с однозначным разложением на множители. (Уловить идею нетрудно, намного труднее получить строгое доказательство.) Пусть $f = X/Y \in k(V)$; найдите $\text{dom } f$ и докажите, что она строго больше, чем множество точек $(Y = 0) \subset V$.

4.10. Пусть $f: \mathbb{A}^1 \rightarrow \mathbb{A}^2$ задано формулой $X \mapsto (X, 0)$, а $g: \mathbb{A}^2 \rightarrow \mathbb{A}^1$ — рациональное отображение, заданное формулой $(X, Y) \mapsto X/Y$. Покажите, что композиция $g \circ f$ нигде не определена. Выясните, на каком максимальном подмножестве поля функций $f(\mathbb{A}^1)$ определена g .

4.11. Определите и изучите понятие произведения двух алгебраических множеств. А именно,

(i) докажите, что если $V \subset \mathbb{A}_k^n$ и $W \subset \mathbb{A}_k^m$ — алгебраические множества, то $V \times W \subset \mathbb{A}_k^{n+m}$ также алгебраично;

(ii) приведите примеры, показывающие, что топология Зарисского на $V \times W$ не является произведением топологий Зарисского на V и на W ;

(iii) докажите, что если V и W неприводимы, то $V \times W$ неприводимо;

(iv) докажите, что если $V \cong V'$ и $W \cong W'$, то $V \times W \cong V' \times W'$.

4.12. (а) Докажите, что любая функция $f \in k(\mathbb{A}^2)$, не регулярная в начале координат $(0, 0)$, не регулярна также в точках некоторой кривой, проходящей через $(0, 0)$;

(б) Докажите, что множество $\mathbb{A}^2 \setminus (0, 0)$ не является аффинным многообразием. (Указание. Для доказательства п. (а) используйте тот факт, что $k(\mathbb{A}^2) = k(X, Y)$ является полем частных кольца $k[X, Y]$ с однозначным разложением на множители, и результат упр. 3.13(б). Для доказательства п. (б) предположите, что $\mathbb{A}^2 \setminus (0, 0)$ аффинно, и определите его координатное кольцо. Используя следствие (4.5), получите противоречие.)

§ 5. Проективная и бирациональная геометрии

Целью первой части § 5 является обобщение результатов § 3—4 на проективный случай. За исключением нескольких содержательных моментов, это делается вполне автоматически. Оставшаяся часть параграфа посвящена бирациональной геометрии, т. е. изучению введенного в конце § 4 поля функций $k(V)$. Этот материал одинаково хорошо вписывается и в проективный, и в аффинный контекст.

(5.0) Почему же проективные многообразия? Кубическая кривая

$$C: (Y^2Z = X^3 + aXZ^2 + bZ^3) \subset \mathbb{P}^2$$

является объединением двух аффинных кривых

$$C_0: (y^2 = x^3 + ax + b) \subset \mathbb{A}^2 \text{ (кусоч } (Z = 1) \text{ кривой } C)$$

и

$$C_1: (z_1 = x_1^3 + ax_1z_1^2 + bz_1^3) \subset \mathbb{A}^2 \text{ (кусоч } (Y = 1)),$$

склеенных с помощью изоморфизма

$$C_0 \setminus (y = 0) \rightarrow C_1 \setminus (z_1 = 0),$$

заданного формулой

$$(x, y) \mapsto (x/y, 1/y).$$

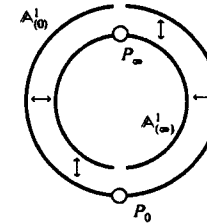
В качестве существенно более простого примера можно взять пространство $\mathbb{P}^1$ с однородными координатами (X, Y) , которое является объединением двух экземпляров $\mathbb{A}^1$ с координатами x_0 и x_1 соответственно, склеенных друг с другом с помощью изоморфизма

$$\mathbb{A}^1 \setminus (x_0 = 0) \rightarrow \mathbb{A}^1 \setminus (y_1 = 0),$$

заданного формулой

$$x_0 \mapsto 1/x_0.$$

Обычная иллюстрация выглядит так:



(стрелки $\leftrightarrow$ обозначают склеивание).

Важно понимать, что *эти многообразия строго больше любого аффинного многообразия*. Действительно, при естественном определении морфизма (которое мы скоро введем) легко убедиться, что ни для какого n не существует непостоянных морфизмов $\mathbb{P}^1 \rightarrow \mathbb{A}^n$ или $C \rightarrow \mathbb{A}^n$ (см. упр. 5.1 и 5.12 и обсуждения в (8.10)).

Одним из решений этой проблемы является введение понятия «абстрактного многообразия» V как объединения $V = \bigcup V_i$ аффинных многообразий по модулю подходящего склеивания. В силу аналогии с определением многообразий в топологии эта идея склеивания может показаться привлекательной, однако она приводит к многочисленным техническим трудностям. Работа с проективными многообразиями устраняет эти сложности путем использования готового объемлющего пространства $\mathbb{P}^n$, так что (за исключением некоторой возни с однородными многочленами) изучать такие многообразия ненамного сложнее, чем аффинные. В действительности, хотя это и не столь очевидно на элементарном уровне знаний, проективные многообразия представляют собой на удивление естественный полигон для изучения алгебраических многообразий (это кратко обсуждается с высоконаучной точки зрения в (8.11)).

(5.1) Градуированные кольца и однородные идеалы

Определение. $f \in k[X_0, \dots, X_n]$ называется *однородным многочленом степени d* , если

$$f = \sum a_{i_0, \dots, i_n} X_0^{i_0} \dots X_n^{i_n},$$

где $a_{i_0, \dots, i_n} \neq 0$, только если $i_0 + \dots + i_n = d$.

Любой многочлен $f \in k[X_0, \dots, X_n]$ обладает однозначным разложением вида $f = f_0 + f_1 + \dots + f_N$, где f_d — однородный многочлен степени d , $d = 0, 1, \dots, N$.

Предложение. Если f — однородный многочлен степени d , то $f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n)$ для всех $\lambda \in k$.

Если поле k бесконечно, то верно и обратное.

Доказательство. Попробуйте и убедитесь.

Определение. Идеал $I \subset k[X_0, \dots, X_n]$ называется *однородным*, если для всех $f \in I$ однородное разложение $f = f_0 + f_1 + \dots + f_n$ удовлетворяет условию $f_i \in I$ для всех i .

Это эквивалентно тому, что I порождается (конечным числом) однородных многочленов.

(5.2) **Однородные соответствия V и I .** Пусть $\mathbb{P}_k^n$ — это n -мерное проективное пространство над полем k с однородными координатами $X_0, \dots, X_n$. Тогда $f \in k[X_0, \dots, X_n]$ не является функцией на $\mathbb{P}_k^n$, так как по определению $\mathbb{P}_k^n = k^{n+1} \setminus \{0\} / \sim$, где $\sim$ — отношение эквивалентности, заданное условием $(X_0, \dots, X_n) \sim (\lambda X_0, \dots, \lambda X_n)$, $\lambda \in k \setminus \{0\}$, а f — функция на k^{n+1} . Тем не менее, если f однородна, для точки $P \in \mathbb{P}_k^n$ выражение $f(P) = 0$ корректно определено. А именно, пусть $P = (X_0 : \dots : X_n)$, т. е. $(X_0, \dots, X_n)$ — представитель класса эквивалентности точки P в $k^{n+1} \setminus \{0\}$. Тогда, поскольку $f(\lambda X) = \lambda^d f(X)$, из соотношения $f(X_0, \dots, X_n) = 0$ вытекает, что $f(\lambda X_0, \dots, \lambda X_n) = 0$, т. е. условие $f(P) = 0$ не зависит от выбора представителя. Учитывая это, определим, как и выше, соответствия

$$\left\{ \begin{array}{l} \text{однородные идеалы} \\ J \subset k[X_0, \dots, X_n] \end{array} \right\} \xleftrightarrow{V, I} \left\{ \begin{array}{l} \text{подмножества} \\ X \subset \mathbb{P}_k^n \end{array} \right\}$$

соотношениями

$$V(J) = \{P \in \mathbb{P}_k^n \mid f(P) = 0 \text{ для всех однородных } f \in J\}$$

и

$$I(X) = \{f \in k[X_0, \dots, X_n] \mid f(P) = 0 \text{ для всех } P \in X\}.$$

В качестве упражнения убедитесь, что вам ясно, почему $I(X)$ — однородный идеал.

Соответствия V и I обладают теми же формальными свойствами, что и их аффинные прототипы, введенные в § 3 (например, $V(J_1 + J_2) = V(J_1) \cap V(J_2)$). Подмножество вида $V(I)$ называется *алгебраическим подмножеством* в $\mathbb{P}_k^n$, и, так же как и в аффинном случае, $\mathbb{P}_k^n$ снабжено *топологией Зарисского*, замкнутыми подмножествами в которой являются алгебраические подмножества.

(5.3) **Проективная Nullstellensatz.** Так же как и в аффинном случае, чисто формальная проверка показывает, что $I(V(J)) \supset \text{rad } J$ для любого идеала J и что $V(I(X)) = X$ для любого алгебраического множества X . Имеется ровно одно место, в котором требуется проявить осторожность. А именно, тривиальный идеал $(1) = k[X_0, \dots, X_n]$ (все кольцо) определяет пустое множество в k^{n+1} , а следовательно, и в $\mathbb{P}_k^n$, как и должно быть; в то же время идеал $(X_0, \dots, X_n)$ определяет $\{0\}$ в k^{n+1} , который также соответствует пустому множеству в $\mathbb{P}_k^n$. Идеал $(X_0, \dots, X_n)$ является весьма неудобным исключением (связанным с пустым множеством) для некоторых утверждений однородной теории, и его традиционно называют *несущественным идеалом*.

Таким образом, однородный вариант Nullstellensatz имеет следующий вид.

Теорема. Пусть k — алгебраически замкнутое поле. Тогда

- (i) $V(J) = \emptyset \Leftrightarrow \text{rad } J \supset (X_0, \dots, X_n)$;
- (ii) если $V(J) \neq \emptyset$, то $I(V(J)) = \text{rad } J$.

Следствие. I и V определяют взаимно обратные биекции

$$\begin{aligned} \left\{ \begin{array}{l} \text{однородные радикальные} \\ \text{идеалы } J \subset k[X_0, \dots, X_n], \\ \text{такие, что } J \neq k[X_0, \dots, X_n] \end{array} \right\} &\leftrightarrow \left\{ \begin{array}{l} \text{алгебраические} \\ \text{подмножества} \\ X \subset \mathbb{P}^n \end{array} \right\} \\ \cup & \\ \left\{ \begin{array}{l} \text{однородные простые} \\ \text{идеалы } J \subset k[X_0, \dots, X_n], \\ \text{такие, что } J \neq k[X_0, \dots, X_n] \end{array} \right\} &\leftrightarrow \left\{ \begin{array}{l} \text{неприводимые} \\ \text{алгебраические} \\ \text{подмножества } X \subset \mathbb{P}^n \end{array} \right\} \end{aligned}$$

Доказательство. Пусть $\pi: \mathbb{A}^{n+1} \setminus \{0\} \rightarrow \mathbb{P}^n$ — отображение, определяющее $\mathbb{P}^n$. Пусть J — однородный идеал $J \subset k[X_0, \dots, X_n]$. Временно обозначим через $V^a(J) \subset \mathbb{A}^{n+1}$ аффинное алгебраическое множество, определенное идеалом J . Так как J однороден, то $V^a(J)$ обладает следующими свойствами:

$$(\alpha_0, \dots, \alpha_n) \in V^a(J) \Leftrightarrow (\lambda \alpha_0, \dots, \lambda \alpha_n) \in V^a(J),$$

и $V(J) = V^a(J) \setminus \{0\} / \sim \subset \mathbb{P}^n$. Следовательно,

$$V(J) = \emptyset \Leftrightarrow V^a(J) \subset \{0\} \Leftrightarrow \text{rad } J \supset (X_0, \dots, X_n),$$

где в последней импликация используется аффинная Nullstellensatz.

Кроме того, если $V(J) \neq \emptyset$, то

$$f \in I(V(J)) \Leftrightarrow f \in I(V^a(J)) \Leftrightarrow f \in \text{rad } J. \quad \text{Ч. т. д.}$$

Использованное выше аффинное подмножество $V^a(J)$ называется *аффинным конусом* над проективным алгебраическим подмножеством $V(J)$.

(5.4) **Рациональные функции на V .** Пусть $V \subset \mathbb{P}_k^n$ — неприводимое алгебраическое множество и $I(V) \subset k[X_0, \dots, X_n]$ — его идеал. Прямое способа определить регулярные функции на V через многочлены нет. Действительно, хотя многочлен $F \in k[X_0, \dots, X_n]$ и задает функцию на аффинном конусе над V , но (см. случай $d = 0$ в предложении (5.1)) эта функция постоянна на классах эквивалентности только в том случае, когда F имеет степень 0, т. е. является константой. Таким образом, с самого начала нам придется работать с рациональными функциями.

Определение. Рациональной функцией на V называется (частично определенная) функция $f: V \rightarrow k$, заданная соотношением $f(P) = g(P)/h(P)$, где $g, h \in k[X_0, \dots, X_n]$ — однородные многочлены одинаковой степени d .

Заметим, что в случае $h(P) \neq 0$ частное $g(P)/h(P)$ корректно определено, так как для всех $0 \neq \lambda \in k$

$$g(\lambda X)/h(\lambda X) = \lambda^d g(X)/\lambda^d h(X) = g(X)/h(X).$$

Далее, очевидно, что g/h и g'/h' определяют одну и ту же рациональную функцию на V тогда и только тогда, когда $h'g - g'h \in I(V)$, так что множество рациональных функций является полем

$$k(V) = \{g/h \mid g, h \in k[X_0, \dots, X_n] \text{ однородны} \\ \text{и одинаковой степени, } h \notin I(V)\} / \sim,$$

где $\sim$ — отношение эквивалентности,

$$g/h \sim g'/h' \Leftrightarrow h'g - g'h \in I(V).$$

$k(V)$ называется (рациональным) *полем функций* многообразия V .

Следующие определения ничем не отличаются от аффинного случая. Пусть $f \in k(V)$ и $P \in V$; назовем функцию f *регулярной* в точке P , если существует представление $f = g/h$, где g и h — однородные многочлены одинаковой степени, такие, что $h(P) \neq 0$. Вве-

дем обозначения

$$\text{dom } f = \{P \in V \mid f \text{ регулярна в точке } P\}$$

и

$$\mathcal{O}_{V,P} = \{f \in k(V) \mid f \text{ регулярна в точке } P\}.$$

Очевидно, что $\text{dom } f \subset V$ является плотным открытым по Зарисскому множеством в V (доказательство как в (4.8(I)), а $\mathcal{O}_{V,P} \subset k(V)$ является подкольцом.

(5.5) **Аффинное покрытие проективного многообразия.** Пусть $V \subset \mathbb{P}^n$ — неприводимое алгебраическое множество, и предположим для простоты, что $V \not\subset (X_i = 0)$ ни для одного i . Мы знаем, что $\mathbb{P}^n$ может быть покрыто $n + 1$ аффинными кусками $\mathbb{A}_{(i)}^n$ с аффинными (неоднородными) координатами $X_0^{(i)}, \dots, X_{i-1}^{(i)}, X_{i+1}^{(i)}, \dots, X_n^{(i)}$, где

$$X_j^{(i)} = X_j/X_i \text{ для } j \neq i.$$

Положим $V_{(i)} = V \cap \mathbb{A}_{(i)}^n$. Тогда $V_{(i)} \subset \mathbb{A}_{(i)}^n$ является, очевидно, аффинным алгебраическим множеством, так как

$$V_{(i)} \ni P = (1, x_1^{(i)}, \dots, x_n^{(i)}) \Leftrightarrow \\ \Leftrightarrow f(1, x_1^{(i)}, \dots, x_n^{(i)}) = 0 \text{ для всех однородных } f \in I(V),$$

что является набором полиномиальных уравнений относительно координат $(x_1^{(i)}, \dots, x_n^{(i)})$ точки P . Для определенности здесь и далее там, где это будет удобно, мы будем считать, что $i = 0$. Читатель должен понимать, что все это верно для любого другого аффинного куска многообразия V . $V_{(i)}$ называются *стандартными аффинными кусками* многообразия V .

Предложение. (i) Соответствие $V \mapsto V_{(0)} = V \cap \mathbb{A}_{(0)}^n$ задает биекцию

$$\left\{ \begin{array}{l} \text{неприводимые алгебраи-} \\ \text{ческие подмножества} \\ V \subset \mathbb{P}^n \end{array} \middle| V \not\subset (X_0 = 0) \right\} \leftrightarrow \left\{ \begin{array}{l} \text{неприводимые алгебраи-} \\ \text{ческие подмножества} \\ V_{(0)} \subset \mathbb{A}_{(0)}^n \end{array} \right\},$$

а обратное соответствие получается взятием замыкания в топологии Зарисского.

(ii) Пусть $I^n(V) \subset k[X_0, \dots, X_n]$ — введенный в этом параграфе однородный идеал подмножества $V \subset \mathbb{P}^n$, а $I^n(V_{(0)}) \subset k[X_1, \dots, X_n]$ — обычный неоднородный идеал подмножества

$V_{(0)} \subset \mathbb{A}_{(0)}^n$ (как в § 3). Тогда $I^h(V)$ и $I^{(a)}(V_{(0)})$ связаны следующим образом:

$$I^a = \{f(1, X_1, \dots, X_n) \mid f \in I^h(V)\},$$

а

$$I^h(V)_d = \{X_0^d f(X_1/X_0, \dots, X_n/X_0) \mid f \in I^a(V_{(0)}), \text{ где } \deg f \leq d\},$$

где нижний индекс в обозначении $I^h(V)_d$ означает взятие всех членов степени d .

(iii) $k(V) \cong k(V_{(0)})$, и для всех $f \in k(V)$ область определения функции f как функции на $V_{(0)}$ совпадает с $V_{(0)} \cap \text{dom } f$.

Доказательство. Утверждения (i) и (ii) очевидны. Докажем (iii). Если $g, h \in k[X_0, \dots, X_n]$ — однородные многочлены степени d и $h \notin I(V)$, то отношение $g/h \in k(V)$, ограниченное на $V_{(0)}$, совпадает с функцией

$$g(1, X_1/X_0, \dots, X_n/X_0)/h(1, X_1/X_0, \dots, X_n/X_0);$$

Это определяет отображение $k(V) \rightarrow k(V_{(0)})$, и легко понять, что является его обращением.

(5.6) Рациональные отображения и морфизмы. Рациональные отображения проективных (или аффинных) многообразий определяются с помощью кольца $k(V)$. А именно, если $V \subset \mathbb{P}^n$ — неприводимое алгебраическое множество, то рациональным отображением $V \rightarrow \mathbb{A}^m$ называется (частично определенное) отображение, заданное формулой $P \mapsto (f_1(P), \dots, f_m(P))$, где $f_1, \dots, f_m \in k(V)$. Рациональное отображение $V \rightarrow \mathbb{P}^m$ определяется формулой $P \mapsto (f_0(P):f_1(P):\dots:f_m(P))$, где $f_0, f_1, \dots, f_m \in k(V)$. Заметим, что если $0 \neq g \in k(V)$, то $gf_0, gf_1, \dots, gf_m$ определяют то же самое рациональное отображение. Следовательно (предположив, что образ множества V при отображении f не лежит в меньшем проективном подпространстве ($X_0 = 0$)), можно считать далее, что $f_0 = 1$.

Отсюда вытекает, что имеет место биекция между следующими двумя множествами:

$$\{\text{рациональные отображения } f: V \rightarrow \mathbb{A}^m \subset \mathbb{P}^m\}$$

и

$$\{\text{рациональные отображения } f: V \rightarrow \mathbb{P}^m \mid f(V) \not\subset (X_0 = 0)\},$$

так как оба этих вида отображений задаются наборами из m элементов $f_i \in k(V)$.

Определение. Рациональное отображение $f: V \rightarrow \mathbb{P}^m$ называется *регулярным* в точке $P \in V$, если существует представление $f = (f_0, \dots, f_m)$, такое, что

(i) каждая из $f_0, \dots, f_m$ регулярна в точке P ;

(ii) $f_i(P) \neq 0$ по крайней мере для одного из f_i .

Второе условие необходимо для того, чтобы отношения различных f_i были определены в точке P . Если f регулярна в точке P (что, как и раньше, обозначается выражением $P \in \text{dom } f$), то $f: U \rightarrow \mathbb{A}_{(0)}^m \subset \mathbb{P}^m$ является морфизмом подходящей открытой окрестности точки $P \in U \subset V$. Достаточно взять $U = \bigcap_j \text{dom}(f_j/f_i)$, где $f_i(P) \neq 0$; тогда f — морфизм, заданный набором $\{f_j/f_i\}_{j=0,1,\dots,m}$.

Если $U \subset V$ — открытое подмножество проективного многообразия V , то морфизмом $f: U \rightarrow W$ называется рациональное отображение $f: V \rightarrow W$, такое, что $\text{dom } f \supset U$. Таким образом, морфизм — это просто всюду регулярное на U рациональное отображение.

(5.7) Примеры. (1) **Рациональная норм-кривая.** Это очень простой пример изоморфного вложения $f: \mathbb{P}^1 \xrightarrow{\cong} C \subset \mathbb{P}^m$, обобщающий параметризованную конику из разд. (1.7), который часто встречается в проективной и алгебраической геометрии. Определим отображение

$$f: \mathbb{P}^1 \rightarrow \mathbb{P}^m$$

формулой

$$(X:Y) \mapsto (X^m: X^{m-1}Y: \dots: Y^m)$$

(выписав все одночлены степени m от переменных X и Y). Действуя последовательно, получим, что

(i) f — рациональное отображение, так как оно задается набором $((X/Y)^m, (X/Y)^{m-1}, \dots, 1)$;

(ii) f — морфизм при $Y \neq 0$ в силу только что написанной формулы, а если $Y = 0$, то $X \neq 0$, и работает такой же трюк с (Y/X) ;

(iii) образом отображения f является множество точек $(X_0: \dots: X_m) \subset \mathbb{P}^m$, таких, что

$$(X_0: X_1) = (X_1: X_2) = \dots = (X_{m-1}: X_m),$$

т. е.

$$X_0X_2 = X_1^2, \quad X_0X_3 = X_1X_2, \quad X_0X_4 = X_1X_3, \quad \text{и т. д.}$$

Всем этим условиям можно одновременно придать удобную детерминантную форму

$$\text{rank} \begin{bmatrix} X_0 & X_1 & X_2 & \dots & X_{m-1} \\ X_1 & X_2 & X_3 & \dots & X_m \end{bmatrix} \leq 1$$

(это условие на ранг означает, что равны нулю детерминанты всех 2×2 -миноров). Эти однородные уравнения определяют алгебраическое множество $C \subset \mathbb{P}^m$.

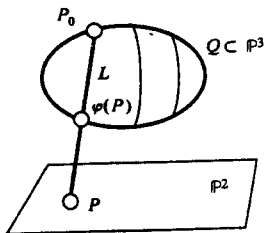
(iv) нетрудно построить обратный морфизм $g: C \rightarrow \mathbb{P}^1$. Для этого следует отобразить точку множества C в отношение $(X_0: X_1) = \dots = (X_{m-1}: X_m) \in \mathbb{P}^1$. В качестве упражнения выясните, что тут нуждается в проверке, и проведите эту проверку.

(2) **Линейная проекция, параметризующая квадрику.** Отображение $\pi: \mathbb{P}^3 \rightarrow \mathbb{P}^2$, заданное формулой $(X_0, X_1, X_2, X_3) \mapsto (X_1, X_2, X_3)$, является рациональным отображением и морфизмом вне точки $P_0 = (1, 0, 0, 0)$. Пусть $Q \subset \mathbb{P}^3$ — квадратичная гиперповерхность и точка P_0 лежит на Q . Тогда каждая точка P на $\mathbb{P}^2$ соответствует некоторой прямой L в $\mathbb{P}^3$, проходящей через P . В общем положении прямая L пересекает Q в точке P_0 и в некоторой второй точке $\varphi(P)$. Например, если $Q: (X_0 X_3 = X_1 X_2)$, то отображение $\varphi: \mathbb{P}^2 \rightarrow Q$, обратное к отображению $\pi|_Q: Q \rightarrow \mathbb{P}^2$, имеет вид

$$(X_1, X_2, X_3) \mapsto (X_1 X_2 / X_3, X_1, X_2, X_3).$$

Здесь использована в точности та же идея, что и при параметризации окружности в разд. (1.1).

В качестве вознаграждения (см. упр. 5.2) можно найти $\text{dom } \pi$ и $\text{dom } \varphi$ и дать геометрическую интерпретацию особенностей отображений π и φ .



(5.8) Бирациональные отображения

Определение. Пусть V и W — аффинные или проективные многообразия. Тогда рациональное отображение $f: V \rightarrow W$ называется **бirationальным отображением** (или **бirationальной эквивалентностью**), если оно имеет рациональное обратное, т. е. существует рациональное отображение $g: W \rightarrow V$, такое, что $f \circ g = \text{id}_W$ и $g \circ f = \text{id}_V$.

Предложение. Следующие три условия на рациональное отображение $f: V \rightarrow W$ эквивалентны:

- (i) f — бирациональная эквивалентность;
- (ii) f доминантно (см. (4.10)) и $f^*: k(W) \rightarrow k(V)$ — изоморфизм;
- (iii) существуют открытые множества $V_0 \subset V$ и $W_0 \subset W$, такие, что $f|_{V_0}$ является изоморфизмом $f: V_0 \rightarrow W_0$.

Доказательство. Отображение f^* определяется так же, как и для аффинных многообразий, и эквивалентность (i) $\Leftrightarrow$ (ii) устанавливается так же, как в разд. (4.11). Импликация (iii) $\Rightarrow$ (i) очевидна, поскольку изоморфизм $f: V_0 \rightarrow W_0$ и его обратный $g = f^{-1}: W_0 \rightarrow V_0$ являются по определению рациональными отображениями между V и W .

Важная импликация (i) $\Rightarrow$ (iii) доказывается более замысловато, хотя и это доказательство не особенно содержательно (если хотите избежать головной боли, приступайте к разд. (5.9)). А именно, согласно предположению (i), имеются взаимно обратные рациональные отображения $f: V \rightarrow W$ и $g: W \rightarrow V$. Положим $V' = \text{dom } f \subset V$ и $\varphi = f|_{V'}: V' \rightarrow W$ и аналогично $W' = \text{dom } g \subset W$ и $\psi = g|_{W'}: W' \rightarrow V$. На диаграмме

$$\begin{array}{ccc} \psi^{-1} V' & \xrightarrow{\psi} & V' \xrightarrow{\varphi} W \\ \cap & & \nearrow \\ W & & \end{array}$$

все стрелки обозначают морфизмы, и совпадение $\text{id}_W|_{\psi^{-1} V'} = \varphi \circ \psi$ как морфизмов вытекает из совпадения $\text{id}_W = f \circ g$ как рациональных отображений. Следовательно, для всех $P \in \psi^{-1} V'$

$$\varphi(\psi(P)) = P.$$

Положим теперь $V_0 = \varphi^{-1} \psi^{-1} V'$ и $W_0 = \psi^{-1} \varphi^{-1} W'$. Тогда по построению $\varphi: V_0 \rightarrow \psi^{-1} V'$ является морфизмом. При этом $\psi^{-1} V' \subset W_0$, поскольку из $P \in \psi^{-1} V'$ вытекает, что $\varphi(\psi(P)) = P$. Таким образом, $P \in \psi^{-1} \varphi^{-1} W' = W_0$. Следовательно, $\varphi: V_0 \rightarrow W_0$ является морфизмом; это же верно и для $\psi: W_0 \rightarrow V_0$. Ч.т.д.

(5.9) **Рациональные многообразия.** Введенное в (5.8) понятие бирациональной эквивалентности является ключевым в алгебраиче-

ской геометрии. Условие (iii) предложения означает, что «плоть» многообразий V и W совпадает, хотя они могут немного отличаться на «ребрах». Примером использования бирациональных преобразований является раздутие особого многообразия, чтобы получить неособое (см. (6.12) ниже). Важным частным случаем предложения (5.8) является следующий результат.

Следствие. Для заданного подмногообразия V следующие условия эквивалентны:

- (а) поле функций $k(V)$ является чисто трансцендентным расширением поля k , т. е. $k(V) \cong k(t_1, \dots, t_n)$ для некоторого n ;
- (б) существует открытое плотное множество $V_0 \subset V$, изоморфное открытому плотному подмножеству $U_0 \subset \mathbb{A}^n$.

Многообразие, удовлетворяющее этим условиям, называется *рациональным*. Условие (б) является точной формулировкой того факта, что многообразие V может быть рационально параметризовано n независимыми переменными. Неявно это понятие уже несколько раз появлялось в этой книге (например, в (1.1), (2.1), (3.11(б)), (5.7(ii))). Большое число элементарных приложений алгебраической геометрии в других областях математики так или иначе связано с рациональными многообразиями.

(5.10) Редукция к случаю гиперповерхности. Простым следствием обсуждений нормализации Нётер в конце § 3 является тот факт, что любое многообразие бирационально эквивалентно гиперповерхности. Прежде всего, так как класс бирациональной эквивалентности зависит только от открытого плотного множества, а любое открытое множество содержит открытое плотное подмножество, изоморфное аффинному многообразию (в силу (4.13)), то достаточно рассмотреть только аффинные многообразия $V \subset \mathbb{A}^n$. В разд. (3.17) было показано, что существуют элементы $y_1, \dots, y_{m+1} \in k[V]$, порождающие расширение полей $k \subset k(V)$ и такие, что $y_1, \dots, y_m$ алгебраически независимы, а y_{m+1} алгебраичен над $k(y_1, \dots, y_m)$. Таким образом, эти элементы определяют морфизм $V \rightarrow \mathbb{A}^{m+1}$, который задает бирациональную эквивалентность многообразия V и гиперповерхности $V' \subset \mathbb{A}^{m+1}$.

(5.11) Произведения. Если V и W — аффинные многообразия, то в некотором естественном смысле $V \times W$ также является многообразием. А именно, если $V \subset \mathbb{A}^n$ и $W \subset \mathbb{A}^m$, то $V \times W$ является

подмножеством в $\mathbb{A}^{n+m}$, заданным условием

$$\{((\alpha_1, \dots, \alpha_n); (\beta_1, \dots, \beta_m)) \mid f(\alpha) = 0 \ \forall f \in I(V), \ g(\beta) = 0 \ \forall g \in I(W)\}.$$

Легко проверить, что произведение $V \times W$ сохраняет свойство неприводимости. Заметим, впрочем, что топология Зарисского на произведении не является произведением топологий Зарисского сомножителей (см. упр. 5.10).

Случай проективных многообразий не столь очевиден. Чтобы определить понятие произведения, мы должны убедиться, что $\mathbb{P}^n \times \mathbb{P}^m$ само является проективным многообразием. Заметьте, что оно никоим образом не изоморфно $\mathbb{P}^{n+m}$ (см. упр. 5.2(ii)). Чтобы убедиться в проективности $\mathbb{P}^n \times \mathbb{P}^m$ воспользуемся конструкцией, близкой по духу к конструкции из (5.7(1)). А именно, зададим вложение (вложение *Сегре*)

$$\varphi: \mathbb{P}^n \times \mathbb{P}^m \rightarrow S_{n,m} \subset \mathbb{P}^N, \text{ где } N = (n+1)(m+1) - 1,$$

следующим образом. Пусть $\mathbb{P}^N$ — проективное пространство с однородными координатами

$$(U_{ij})_{i=0, \dots, n; j=0, \dots, m}.$$

Удобно представлять себе, что U_{ij} реализованы в виде матрицы

$$\begin{bmatrix} U_{00} & \dots & U_{0m} \\ U_{10} & \dots & \dots \\ \dots & \dots & U_{nm} \end{bmatrix}$$

Определим теперь φ следующим образом: $((X_0, \dots, X_n), (Y_0, \dots, Y_m)) \mapsto (X_i Y_j)_{i=0, \dots, n; j=0, \dots, m}$. Очевидно, что φ — корректно определенный морфизм, и образ $S_{n,m}$, как легко видеть, является проективным многообразием, заданным соотношением

$$\text{rank} \begin{bmatrix} U_{00} & \dots & U_{0m} \\ U_{10} & \dots & \dots \\ \dots & \dots & U_{nm} \end{bmatrix} \leq 1, \quad \text{т. е.} \quad \det \begin{bmatrix} U_{ik} & U_{il} \\ U_{jk} & U_{jl} \end{bmatrix} = 0 \quad \begin{matrix} \forall i, j = 0, \dots, n, \\ \forall k, l = 0, \dots, m. \end{matrix}$$

Определим обратное отображение $S_{n,m} \rightarrow \mathbb{P}^n \times \mathbb{P}^m$ следующим образом. Для каждой точки $P \in S_{n,m}$ существует по крайней мере одна пара (i, j) , такая, что $U_{ij}(P) \neq 0$. Зафиксируем эту пару (i, j) и зададим отображение

$$S_{n,m} \ni P \mapsto ((U_{0j}, \dots, U_{nj}), (U_{i0}, \dots, U_{im})) \in \mathbb{P}^n \times \mathbb{P}^m.$$

Заметим, что конкретный выбор пары (i, j) не имеет значения, так как ранг матрицы $U_{ij}(P)$ равен 1 и, следовательно, все ее строки и столбцы пропорциональны.

Отсюда нетрудно заключить, что если $V \subset \mathbb{P}^n$ и $W \subset \mathbb{P}^m$ — проективные многообразия, то $V \times W \subset \mathbb{P}^n \times \mathbb{P}^m \cong S_{n,m} \subset \mathbb{P}^N$ также проективно (см. упр. 5.11).

Упражнения к § 5.

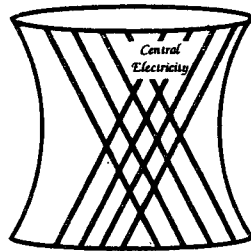
5.1. Докажите, что регулярная на $\mathbb{P}^1$ функция является константой. (Указание. Пользуясь обозначениями разд. (5.0), предположите, что $f \in k(\mathbb{P}^1)$ регулярна во всех точках $\mathbb{P}^1$. Примените предложение (4.8(II)) к аффинному куску $\mathbb{A}_{(0)}^1$, чтобы показать, что $f = p(x_0) \in k[x_0]$. Тогда в другом аффинном куске $\mathbb{A}_{(\infty)}^1$ имеем $f = p(1/y_1) \in k[y_1]$. Но как же $p(1/y_1)$ может быть многочленом? Выведите отсюда, что ни для какого m не существует непостоянного морфизма $\mathbb{P}^1 \rightarrow \mathbb{A}^m$).

5.2. Квадрика в $\mathbb{P}^3$. (i) Покажите, что вложение Сегре пространства $\mathbb{P}^1 \times \mathbb{P}^1$ (как в (5.10)) задает изоморфизм $\mathbb{P}^1 \times \mathbb{P}^1$ и квадрики

$$S_{1,1} = Q: (X_0 X_3 = X_1 X_2) \subset \mathbb{P}^3.$$

(ii) Каковы образы в Q двух семейств прямых $\{p\} \times \mathbb{P}^1$ и $\mathbb{P}^1 \times \{p\}$ на $\mathbb{P}^1 \times \mathbb{P}^1$? Воспользуйтесь этим, чтобы построить непересекающиеся прямые на $\mathbb{P}^1 \times \mathbb{P}^1$, и как следствие получите, что $\mathbb{P}^1 \times \mathbb{P}^1 \not\cong \mathbb{P}^2$.

(То обстоятельство, что квадратичная поверхность имеет две системы образующих прямых, находит применение в архитектуре. Если вам необходимо построить искривленную поверхность из бетона, то возможность задать ее форму, используя линейные ребра жесткости, является очевидным преимуществом. (См. [Берже, 14.4.6—7 и 15.3.3], где приведены обсуждения и рисунки.)



(iii) Покажите, что имеются две прямые на Q , проходящие через точку $P = (1, 0, 0, 0)$, и что дополнение U к этой паре прямых является образом пространства $\mathbb{A}^1 \times \mathbb{A}^1$ при вложении Сегре.

(iv) Покажите, что при проекции $\pi|_Q: Q \rightarrow \mathbb{P}^2$ (в обозначениях (5.7(2))) U изоморфно отображается на экземпляр $\mathbb{A}^2$, а две прямые, проходящие через точку P , отображаются в точки на $\mathbb{P}^2$.

(v) Вычислите $\text{dom } \varphi$ и $\text{dom } \pi$ (в обозначениях (5.7(2))) и дайте геометрическую интерпретацию особенностей отображений π и φ .

5.3. Какие из приведенных ниже выражений задают рациональные отображения $\varphi: \mathbb{P}^n \rightarrow \mathbb{P}^m$ проективных пространств соответствующих размерностей ($n, m = 1$ или 2)? В каждом случае вычислите $\text{dom } \varphi$, укажите, является ли φ бирациональным, и если является, то опишите обратное отображение.

- (a) $(x, y, z) \mapsto (x, y)$; (b) $(x, y) \mapsto (x, y, 1)$;
- (c) $(x, y) \mapsto (x, y, 0)$; (d) $(x, y, z) \mapsto (1/x, 1/y, 1/z)$;
- (e) $(x, y, z) \mapsto ((x^3 + y^3)/z^3, y^2/z^2, 1)$;
- (f) $(x, y, z) \mapsto (x^2 + y^2, y^2, y^2)$.

5.4. Рациональной норм-кривой третьей степени называется (см. 5.7(1)) кривая $C \subset \mathbb{P}^3$, определенная пересечением трех квадрик $C = Q_1 \cap Q_2 \cap Q_3$, где

$$Q_1: (XZ = Y^2), Q_2: (XT = YZ), Q_3: (YT = Z^2).$$

Эта кривая называется также *скрученной кубикой*, где «скрученная» означает, что рассматриваемая кривая не является плоской. Проверьте, что для любых двух квадрик Q_i и Q_j пересечение $Q_i \cap Q_j = C \cup l_{ij}$, где l_{ij} — некоторая прямая. Значит, кривая C в трехмерном пространстве отличается от пересечения любых двух квадрик.

5.5. Пусть $Q_1: (XZ = Y^2)$ и $F: (XT^2 - 2YZT + Z^3 = 0)$. Докажите, что $C = Q_1 \cap F$ является скрученной кубикой из упр. 5.4. (Указание. После умножения F на X и вычитания подходящего кратного Q_1 получается точный квадрат.)

5.6. Пусть $C \subset \mathbb{P}^3$ — неприводимая кривая, определенная соотношением $C = Q_1 \cap Q_2$, где $Q_1: (TX = q_1)$ и $Q_2: (TY = q_2)$, а q_1 и q_2 — квадратичные формы от X, Y, Z . Покажите, что ограничение проекции $\pi: \mathbb{P}^3 \rightarrow \mathbb{P}^2$, заданной формулой $(X, Y, Z, T) \mapsto (X, Y, Z)$, задает изоморфизм кривой C и плоской кривой $D \subset \mathbb{P}^2$, определенной уравнением $Xq_2 = Yq_1$.

5.7. Пусть $\varphi: \mathbb{P}^1 \rightarrow \mathbb{P}^1$ — некоторый изоморфизм. (Представьте график φ как подмногообразие в $\mathbb{P}^1 \times \mathbb{P}^1 \cong Q \subset \mathbb{P}^3$. Прodelайте то же самое для двулистного накрытия $\varphi: \mathbb{P}^1 \rightarrow \mathbb{P}^1$, заданного формулой $(X, Y) \mapsto (X^2, Y^2)$).

5.8. Докажите, что любая неприводимая квадрика $Q \subset \mathbb{P}^{n+1}$ рациональна, т. е. покажите, что если $P \in Q$ — неособая точка, то линейная проекция $\mathbb{P}^{n+1}$ на $\mathbb{P}^n$ индуцирует бирациональное отображение $Q \rightarrow \mathbb{P}^n$ (как на рисунке из (5.7(2))).

5.9. Запишите уравнение каждой из следующих плоских кривых в 3-х стандартных аффинных кусках и определите пересечение этих кривых с координатными осями:

- (a) $y^2 z = x^3 + axz^2 + bz^3$;
- (b) $x^2 y^2 + x^2 z^2 + y^2 z^2 = 2xyz(x + y + z)$;
- (c) $xz^3 = (x^2 + y^2)y^2$.

5.10. (i) Докажите, что произведение двух неприводимых алгебраических множеств неприводимо. (Указание. Подмножества вида $V \times \{w\}$ неприводимы для $w \in W$. Для заданного разложения $V \times W = U_1 \cup U_2$ рассмотрите подмножества $W_i = \{w \in W \mid V \times \{w\} \subset U_i\}$, $i = 1, 2$.)

(ii) Опишите замкнутые подмножества в топологии на $\mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1$, которая является произведением топологий Зарисского сомножителей. Найдите замкнутое подмножество в топологии Зарисского на $\mathbb{A}^2$, которое не имеет такого вида.

5.11. (a) Пусть $\mathbb{A}_{(0)}^n$ и $\mathbb{A}_{(0)}^m$ — стандартные аффинные куски на $\mathbb{P}^n$ и $\mathbb{P}^m$ соответственно. Проверьте, что при вложении Сегре из (5.11) $\mathbb{A}_{(0)}^n \times \mathbb{A}_{(0)}^m$ изоморфно отображается на аффинный кусок многообразия $S_{n,m} \subset \mathbb{P}^N$, который мы обозначим через $S_{(0)} \subset \mathbb{A}^N$, и что N координат в $\mathbb{A}^N$ переходят при ограничении в $X_1, \dots, X_n, Y_1, \dots, Y_m$ и nm произведений $X_i Y_j$.

(b) Пусть $V \subset \mathbb{P}^n$ и $W \subset \mathbb{P}^m$. Докажите, что произведение $V \times W$ является проективным подмногообразием в $\mathbb{P}^n \times \mathbb{P}^m = S_{n,m} \subset \mathbb{P}^N$. (Указание. Произведение аффинных кусков $V_{(0)} \times W_{(0)} \subset \mathbb{A}^{n+m}$ является, как объяснялось в (5.11), подмногообрази-

ем, заданным многочленами. Покажите, что каждый из них является ограничением на $\mathbb{A}^{n+m} \cong S_{(0)}$ однородных многочленов от переменных U_{ij} .

5.12. Пусть C — кубическая кривая из разд. (5.0). Докажите, что любая регулярная функция f на C является константой. Проведите доказательство в следующей последовательности:

Шаг 1. Применяя (4.8 (II)) к аффинному куску $C_{(0)}$, запишите f в виде $f = p(x, y) \in k[x, y]$.

Шаг 2. Вычитая подходящее кратное выражения $y^2 - x^3 - ax - b$, добейтесь, чтобы $p(x, y)$ имело вид $p(x, y) = q(x) + yr(x)$, где $q, r \in k[x]$.

Шаг 3. Применяя (4.8 (II)) к аффинному куску $C_{(\infty)}$, запишите

$$f = q(x_1/z_1) + (1/z_1)r(x_1/z_1) \in k[C_{(\infty)}].$$

Таким образом, существует многочлен $S(x_1, z_1)$, такой, что

$$q(x_1/z_1) + (1/z_1)r(x_1/z_1) = S(x_1, z_1).$$

Шаг 4. Выполнив приведение к общему знаменателю и используя тот факт, что $k[C_{(\infty)}] = k[x_1, z_1]/g$, где $g = z_1^2 - x_1^3 - ax_1z_1^2 - bz_1^3$, получите следующее полиномиальное тождество в кольце $k[x_1, z_1]$:

$$Q_m(x_1, z_1) + R_{m-1}(x_1, z_1) = S(x_1, z_1)z_1^m + A(x_1, z_1)g,$$

где Q_m и R_{m-1} — однородные многочлены указанных степеней.

Шаг 5. Теперь, если разложить $S = S^+ + S^-$ и $A = A^+ + A^-$ в сумму членов четной и нечетной степеней и заметить, что g содержит только члены нечетной степени, то тождество при четном m распадается на два:

$$Q_m = S^+ z_1^m + A^- g \text{ и } R_{m-1} = S^- z_1^m + A^+ g.$$

Аналогичное разложение имеет место для нечетного m .

Шаг 6. Q_m — однородный многочлен степени m . Следовательно, $A^- g$ имеет степень $\geq m$. Рассматривая член наименьшей степени в $A^- g$, докажите, что Q_m делится на z_1 . Аналогичное свойство имеет место для R_{m-1} . Взяв минимальное значение m в тождестве шага 4, докажите, что $q(x)$ имеет степень 0 и $r(x) = 0$.

5.13. Поверхность Веронезе. Изучите вложение $\varphi: \mathbb{P}^2 \rightarrow \mathbb{P}^5$, заданное формулой $(X, Y, Z) \mapsto (X^2, XY, XZ, Y^2, YZ, Z^2)$. Напишите уравнения, определяющие образ $S = \varphi(\mathbb{P}^2)$, и докажите, что φ — изоморфизм (выписывая уравнения для обратного морфизма). Покажите, что прямые на $\mathbb{P}^2$ переходят в коники в $\mathbb{P}^5$, а коники на $\mathbb{P}^2$ переходят в скрученные квартики в $\mathbb{P}^5$ (см. (5.7)).

Для любой прямой $l \subset \mathbb{P}^2$ обозначим через $\pi(l) \subset \mathbb{P}^5$ проективную плоскость, натянутую на конику $\varphi(l)$. Покажите, что объединение $\pi(l)$ по всем $l \subset \mathbb{P}^2$ является кубической гиперповерхностью $\Phi \subset \mathbb{P}^5$ (Указание. Вы можете, как в разд. (5.7) и (5.11), записать уравнения, задающие S , в виде условия $\text{rank } M \leq 1$, где M — симметрическая 3×3 -матрица, элементы которой — однородные координаты на $\mathbb{P}^5$. Покажите, что Φ задается уравнением $\Phi: (\det M = 0)$. Дальнейшие детали см. в [Semple, Roth, p. 128].

§ 6. Касательное пространство и неособость, размерность

(6.1) Неособые точки гиперповерхности. Пусть $f \in k[X_1, \dots, X_n]$ — неприводимый многочлен, $f \notin k$. Положим $V = V(f) \subset \mathbb{A}^n$. Пусть

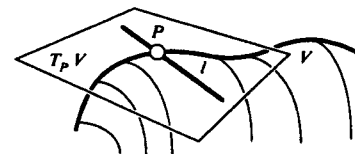
$P = (a_1, \dots, a_n) \in V$ — точка и l — прямая, проходящая через точку P . Так как $P \in V$, то P , очевидно, является корнем $f|_l$.

Вопрос. Когда P — кратный корень $f|_l$?

Ответ. P является кратным корнем тогда и только тогда, когда l лежит в аффинном подпространстве

$$T_P V: \left(\sum_i \frac{\partial f}{\partial X_i}(P) \cdot (X_i - a_i) = 0 \right) \subset \mathbb{A}^n,$$

которое называется касательным пространством к V в точке P .



Для доказательства параметризуем l так:

$$l: X_i = a_i + b_i T,$$

где $P = (a_1, \dots, a_n)$, а $(b_1, \dots, b_n)$ — направляющий вектор прямой l . Тогда $f|_l = f(\dots, a_i + b_i T, \dots) = g(T)$ является многочленом по T , и мы знаем, что $T = 0$ является одним из корней g . Следовательно,

$$0 \text{ — кратный корень } g \Leftrightarrow \frac{\partial g}{\partial T}(0) = 0,$$

т. е.

$$\Leftrightarrow \sum_i b_i \frac{\partial f}{\partial X_i}(P) = 0 \Leftrightarrow l \subset T_P V.$$

Определение. $P \in V \subset \mathbb{A}^n$ называется неособой точкой поверхности V , если $\partial f / \partial X_i(P) \neq 0$ для некоторого i . В противном случае P называется особой точкой V .

Очевидно, что если P — неособая точка, то $T_P V$ является $(n-1)$ -мерным аффинным подпространством в $\mathbb{A}^n$, и $T_P V = \mathbb{A}^n$ для особой точки P .

(6.2) Замечания. (а) Используя выше частные производные $\partial f / \partial X_i(P)$ в действительности можно считать формальными алгебраическими операциями (а именно, $\partial / \partial X_i$ переводит X_i^n в nX_i^{n-1}). Дифференциальным исчислением здесь и не пахнет.

(b) Предположим, что $k = \mathbb{R}$ или $k = \mathbb{C}$ и $\partial f / \partial X_i(P) \neq 0$. Для определенности положим $i = 1$. Тогда отображение $p: \mathbb{A}^n \rightarrow \mathbb{A}^n$, заданное формулой $(X_1, \dots, X_n) \mapsto (f, X_2, \dots, X_n)$, имеет в точке P ненулевой якобиан. Таким образом, по теореме об обратной функции существует окрестность $P \in U \subset \mathbb{A}^n$ точки P , такая, что $p|_U: U \rightarrow p(U) \subset \mathbb{A}^n$ является диффеоморфизмом U и открытого множества $p(U)$ в $\mathbb{A}^n$ (в обычной топологии пространств $\mathbb{R}^n$ или $\mathbb{C}^n$). Это означает, что $p|_U$ — биекция, а p и p^{-1} являются дифференцируемыми функциями (вещественных или комплексных) переменных. Другими словами, $(f, X_2, \dots, X_n)$ задают новую дифференцируемую систему координат в $\mathbb{A}^n$ в окрестности точки P . Отсюда вытекает, что окрестность точки P на $V: (f = 0)$ диффеоморфна открытому подмножеству в $\mathbb{A}^{n-1}$ с координатами $(X_2, \dots, X_n)$. Значит, V в окрестности неособой точки P является гладким многообразием с локальными координатами $(X_2, \dots, X_n)$.

(6.3) Предложение. Множество $V_{\text{nonsing}} = \{P \in V \mid P \text{ неособа}\}$ является плотным открытым по Зарисскому множеством в V .

Доказательство. Дополнением к V_{nonsing} является множество V_{sing} особых точек, которое определяется системой $\partial f / \partial X_i(P) = 0$ для всех i , т. е.

$$V_{\text{sing}} = V \left(f, \frac{\partial f}{\partial X_1}, \dots, \frac{\partial f}{\partial X_n} \right) \subset \mathbb{A}^n;$$

оно замкнуто по определению топологии Зарисского. Так как V неприводимо (согласно (3.11)), то для того, чтобы доказать, что открытое множество V_{nonsing} является плотным, достаточно (согласно предложению (4.2)) показать, что оно непусто. Рассуждая от противного, предположим, что оно пусто, т. е. $V = V(f) = V_{\text{sing}}$. Тогда каждый из многочленов $\partial f / \partial X_i$ обращается в нуль на всем V . Следовательно (опять в силу (3.11)) получаем, что они должны делиться на f в кольце $k[X_1, \dots, X_n]$. Но производная $\partial f / \partial X_i$, рассматриваемая как многочлен от переменной X_i , имеет степень, строго меньшую, чем многочлен f . Следовательно, если $\partial f / \partial X_i$ делится на f , то $\partial f / \partial X_i = 0$ как многочлен. Над полем $\mathbb{C}$ это, очевидно, возможно, только если переменная X_i не входит в многочлен f . Таким образом, если это выполняется для всех i , то f равен комплексной константе, что невозможно. Над произвольным полем k условие $\partial f / \partial X_i = 0$ выполняется, только если многочлен f несепаабелен по переменной X_i , т. е. если $\text{char } k = p$ и X_i входит в f только в p -й степени. Если это выполняется для всех i , то, согласно рассужде-

нию из разд. (3.16), многочлен f является в кольце $k[X_1, \dots, X_n]$ p -й степени, что противоречит неприводимости f . Ч. т. д.

(6.4) Касательное пространство.

Определение. Пусть $V \subset \mathbb{A}^n$ — подмногообразие, а $V \ni P = (a_1, \dots, a_n) \in V$ — его точка. Положим для любого $f \in k[X_1, \dots, X_n]$

$$f_P^{(1)} = \sum_i \frac{\partial f}{\partial X_i}(P) \cdot (X_i - a_i).$$

Это линейный неоднородный многочлен (т. е. линейный член плюс константа), являющийся линейной частью многочлена f в точке P . Определим теперь касательное пространство к V в точке P соотношением

$$T_P V = \bigcap (f_P^{(1)} = 0) \subset \mathbb{A}^n.$$

где пересечение берется по всем $f \in I(V)$.

(6.5) Предложение. Функция $V \rightarrow \mathbb{N}$, заданная правилом $P \mapsto \dim T_P V$, полунепрерывна сверху (в топологии Зарисского многообразия V). Другими словами, для любого r подмножество

$$S(r) = \{P \in V \mid \dim T_P V \geq r\} \subset V$$

замкнуто.

Доказательство. Пусть $(f_1, \dots, f_m)$ — набор образующих идеала $I(V)$. Легко видеть, что линейная часть $g_P^{(1)}$ любого многочлена $g \in I(V)$ является линейной комбинацией линейных частей f_i , что упрощает определение $T_P V$ до следующего:

$$T_P V = \bigcap_{i=1}^m (f_i^{(1)} = 0) \subset \mathbb{A}^n.$$

Далее с помощью элементарной линейной алгебры получаем, что

$$P \in S(r) \Leftrightarrow \text{матрица } \left(\frac{\partial f_i}{\partial X_j}(P) \right)_{i=1, \dots, m, j=1, \dots, n} \text{ имеет ранг } \leq n - r \Leftrightarrow$$

$$\Leftrightarrow \text{каждый } (n - r + 1) \times (n - r + 1)\text{-минор матрицы } \left(\frac{\partial f_i}{\partial X_j}(P) \right)_{ij}$$

обращается в нуль.

Каждый элемент матрицы $\partial f_i / \partial X_j(P)$ является многочленом по P .

Следовательно, каждый минор — это детерминант полиномиальной матрицы и тем самым многочлен. Таким образом, $S(r) \subset V \subset \mathbb{A}^n$ — алгебраическое подмножество. Ч. т. д.

(6.6) Следствие-определение. Существует целое число r и открытое плотное подмножество $V_0 \subset V$, такие, что

$$\dim T_P V = r \text{ для всех } P \in V_0 \text{ и } \dim T_P V \geq r \text{ для всех } P \in V.$$

Назовем r размерностью многообразия V , $\dim V = r$, и скажем, что точка $P \in V$ неособая, если $\dim T_P V = r$, и особая, если $\dim T_P V > r$. Многообразие называется неособым, если каждая его точка неособая.

Доказательство. Пусть r равняется минимуму $\{\dim T_P V\}$, где минимум берется по всем точкам $P \in V$. Тогда очевидно, что

$$S(r-1) = \emptyset, S(r) = V \text{ и } S(r+1) \text{ строго содержится в } V.$$

Следовательно, множество $S(r) \setminus S(r+1) = \{P \in V \mid \dim T_P V = r\}$ открыто и непусто. Ч. т. д.

(6.7) Из (6.3) следует, что если $V = V(f) \subset \mathbb{A}^n$ — гиперповерхность, определяемая некоторым многочленом f , отличным от константы, то $\dim V = n - 1$. С другой стороны, в случае гиперповерхности координатное кольцо имеет вид $k[V] = k[X_1, \dots, X_n]/(f)$, т. е., предположив, что X_1 входит в f нетривиальным образом, получаем для поля функций представление

$$k(V) = k(X_2, \dots, X_n)[X_1]/(f),$$

т. е. оно получается из поля k присоединением $n - 1$ алгебраически независимых элементов и затем взятием примитивного алгебраического расширения.

Определение. Пусть $k \subset K$ — расширение полей. Степенью трансцендентности поля K над k назовем максимальное число элементов из K , алгебраически независимых над k . Оно обозначается через $\text{tr deg}_k K$.

Элементарная теория степени трансцендентности расширений полей K/k с формальной точки зрения вполне аналогична теории размерности векторных пространств. Что означает алгебраическая независимость данных элементов $\alpha_1, \dots, \alpha_m \in K$ над k , нам уже известно (см. (3.13)). Они порождают трансцендентную часть расши-

рения, если $K/k(\alpha_1, \dots, \alpha_m)$ алгебраично, и образуют трансцендентный базис, если они алгебраически независимы и порождают трансцендентную часть. Легко доказывается утверждение, что трансцендентный базис является максимальным алгебраически независимым множеством и минимальным порождающим множеством; кроме того, любые два трансцендентных базиса в K/k состоят из одинакового числа элементов (см. упр. 6.1).

Таким образом, для гиперповерхности $V \subset \mathbb{A}^n$ имеем $\dim V = n - 1 = \text{tr deg}_k k(V)$. Оставшаяся часть этого параграфа посвящена доказательству того, что равенство $\dim V = \text{tr deg}_k k(V)$ выполняется для произвольных многообразий, с помощью редукции к случаю гиперповерхностей. Прежде всего мы докажем, что для любой точки многообразия $P \in V$ касательное пространство $T_P V$, которое до настоящего момента определялось с помощью конкретной системы координат в объемлющем пространстве $\mathbb{A}^n$, в действительности имеет локальное инвариантное определение в окрестности точки $P \in V$.

(6.8) Инвариантная природа пространства $T_P V$. Начиная с этого момента, мы будем связывать с каждой точкой $P = (a_1, \dots, a_n) \in V \subset \mathbb{A}^n$ новую систему координат $X'_i = X_i - a_i$, перенося тем самым точку P в начало координат $P = (0, \dots, 0)$. Тогда $T_P V \subset \mathbb{A}^n$ — линейное подпространство в k^n .

Обозначения. Обозначим через m_P идеал точки P в $k[V]$, а через M_P

$$\text{идеал } (X_1, \dots, X_n) \subset k[X_1, \dots, X_n].$$

Тогда очевидно, что $m_P = M_P/I(V) \subset k[V]$.

Теорема. Во введенных обозначениях

(а) имеет место естественный изоморфизм векторных пространств

$$(T_P V)^* = m_P/m_P^2,$$

где $(\)^*$ обозначает двойственное векторное пространство.

(б) Если функция $f \in k[V]$ такова, что $f(P) \neq 0$, и $V_f \subset V$, как и в разд. (4.13), — стандартное аффинное открытое множество, то естественное отображение

$$T_P(V_f) \rightarrow T_P V$$

является изоморфизмом.

Доказательство п. (а). Обозначим через $(k^n)^*$ векторное пространство линейных форм на k^n , т. е. векторное пространство с базисом $X_1, \dots, X_n$. Так как $P = (0, \dots, 0)$, то для любой функции $f \in k[X_1, \dots, X_n]$ ее линейная часть f_P^1 естественно является элементом из $(k^n)^*$. Определим отображение $d: M_P \rightarrow (k^n)^*$, сопоставляя $f \in M_P$ элемент $d_f = f_P^{(1)}$.

Отображение d сюръективно, так как элементы $X_i \in M_P$ отображаются в естественный базис пространства $(k^n)^*$. Кроме того, $\ker d = M_P^2$, так как

$$f_P^{(1)} = 0 \Leftrightarrow f \text{ начинается с квадратичных по } X_1, \dots, X_n \text{ членов} \Leftrightarrow f \in M_P^2.$$

Следовательно, $M_P/M_P^2 \cong (k^n)^*$. Это и есть утверждение (а) для частного случая $V = \mathbb{A}^n$. В общем случае имеет место отображение ограничения $(k^n)^* \rightarrow (T_P V)^*$, двойственное включению $T_P V \subset k^n$, переводящее линейную форму λ на k^n в ее ограничение на $T_P V$. Взяв композицию рассмотренных отображений, получаем

$$D: M_P \rightarrow (k^n)^* \rightarrow (T_P V)^*.$$

Композиция D сюръективна, так как сюръективно каждое из составляющих отображений.

Покажем, что ядро отображения D совпадает с $M_P^2 + I(V)$ и, значит,

$$m_P/m_P^2 = M_P/(M_P^2 + I(V)) \cong (T_P V)^*,$$

что нам и требуется. Чтобы доказать это утверждение, воспользуемся тем, что

$$f \in \ker D \Leftrightarrow f_P^{(1)}|_{T_P V} = 0 \Leftrightarrow f_P^{(1)} = \sum_i a_i g_i^{(1)}|_{T_P V} \text{ для некоторых } g_i \in I(V)$$

(так как $T_P V \subset k^n$ является векторным подпространством, определенным условием $g_P^{(1)} = 0$ для $g \in I(V)$). Цепочка эквивалентностей продолжается:

$$\Leftrightarrow f - \sum_i a_i g_i \in M_P^2 \text{ для некоторых } g_i \in I(V) \Leftrightarrow f \in M_P^2 + I(V). \text{ Ч. т. д.}$$

Доказательство п. (б) теоремы (6.8) остается читателю (см. упр. 6.2).

(6.9) Следствие. С точностью до изоморфизма $T_P V$ зависит только от окрестности точки $P \in V$. Точнее, пусть $P \in V_0 \subset V$ и $Q \in W_0 \subset W$ — открытые подмножества аффинных многообразий и $\varphi: V_0 \rightarrow W_0$ — изоморфизм, переводящий P в Q ; тогда имеет ме-

сто естественный изоморфизм $T_P V_0 \rightarrow T_Q W_0$. Следовательно, $\dim T_P V_0 = \dim T_Q W_0$.

В частности, если V и W — бирационально эквивалентные многообразия, то $\dim V = \dim W$.

Доказательство. Переходя к меньшей окрестности точки P в V , мы можем считать, что V_0 изоморфно аффинному многообразию (предложение (4.13)). Тогда и W_0 обладает теми же свойствами, а отображение φ индуцирует изоморфизм $k[V_0] \cong k[W_0]$, переводящий t_P в t_Q . Последнее утверждение верно, поскольку в силу (5.8) V и W содержат изоморфные открытые плотные подмножества.

(6.10) Теорема. $\dim V = \operatorname{tr} \deg k(V)$ для любого многообразия.

Доказательство. Этот факт уже установлен, если V — гиперповерхность. С другой стороны (в силу (5.10)) каждое многообразие бирационально эквивалентно гиперповерхности, а обе части доказываемого соотношения для бирационально эквивалентных многообразий одинаковы. Ч.т.д.

(6.11) Неособость и проективные многообразия. Хотя приведенные результаты были получены для случая аффинных многообразий, понятие неособости и размерности непосредственно применимы к произвольному многообразию V . А именно, точка $P \in V$ неособа, если она является неособой в содержащей ее аффинной части $V_0 \subset V$. В силу следствия (6.9) это понятие не зависит от выбора V_0 . С другой стороны, для проективного многообразия $V \subset \mathbb{P}^n$ касательное пространство к V в точке P иногда удобно рассматривать как проективное подпространство в $\mathbb{P}^n$. Я дам определение только для случая гиперповерхности. Пусть $V = V(f)$ — гиперповерхность, определенная формой (т. е. однородным многочленом) $f \in k[X_0, \dots, X_n]$ степени d и $V \ni P = (a_0, \dots, a_n)$; тогда уравнение $\sum \partial f / \partial X_i(P) \cdot X_i = 0$ задает в $\mathbb{P}^n$ гиперплоскость, которая играет роль касательного пространства к V в точке P . Если $P \in \mathbb{A}_{(0)}^n$, то эта проективная гиперплоскость является проективным замыканием аффинной касательной гиперплоскости к $V_{(0)}$ в точке P , что легко проверяется с помощью формулы Эйлера: если $f \in k[X_0, \dots, X_n]$ — однородный многочлен степени d , то

$$\sum X_i \left(\frac{\partial f}{\partial X_i} \right) = df.$$

В силу этой формулы для того, чтобы определить, является ли точка $P \in \mathbb{P}^n$ особой точкой на многообразии V , нам достаточно проверить $n + 1$ из $n + 2$ условий

$$f(P) = 0, \quad \frac{\partial f}{\partial X_i}(P) = 0, \quad i = 0, \dots, n.$$

Так например, в случае, если степень многочлена f не делится на $\text{char } k$, имеем

$$\frac{\partial f}{\partial X_i}(P) = 0 \text{ для } i = 0, \dots, n \Rightarrow f(P) = 0,$$

и точка $P \in V$ является особенностью.

(6.12) Пример. Раздутие. Пусть $B = \mathbb{A}^2$ — плоскость с координатами (u, v) и $\sigma: B \rightarrow \mathbb{A}^2$ — отображение $(u, v) \mapsto (x = u, y = uv)$. Очевидно, что σ — бирациональный морфизм. Он отображает v -ось $l: (u = 0)$ в точку 0 и является изоморфизмом вне этого исключительного множества. Постараемся выяснить, что произойдет под действием σ с кривой $C: (f = 0) \subset \mathbb{A}^2$. Вопрос нетривиален только в случае, когда C проходит через точку 0.

Очевидно, что $\sigma^{-1}(C) \subset B$ является алгебраическим подмножеством, определенным формулой $(f \circ \sigma)(u, v) = f(u, uv) = 0$. Так как по предположению точка 0 принадлежит C , то прямая $l: (u = 0)$ содержится в $\sigma^{-1}(C)$, или, эквивалентно, $u \mid f(u, uv)$. Легко понять, что наибольшая степень u , на которую делится $f(u, uv)$, равна наименьшей степени $m = a + b$ одночленов $x^a y^b$, встречающихся в f , т. е. кратности f в нуле. Значит, $\sigma^{-1}(C)$ является объединением исключительной кривой $\sigma^{-1}(0) = l$ (взятой с кратностью m) и новой кривой C_1 , определенной многочленом $f_1(u, v) = f(u, uv)/u^m$. Рассмотрим следующие примеры:

$$(a) f = \alpha x - y + \dots; \quad (b) f = y^2 - x^2 + \dots \text{ или } (c) f = y^2 - x^3,$$

где многоточие обозначает члены более высокой степени. Очевидно, что в случае (a) функция f имеет кратность 1 и $f_1 = \alpha - v + \dots$ (где многоточие обозначает члены, которые делятся на u). Таким образом, C_1 также является неособой и пересекает l в точке $(0, \alpha)$ трансверсально. Это означает, что σ заменяет точку $0 \in \mathbb{A}^2$ на прямую l , точки которой соответствуют касательным направлениям в точке 0 (за исключением прямой $(x = 0)$). В случае (b) $f_1 = v^2 - 1 + \dots$, т. е. C_1 имеет над точкой $0 \in C$ две неособые точки $(0, \pm 1)$. Тем самым раздутие σ «разделяет две ветви» особой

кривой C . В случае (c) $f_1 = v^2 - u$, т. е. C_1 неособа, но над точкой 0 она касается стягиваемой кривой l .

В обоих случаях (b) и (c) отображение σ заменяет особую кривую C неособой кривой C_1 , которая бирационально эквивалентна C (благодаря введению «новых координат» $u = x, v = y/x$). Это и принято понимать под разрешением особенностей. В случае плоских кривых разрешение можно сделать с помощью цепочки раздутий (примеры см. в упр. 6.6, а дальнейшие подробности — в книге [Fulton, p. 162—171]); В этом случае процесс разрешения особенностей дает об особенностях подробную информацию. Знаменитая теорема Х. Хиронаки гарантирует возможность разрешения особенностей с помощью раздутий (в любой размерности над полем нулевой характеристики). Это — ключевой теоретический результат, который сводит изучение многообразий с точностью до бирациональной эквивалентности к исследованию неособых многообразий. Однако сам процесс разрешения особенностей с помощью раздутий является в общем случае очень сложным и не всегда способствует пониманию особенностей или многообразий, их содержащих.

Упражнения к § 6

6.1. Пусть $k \subset K$ — расширение полей, а $(u_1, \dots, u_r)$ и $(v_1, \dots, v_s)$ — два набора элементов поля K . Предположим, что $u_1, \dots, u_r$ алгебраически независимы, а $v_1, \dots, v_s$ алгебраически порождают расширение $k \subset K$. Докажите, что $r \leq s$. (Указание. Шаг индукции заключается в том, чтобы предположить, что $u_1, \dots, u_i, v_1, \dots, v_s$ алгебраически порождают K/k и рассмотреть u_{i+1} .) Выведите отсюда, что любые два трансцендентных базиса в K/k имеют одинаковое число элементов.

6.2. Докажите теорему (6.8 (b)) (Указание. $I(V_f) = (I(V), Yf - 1) \subset k[X_1, \dots, X_n, Y]$, так что если $Q = (a_1, \dots, a_n, b) \in V_f$, то $T_Q V_f \subset \mathbb{A}^{n+1}$ определяется уравнениями для касательной плоскости $T_P V \subset \mathbb{A}^n$ и одним уравнением, включающим Y .)

6.3. Найдите все особые точки следующих кривых в $\mathbb{A}^2$:

- (a) $y^2 = x^3 - x$; (b) $y^2 = x^3 - 6x^2 + 9x$;
(c) $x^2 y^2 + x^2 + y^2 + 2xy(x + y + 1) = 0$;
(d) $x^2 = x^4 + y^4$; (e) $xy = x^6 + y^6$;
(f) $x^3 = y^2 + x^4 + y^4$; (g) $x^2 y + xy^2 = x^4 + y^4$.

6.4. Найдите все особые точки поверхностей в $\mathbb{A}^3$, заданных уравнениями
(a) $xy^2 = z^2$; (b) $x^2 + y^2 = z^2$; (c) $xy + x^3 + y^3 = 0$.

(Вам будет полезно нарисовать в меру своих возможностей вещественные части этих поверхностей. Алгебраические геометры, как правило, рисовать не умеют.)

6.5. Покажите, что гиперповерхность $V_d \subset \mathbb{P}^n$, заданная уравнением

$$X_0^d + X_1^d + \dots + X_n^d = 0,$$

неособа (если d не делится на $\text{char } k$).

6.6 (а) Пусть $C_n \subset \mathbb{A}^2$ — кривая, заданная многочленом $f_n = y^2 - x^{2n+1}$, $\sigma: B \rightarrow \mathbb{A}^2$ — отображение из (6.12), а $l = \sigma^{-1}(0)$. Покажите, что $\sigma^{-1}(C_n)$ разлагается в объединение l и кривой, изоморфной C_{n-1} . Докажите, что особенность кривой C_n может быть разрешена цепочкой из n раздутий.

(б) Покажите, как разрешить особенности следующих кривых с помощью одного или нескольких раздутий: (i) $y^3 = x^4$, (ii) $y^3 = x^5$, (iii) $(y^2 - x^2)(y^2 - x^5) = x^8$.

6.7. Докажите, что пересечение гиперповерхности $V \subset \mathbb{A}^n$ (не являющейся гиперплоскостью) с касательной гиперплоскостью $T_P V$ особо в точке P .

§ 7. 27 прямых на кубической поверхности

В этом параграфе $S \subset \mathbb{P}^3$ будет означать неособую кубическую поверхность, заданную однородной кубикой $f = f(X, Y, Z, T)$. Рассмотрим прямые l в $\mathbb{P}^3$, лежащие на S .

(7.1) Следствия неособости.

Предложение. (а) *Через любую точку $P \in S$ проходит не более трех прямых, лежащих на S . Если этих прямых две или три, то они лежат в одной плоскости* (см. рисунки).



(б) *Произвольная плоскость $\Pi \subset \mathbb{P}^3$ пересекается с поверхностью S по одной из следующих трех кривых:*

(i) *неприводимая кубика; (ii) коника и прямая; (iii) три различные прямые.*

Доказательство. (а) Если $l \subset S$, то $l = T_P l \subset T_P S$, так что все прямые на поверхности S , проходящие через точку P , содержатся в плоскости $T_P S$. В силу (б) их число не превышает 3.

(б) Докажем, что кратные прямые исключаются. Пусть $\Pi: (T=0)$ и $l: (Z=0) \subset \Pi$; если прямая l является кратной прямой пересечения $S \cap \Pi$, то f имеет вид

$$f = Z^2 \cdot A(X, Y, Z, T) + T \cdot B(X, Y, Z, T),$$

где A — линейная, а B — квадратичная формы. Тогда поверхность $S: (f=0)$ имеет особенность во всех точках, где $Z = T = B = 0$. Это множество непусто, так как оно является множеством нулей формы B на прямой $l: (Z = T = 0)$.

(7.2) Предложение. *Существует по крайней мере одна прямая l , лежащая на S .*

Имеется несколько способов доказательства этого факта. Стандартное рассуждение основано на подсчете размерностей. А именно, прямые на $\mathbb{P}^3$ параметризуются четырехмерным многообразием, и для того чтобы прямая l лежала на S , требуется выполнение четырех условий (поскольку ограничение f на l является кубической формой, четыре коэффициента которой должны обращаться в нуль). Требуется некоторое усилие, чтобы превратить это рассуждение в строгое доказательство, так как само оно показывает лишь, что множество таких прямых имеет размерность ≥ 0 , а не то, что оно непусто (в разд. (8.15) обсуждается традиционное доказательство и трудности, с которыми приходится в нем сталкиваться).

Вполне логично считать предложение выполненным (т. е. ограничиться рассмотрением кубических поверхностей, содержащих прямые). Ниже я привожу прямое доказательство предложения (7.2) путем явных координатных рассмотрений и исключений. Оно подразделяется на четыре шага. Если вы предпочитаете пропустить его, переходите к (7.3).

Шаг 1 (предварительная конструкция).

Для любой точки $P \in S$ кривая, по которой S пересекается с касательной плоскостью $T_P S$, является плоской кубикой $C = S \cap T_P S$, которая, согласно упр. 6.7, имеет особенность в точке P .

Можно предположить, что кривая C неприводима, ибо в противном случае точка P лежит на прямой в S и доказывать нечего. Таким образом, C — каспидальная или нодальная плоская кубика и в подходящих координатах (X, Y, Z, T) в $\mathbb{P}^3$

$$T_P S: (T=0), P = (0, 0, 1, 0) \text{ и}$$

$$C: (X^2 Z = Y^3) \text{ или } (XYZ = X^3 + Y^3).$$

Какая из этих возможностей реализуется в точке $P \in S$, зависит от матрицы вторых производных (матрицы Гессе) функции f в P . Детальнее это изучается в упр. 7.3, содержащем набросок доказательства (в характеристике $\neq 2$) того, что каспидальный случай обязательно реализуется в какой-нибудь точке $P \in S$.

Для простоты я доказываю предложение (7.2) в каспидальном случае. В принципе доказательство точно так же проходит и в нодальном случае, но исключения становятся довольно неприятными

(см. упр. 7.10). Итак, предположим, что

$$f = X^2 Z - Y^3 + g T,$$

где $g = g_2(X, Y, Z, T)$ — квадратичная форма; $g(0, 0, 1, 0) \neq 0$ в силу гладкости поверхности S в точке P , так что можно положить $g(0, 0, 1, 0) = 1$.

Шаг 2 (формулировка основного утверждения). Рассмотрим переменную точку $P_\alpha = (1, \alpha, \alpha^3, 0) \in S$. Любая прямая в $\mathbb{P}^3$, проходящая через P_α , пересекает дополнительную плоскость $\Pi: (X = 0)$ в точке $Q = (0, Y, Z, T)$. Записываем условие, что прямая $P_\alpha Q$ содержится в S , в терминах α и Q ; разлагая $f(\lambda P_\alpha + \mu Q) = 0$ по степеням λ и μ , получаем

$$P_\alpha Q \subset S \Leftrightarrow A(Y, Z, T) = B(Y, Z, T) = C(Y, Z, T) = 0,$$

где A, B и C — формы степени 1, 2 и 3 от (Y, Z, T) , в коэффициенты которых входит α .

Основное утверждение. Существует нормированный многочлен «результант» $R_{27}(\alpha)$ от α степени 27, такой, что

$$R(\alpha) = 0 \Leftrightarrow A = B = C = 0 \text{ имеет общий нуль } (\eta: \xi: \tau) \text{ в } \mathbb{P}^2.$$

Это утверждение доказывает (7.2), так как из него следует что для каждого корня α многочлена R существует точка $Q = (0: \eta: \xi: \tau)$ в Π , такая, что прямая $P_\alpha Q$ лежит в S . Идея доказательства здесь — стандартное вычисление, связанное с исключением переменных, основанное на упр. 1.10. Остальная часть доказательства заключается в точном выписывании A, B и C .

Шаг 3 (полярная форма). Поляризацией однородного многочлена f называется форма от двух наборов переменных (X, Y, Z, T) и (X', Y', Z', T') , задаваемая формулой

$$f_1(X, Y, Z, T; X', Y', Z', T') = \frac{\partial f}{\partial X} X' + \frac{\partial f}{\partial Y} Y' + \frac{\partial f}{\partial Z} Z' + \frac{\partial f}{\partial T} T'.$$

Из определения касательного пространства (см. (6.4) и (6.10)) ясно, что для $P = (X, Y, Z, T) \in S$ и $P \neq Q = (X', Y', Z', T') \in \mathbb{P}^3$

$$f_1(P; Q) = 0 \Leftrightarrow \text{прямая } PQ \text{ касается } S \text{ в } P.$$

Ясно, что

$$f(\lambda P + \mu Q) = \lambda^3 f(P) + \lambda^2 \mu f_1(P; Q) + \lambda \mu^2 f_1(Q; P) + \mu^3 f(Q),$$

так что для $P \neq Q \in \mathbb{P}^3$ четыре условия

$$f(P) = f_1(P; Q) = f_1(Q; P) = f(Q) = 0$$

являются необходимыми и достаточными для того, чтобы прямая $l = PQ$ лежала на S : ($f = 0$). Более геометрически, они утверждают, что прямая l касается S в обеих точках P и Q , т. е. $f|_l$ имеет в этих точках два двойных корня и в силу предложения (1.8) $l \subset S$.

Поляризация многочлена $f = X^2 Z - Y^3 + g T$ — это

$$f_1 = 2XZ \cdot X' - 3Y^2 \cdot Y' + X^2 \cdot Z' + g(X, Y, Z, T) \cdot T' + T \cdot g_1.$$

Здесь $g_1 = g_1(X, Y, Z, T; X', Y', Z', T')$ — поляризация квадратичной формы g , определяемая аналогично, и, значит, g_1 — симметрическая билинейная форма, такая, что $g_1(P; P) = 2g(P)$.

Подставляя $P_\alpha = (1, \alpha, \alpha^3, 0)$ и $Q = (0, Y, Z, T)$, получаем уравнения для $P_\alpha Q \subset S$ в виде $A = B = C = 0$, где

$$A = Z - 3\alpha^2 Y + g(1, \alpha, \alpha^3, 0) T,$$

$$B = -3\alpha Y^2 + g_1(1, \alpha, \alpha^3, 0; 0, Y, Z, T) T,$$

$$C = -Y^3 + g(0, Y, Z, T) T.$$

Шаг 4 (исключение). Исключим теперь Y, Z, T из трех предыдущих уравнений, следя за старшими степенями переменной α . Заметим, что, так как $g(0, 0, 1, 0) = 1$,

$$g(1, \alpha, \alpha^3, 0) = \alpha^6 + \dots = a^{(6)},$$

где $\dots$ обозначает члены меньшей степени по α ; таким образом, $a^{(6)}$ — нормированный многочлен шестой степени. Тогда условие $A = 0$ выражает Z как линейную форму от Y и T ,

$$Z = 3\alpha^2 Y - a^{(6)} T.$$

Подставляя это соотношение в B и пользуясь билинейностью g_1 , получаем

$$\begin{aligned} B &= -3\alpha Y^2 + g_1(1, \alpha, \alpha^3, 0; 0, Y, 3\alpha^2 Y - a^{(6)} T, T) T = \\ &= b_0 Y^2 + b_1 Y T + b_2 T^2, \end{aligned}$$

где

$$b_0 = -3\alpha, \quad b_1 = g_1(1, \alpha, \alpha^3, 0; 0, 1, 3\alpha^2, 0) = 6\alpha^5 + \dots,$$

$$b_2 = g_1(1, \alpha, \alpha^3, 0; 0, 0, -a^{(6)}, 1) = -2\alpha^9 + \dots$$

Аналогично, подставляя выражение для Z в C и разлагая квадратичную форму g , получаем

$$C = -Y^3 + g(0, Y, 3\alpha^2 Y - a^{(6)} T, T) T = c_0 Y^3 + c_1 Y^2 T + c_2 Y T^2 + c_3 T^3,$$

где

$$\begin{aligned} c_0 &= -1, \quad c_1 = g(0, 1, 3\alpha^2, 0) = 9\alpha^4 + \dots, \\ c_2 &= g_1(0, 1, 3\alpha^2, 0; 0, 0, -a^{(6)}, 1) = -6\alpha^8 + \dots, \\ c_3 &= g(0, 0, -a^{(6)}, 1) = \alpha^{12} + \dots \end{aligned}$$

Теперь в силу упр. 1.10 B и C имеют общий нуль $(\eta: \tau)$ в том и только том случае, если

$$\det \begin{bmatrix} b_0 & b_1 & b_2 & & \\ & b_0 & b_1 & b_2 & \\ & & b_0 & b_1 & b_2 \\ c_0 & c_1 & c_2 & c_3 & \\ & c_0 & c_1 & c_2 & c_3 \end{bmatrix} = 0.$$

Этот детерминант есть многочлен от α , и не трудно видеть, что его старший член получается из старших членов элементов матрицы

$$\begin{aligned} \det \begin{bmatrix} -3\alpha & 6\alpha^5 & -2\alpha^9 & & \\ & -3\alpha & 6\alpha^5 & -2\alpha^9 & \\ & & -3\alpha & 6\alpha^5 & -2\alpha^9 \\ -1 & 9\alpha^4 & -6\alpha^8 & \alpha^{12} & \\ & -1 & 9\alpha^4 & -6\alpha^8 & \alpha^{12} \end{bmatrix} = \\ = \alpha^{27} \cdot \det \begin{bmatrix} -3 & 6 & -2 & & \\ & -3 & 6 & -2 & \\ & & -3 & 6 & -2 \\ -1 & 9 & -6 & 1 & \\ & -1 & 9 & -6 & 1 \end{bmatrix} = \alpha^{27}. \end{aligned}$$

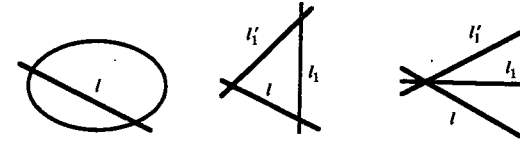
Это завершает доказательство основного утверждения.

(7.3) Предложение. Для данной прямой $l \subset S$ существует пять пар прямых (l_i, l'_i) на S , пересекающих l так, что

- (i) $l \cup l_i \cup l'_i$ лежит в одной плоскости при каждом $i = 1, \dots, 5$;
- (ii) $(l_i \cup l'_i) \cap (l_j \cup l'_j) = \emptyset$ для $i \neq j$.

Доказательство (заимствовано из [Beauville, p. 51]). Пусть Π — некоторая плоскость в $\mathbb{P}^3$, содержащая l . Тогда $\Pi \cap S = l +$ коника

(так как $f|_{\Pi}$ делится на уравнение прямой l). Эта коника может быть как особой, так и неособой:



Требуется доказать, что существует ровно пять различных плоскостей $\Pi_i \supset l$, для которых коника особая. Тогда сформулированное в п. (ii) утверждение о том, что прямые, лежащие в различных плоскостях, не пересекаются, будет вытекать из (7.1(a)).

Рассмотрим прямую $l: (Z = T = 0)$. Можно разложить f следующим образом:

$$f = AX^2 + BXY + CY^2 + DX + EY + F, \quad (*)$$

где $A, B, C, D, E, F \in k[Z, T]$, A, B и C — линейные формы, D и E — квадратичные формы, а F — кубическая форма. Если рассмотреть это уравнение как уравнение переменной коники на плоскости (X, Y) , то эта коника будет особой тогда и только тогда, когда

$$\Delta(Z, T) = 4ACF + BDE - AE^2 - B^2F - CD^2 = 0.$$

(Здесь Δ равен обычному детерминанту, умноженному на 4, если характеристика не равна 2; в характеристике 2 это утверждение является легким упражнением.)

Точнее, любая плоскость, проходящая через прямую l , задается как $\Pi: (\mu Z = \lambda T)$. Если $\mu \neq 0$, то можно считать, что $\mu = 1$, так что $Z = \lambda T$. В однородных координатах (X, Y, T) на плоскости Π получим $f|_{\Pi} = T \cdot Q(X, Y, T)$, где

$$\begin{aligned} Q &= A(\lambda, 1)X^2 + B(\lambda, 1)XY + C(\lambda, 1)Y^2 + \\ &+ D(\lambda, 1)TX + E(\lambda, 1)TY + F(\lambda, 1)T^2. \end{aligned}$$

Детерминант $\Delta(Z, T)$ является однородной квинтикой, поэтому в силу (1.8) он имеет пять нулей с учетом кратности. Чтобы доказать предложение (7.3), надо показать, что детерминант не имеет кратных корней. Это также будет следствием неособости поверхности S .

Утверждение. $\Delta(Z, T)$ имеет только простые корни.

Предположим, что $Z = 0$ — корень многочлена Δ , а $\Pi: (Z = 0)$ — соответствующая плоскость. Мне нужно доказать, что Δ не делится на Z^2 . Как следует из приведенного выше рисунка, пересечение $\Pi \cap S$ состоит из трех прямых, и, в зависимости от того, пересекаются ли они в одной точке, можно выбрать координаты так, что

либо (i) $l: (T = 0), l_1: (X = 0), l'_1: (Y = 0),$

либо (ii) $l: (T = 0), l_1: (X = 0), l'_1: (X = T).$

Следовательно, в случае (i) $f = XYT + Zg$, где g — квадратика; в обозначениях формулы (*) это означает, что $B = T + aZ$ и $Z \mid A, C, D, E, F$. Следовательно, по модулю членов, кратных Z^2 ,

$$\Delta = -T^2 F \pmod{Z^2}.$$

Кроме того, точка $P = (0, 0, 0, 1)$ принадлежит S , и неособость поверхности S в точке P означает, что член ZT^2 входит в F с ненулевым коэффициентом. В частности, F не делится на Z^2 . Поэтому $Z = 0$ — простой корень Δ .

В случае (ii) можно провести аналогичную выкладку (см. упр. 7.1).

(7.4) Следствие. (а) Существуют две непересекающиеся прямые $l, m \subset S$.

(б) поверхность S рациональна (т. е. бирационально эквивалентна $\mathbb{P}^2$; см. (5.9)).

Доказательство. (а) В силу (7.3 (ii)) можно прямо взять l_1 и l_2 .

(б) Рассмотрим две непересекающиеся прямые $l, m \subset S$ и определим рациональные отображения

$$\varphi: S \dashrightarrow l \times m \text{ и } \psi: l \times m \dashrightarrow S$$

следующим образом. Если $P \in \mathbb{P}^3 \setminus (l \cup m)$, то существует единственная прямая n , проходящая через точку P и пересекающая l и m :

$$P \in n \text{ и } l \cap n \neq \emptyset, m \cap n \neq \emptyset.$$

Пусть $\Phi(p) = (l \cap n, m \cap n) \in l \times m$. Этим определяется морфизм

$$\Phi: \mathbb{P}^3 \setminus (l \cup m) \rightarrow l \times m,$$

слой которого над $(Q, R) \in l \times m$ является прямой QR на $\mathbb{P}^3$. Определим $\varphi: S \dashrightarrow l \times m$ как ограничение отображения Φ на S .

И в обратную сторону, определим для $(Q, R) \in l \times m$ прямую $n = QR$ на $\mathbb{P}^3$. В силу предложения (7.3) существует только конечное число прямых на S , пересекающих l . Таким образом, для почти всех значений (Q, R) n пересекает S в трех точках $\{P, Q, R\}$, из которых Q и R — заданные точки на l и m . Следовательно, если задать отображение $\psi: l \times m \dashrightarrow S$ правилом $(Q, R) \mapsto P$, то ψ является рациональным отображением, так как отношение координат точки P является рациональной функцией отношений координат точек Q и R .

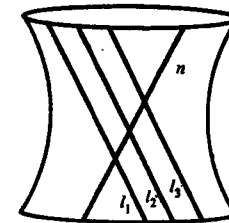
Очевидно, что φ и ψ являются взаимно обратными. Ч. т. д.

(7.5) Я хочу найти все прямые на S с помощью конфигурации из предложения (7.3), состоящей из прямой l и пяти непересекающихся пар (l_i, l'_i) . Любая другая прямая $n \subset S$ должна пересекать в точности одну прямую из пары (l_i, l'_i) для всех $i = 1, \dots, 5$. Это вытекает из того, что в $\mathbb{P}^3$ прямая n пересекает плоскость Π_i и $\Pi_i \cap S = l \cup l_i \cup l'_i$; кроме того, n не может пересекать одновременно l_i и l'_i , так как это противоречило бы (7.1(a)). Следующая лемма, утверждающая, что прямая n однозначно определяется тем, с какими из прямых l_i и l'_i она пересекается, позволяет упорядочить остальные прямые. Мы будем говорить, что прямая n инцидентна прямой l , если $l \cap n \neq \emptyset$.

Лемма. Если $l_1, \dots, l_4 \subset \mathbb{P}^3$ — непересекающиеся прямые, то либо все четыре прямые l_i лежат на гладкой квадратике, $l_1, \dots, l_4 \subset Q \subset \mathbb{P}^3$, и тогда они имеют бесконечно много общих инцидентных им прямых;

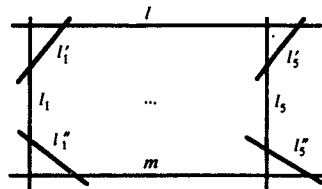
либо четыре прямые l_i не лежат ни на какой квадратике, $l_1, \dots, l_4 \not\subset Q$, и тогда они имеют одну или две общие инцидентные им прямые.

Доказательство. Имеется несколько способов доказательства (см. упр. 7.2) существования гладкой квадратки $Q \supset l_1, \dots, l_3$.



При подходящем выборе координат она имеет вид $Q: (XT - YZ)$ и содержит два семейства прямых (образующих). При этом любая прямая, инцидентная прямым $l_1, \dots, l_3$, должна лежать на квадрике Q , так как она имеет с Q три общие точки. Далее, если $l_4 \notin Q$, то $l_4 \cap Q = \{1 \text{ или } 2 \text{ точки}\}$, и образующие из другого семейства, проходящие через эти точки, являются общими инцидентными $l_1, \dots, l_4$ прямыми. Ч.т.д.

(7.6) 27 прямых. Пусть l и m — две непараллельные прямые на S . Как уже указывалось, m пересекает в точности одну прямую для каждой из пяти пар (l_i, l'_i) прямых, пересекающихся с l . Перенумеровав прямые в этих парах, будем считать, что m пересекается с $l_i, i = 1, \dots, 5$. Обозначим прямые, пересекающиеся с l или m , следующим образом:



Значит, пятью парами прямых, пересекающих m , являются $(l_i, l'_i), i = 1, \dots, 5$. Применяя к прямой m предложение (7.3(ii)), получим, что l'_i не пересекается с l_j при $i \neq j$. С другой стороны, каждая прямая на S должна пересекать одну из прямых l, l_j или l'_j . Следовательно, l'_i пересекает l'_j при $i \neq j$.

Утверждение. (I) Если $n \subset S$ — некоторая прямая, отличная от 17 рассмотренных, то n пересекает в точности три из пяти прямых $l_1, \dots, l_5$.

(II) Обратно, при любом выборе трех чисел $\{i, j, k\}$ из множества $\{1, 2, 3, 4, 5\}$ существует единственная прямая $l_{ijk} \subset S$, пересекающаяся с l_i, l_j, l_k .

Доказательство. (I) Четыре заданных непараллельных прямых на S , очевидно, не лежат все одновременно на неособой квадрике Q , так как в противном случае получалось бы, что $Q \subset S$, а это противоречит неприводимости S .

Если n пересекает не менее четырех из прямых l_i , то в силу леммы (7.5) $n = l$ или $n = m$, что противоречит условию. Если n пере-

секает не более двух из прямых l_i , то она должна пересекать не менее трех из прямых l'_i . Пусть она пересекает, скажем, или l'_2, l'_3, l'_4, l'_5 или l_1, l'_3, l'_4, l'_5 . В силу изложенного выше l и l'_1 являются общими инцидентными этим пяти непараллельным прямым l'_2, l'_3, l'_4, l'_5 и l_1 прямыми. Тем самым, опять в силу леммы (7.5), получаем, что если n пересекает не менее четырех из них, то либо $n = l$ либо $n = l'_1$, т. е. то же самое противоречие.

(II) Из предложения (7.3) вытекает, что существуют десять прямых, пересекающих l_1 , из которых до настоящего момента фигурировали только четыре (а именно l, l'_1, m и l'_1). Шесть других прямых должны пересекать в точности две из оставшихся четырех прямых $l_2, \dots, l_5$. И существует в точности $6 = \binom{4}{2}$ возможностей, каждая из которых реализуется. Ч.т.д.

Следовательно, прямые на S — это

$$\{l, m, l_i, l'_i, l_{ijk}\},$$

а их общее количество равно

$$1 + 1 + 5 + 5 + 5 + 10 = 27.$$

(7.7) Конфигурация прямых. Другой способ перечисления: на S лежат прямые $l, l_1, \dots, l_5, l'_1, \dots, l'_5$, а также 16 других прямых, пересекающих нечетное число из прямых $l_1, \dots, l_5$, а именно

l'_i пересекает только l_i ;

l_{ijk} пересекает только l_i, l_j, l_k ;

m пересекает все $l_1, \dots, l_5$.

Легко убедиться, что во введенных обозначениях отношение инцидентности между 27 прямыми на S имеет следующий вид:

l пересекает $l_1, \dots, l_5, l'_1, \dots, l'_5$;

l_1 пересекает l, m, l'_1, l'_1 и l_{1jk} для всех шести возможностей выбора $\{j, k\} \subset \{2, 3, 4, 5\}$;

l'_1 пересекает l, l_1, l'_1 (четыре возможности для $j \neq 1$)

и l_{ijk} (четыре возможности для $\{i, j, k\} \subset \{2, 3, 4, 5\}$);

l'_1 пересекает m, l_1, l'_1 (четыре возможности для $j \neq 1$)

и l_{ijk} (четыре возможности для $\{i, j, k\} \subset \{2, 3, 4, 5\}$);

l_{123} пересекает $l_1, l_2, l_3, l_{145}, l_{245}, l_{345}, l'_4, l'_5, l'_4, l'_5$.

Эта комбинаторная конфигурация имеет много различных представлений, и некоторые из них имеют гораздо более симметричный вид, чем приведенный выше (см., например, [Semple, Roth, p. 122—128 и 151—152]).

Упражнения к § 7

7.1. Докажите п. (ii) утверждения из предложения (7.3). (Указание. Так же как и в приведенном доказательстве случая (i), f имеет вид $f = X(X - T)T + Zg$. При этом коэффициенты f имеют вид $A = T + aZ$, $D = -T^2 + Zl$, где l — линейная форма, так что $Z \nmid B$, C , E , F , и Z не делится на D . Кроме того, из неособости поверхности S в точке $(0, 1, 0, 0)$ вытекает, что $C = cZ$, где $c \neq 0$. Вычислите теперь $\Delta(Z, T)$ по модулю Z^2 .)

7.2. Докажите, что для трех непересекающихся прямых $l_1, l_2, l_3 \subset \mathbb{P}^3$ существует неособая quadрика $Q \supset l_1, l_2, l_3$. (Указание. Возьмите по три точки $P_i, P'_i, P''_i = l_i$ на каждой из них и, аналогично (1.11) или (2.4), покажите, что существует по крайней мере одна quadрика Q , содержащая их. Следовательно, $l_i \subset Q$ для каждой l_i . Покажите, что Q гладкая, — разберитесь, например, что происходит, если Q — пара плоскостей.)

7.3. Гессиан. Пусть $f = f_d(x_0, \dots, x_n)$ — форма степени d от $x_0, \dots, x_n$, определяющая гиперповерхность $V: (f = 0) \subset \mathbb{P}^n$; предположим для простоты, что характеристика не равна 2 и не делит $d - 1$. Пусть $f_{x_i} = \partial f / \partial x_i$ и $f_{x_i x_j} = \partial^2 f / \partial x_i \partial x_j$ — первая и вторая производные функции f . Разложение Тейлора формы f в окрестности точки $P \in \mathbb{P}^n$ имеет вид

$$f = f(P) + f^{(1)}(x) + f^{(2)}(x) + \dots,$$

где $f^{(1)}$ и $f^{(2)}$ — линейная и квадратичная формы:

$$f^{(1)} = \sum f_{x_i}(P) \cdot x_i \text{ и } f^{(2)} = (1/2) \sum f_{x_i x_j}(P) \cdot x_i x_j.$$

Если $P \in V$ — особая точка, то $f(P)$ и $f^{(1)}$ обращаются в P в нуль, и поведение V или f в окрестности P определяется до второго порядка квадратичной формой $f^{(2)}$. Аналогично, если $P \in V$ — неособая точка, то поведение формы f , ограниченной на гиперплоскость $T_P V$ (или особое сечение гиперповерхностью $V \cap T_P V$), определяется формой $f^{(2)}$. Определим матрицу Гессе формы f (относительно координат $x_0, \dots, x_n$) формулой $H(f) = H(f, x) = \{f_{x_i x_j}\}_{ij}$ и гессиан $h(f) = h(f, x)$ как детерминант $h(f) = \det H(f)$.

(i) Пусть $x'_i = \sum a_{ij} x_j$ — проективная замена координат с невырожденной $(n+1) \times (n+1)$ -матрицей $A = (a_{ij})$. Если $g(x') = f(Ax)$, то докажите, что матрица Гессе преобразуется так:

$$H(g, x') = ({}^t A) H(f, x) A,$$

где ${}^t A$ — транспонированная матрица. Выведите отсюда, что $h(g, x') = (\det A)^2 h(f, x)$.

(ii) Рассмотрите аффинный кусок $V_{(0)} \subset \mathbb{A}_{(0)}^n$ гиперповерхности $V: (f = 0)$, как в (5.5). Пусть $P \in V_{(0)}$ — неособая точка, а $\Pi = T_P V_{(0)}$ — аффинная касательная плоскость; обозначим через φ ограничение на Π определяющего многочлена f/x_0^d для $V_{(0)}$. Проверьте, что разложение Тейлора функции φ в точке P начинается с невырожденной квадратичной формы $\varphi^{(2)}$ (от $n-1$ переменных) в том и только том случае, когда $h(f)(P) \neq 0$.

(Указание. Используя п. (i), сведите все к случаю $P = (1, 0, \dots, 0)$ и $T_P V: (x_1 = 0)$. Тогда $\varphi^{(2)}$ — это нижний правый $(n-1) \times (n-1)$ -блок проективной матрицы Гессе $H(f)$. Воспользуйтесь равенством $f_{x_i}(P) = 0$ для $i \neq 1$ и формулой Эйлера $\sum f_{x_i x_j} \cdot x_j = (d-1)f_{x_1}$, чтобы показать, что матрица $H(f)$ имеет в точности по одному ненулевому элементу в строке и столбце с номером 0.

(iii) Пусть $C: (f = 0) \subset \mathbb{P}^2$ — невырожденная плоская кубическая кривая; выведите из (iii), что $P \in C$ является точкой перегиба тогда и только тогда, когда $H(f)(P) = 0$. Из теоремы Безу следует, что $(f = H(f) = 0) \subset \mathbb{P}^2$ непусто (см. (1.9) и [Fulton, p. 112]).

(iv) Пусть $S: (f = 0) \subset \mathbb{P}^3$ — неособая кубическая поверхность. Докажите, что если $P \in S$ не принадлежит ни одной прямой, лежащей в S , то пересечение $S \cap T_P S$ является каспидальной кубикой тогда и только тогда, когда $H(f)(P) = 0$. Выведите отсюда существование сечений, имеющих вид каспидальных кубик, как требуется на шаге 1 доказательства предложения (7.2).

7.4. (i) Докажите, что если $P \in S$ — особая точка кубической поверхности, то существует по крайней мере одна прямая $l \subset S$, проходящая через P («в общем положении» таких прямых 6).

(ii) Если $X \subset \mathbb{P}^4$ — неособая кубическая гиперповерхность (трехмерная кубика) и $P \in X$, то существует по крайней мере одна прямая $l \subset X$, проходящая через точку P («в общем положении» 6). (Указание. Выпишите уравнение для X в координатах, в которых $P = (1, 0, \dots, 0)$.)

7.5. Покажите, что рациональное отображение $\varphi: S \rightarrow l \times t$ из следствия (7.4 (b)) в действительности является морфизмом. Покажите, что оно стягивает в точки пять прямых на S .

7.6. Найдите 27 прямых на диагональной кубической поверхности (поверхности Ферма)

$$S: (X^3 + Y^3 + Z^3 + T^3 = 0) \subset \mathbb{P}^3$$

с помощью плоскостей вида $(X = qY)$, где $q^3 = 1$.

7.7. Пусть $S \subset \mathbb{P}^3$ — кубическая поверхность, заданная уравнением $S: (f = 0)$, где

$$f(X, Y, Z, T) = ZX^2 + TY^2 + (Z - d^2 T)(Z - e^2 T)(Z - f^2 T),$$

а d, e, f — различные ненулевые элементы поля k , $l \subset S$ — прямая, заданная уравнением $Z = T = 0$. Рассматривая, как и в предложении (7.3), переменную плоскость, содержащую прямую l , получите уравнения 10 прямых на S , пересекающихся с l .

7.8 (предложено Р. Касдагли). Рассмотрим кубическую поверхность $S_{(0)} \subset \mathbb{R}^3$, заданную в аффинных координатах уравнением

$$x^2 + y^2 + z^2 - 2xyz = 1 + \lambda^2, \quad (*)$$

где $\lambda \in \mathbb{R}$, $\lambda > 0$, — константа. (i) Переписывая (*) в виде

$$(x - yz)^2 = (y^2 - 1)(z^2 - 1) + \lambda^2,$$

получаем, что $S_{(0)}$ имеет 4 полы, уходящих в бесконечность. С другой стороны, соответствующая проективная поверхность $S \subset \mathbb{P}_{\mathbb{R}}^3$ пересекает бесконечность по трем прямым $XYZ = 0$. Используйте это, чтобы описать топологию поверхности S .

(ii) Рассматривая (*) как уравнение переменной коники в (x, y) -плоскости с параметром z , покажите, что четыре пары прямых, лежащие в $S_{(0)}$, которые пересекают $(Z = 0)$ на бесконечности, задаются уравнениями $z = \mu$, $x = (\mu \pm \lambda)y$; $z = -\mu$, $x = (-\mu \pm \lambda)y$; $z = 1$, $x - y = \pm \lambda$; $z = -1$, $x + y = \pm \lambda$, где $\mu^2 = 1 + \lambda^2$. Изобразите поверхность $S_{(0)}$ в $\mathbb{R}^3$ и ее 24 прямые на дисплее компьютера либо смастерите ее гипсовую модель.

7.9. Случай, когда все прямые рациональны. Предположим, что $\text{char } k \neq 2$, и пусть $S: (f = 0)$ — неособая кубическая поверхность, где

$$f = A(X, Y) \cdot T - B(X, Y) \cdot Z + (\text{члены степени } \geq 2 \text{ от } Z \text{ и } T).$$

Тогда $S: (f = 0)$ содержит $l: (Z = T = 0)$ и касательная плоскость в точке $P = (1, \lambda, 0, 0)$ — это $T_P S: A(1, \lambda)T = B(1, \lambda)Z$.

(i) Используйте линейные замены координат в плоскостях (X, Y) и в (Z, T) , чтобы привести A, B к $A = X^2 + \Delta Y^2, B = XY$ (где $\Delta \in k$), а если Δ — полный квадрат, то к $A = X^2, B = Y^2$.

(ii) Предположим, что S также содержит прямую $m: (X = Y = 0)$ и для упрощения обозначений что $A = X^2, B = Y^2$. Пусть $l_i, i = 1, \dots, 5$, — пять общих неинцидентных l и m прямых, и обозначим через $P_i = (1, \lambda_i, 0, 0) = l_i \cap l$ точки пересечения l и l_i . Докажите, что

$$l_i: (Y = \lambda_i X, T = \lambda_i^2 Z) \text{ при } i = 1, \dots, 5$$

и что

$$f = X^2 T - Y^2 Z + X(\sigma_5 Z^2 + \sigma_3 ZT + \sigma_1 T^2) - Y(\sigma_4 Z^2 + \sigma_2 ZT + T^2),$$

где $\sigma_1, \dots, \sigma_5$ — элементарные симметрические функции от $\lambda_1, \dots, \lambda_5$.

(iii) Найдите остальные прямые на S . (Указание. l_i и l_i^* содержатся в плоскостях, которые вы уже знаете. Рассуждая, как в (7.6), нетрудно показать, что каждая прямая, пересекающая все три прямые l_1, l_2, l_3 , задается условием $(\tau_2 Z + T): X = (\tau_3 Z + \tau_1 T): Y = \alpha: \beta$ для некоторого $\alpha: \beta \in \mathbb{P}^1$, где $\tau_1, \dots, \tau_3$ — элементарные симметрические функции от $\lambda_1, \dots, \lambda_3$).

7.10. Это упражнение для тех, кто любит длинные вычисления или имеет доступ к программам компьютерной алгебры. Если неособая кубическая поверхность S содержит в качестве сечения нодальную кубическую кривую C , ее уравнение можно записать в виде

$$f = XYZ - X^3 - Y^3 + Tg.$$

Пусть $P_\alpha = (\alpha, \alpha^2, 1 + \alpha^3, 0)$, где $\alpha \neq 0, \infty$ — переменная точка кривой C и $Q = (0, Y, Z, T)$. Тогда, представляя $f(\lambda P_\alpha + \mu Q)$ через поляризацию многочлена f , как в шаге 3 доказательства предложения (7.2), покажем, что прямая $P_\alpha Q$ лежит в S тогда и только тогда, когда $A = B = C = 0$, где

$$\begin{aligned} A &= (-2\alpha^4 + \alpha)Y + \alpha^3 Z + g(\alpha, \alpha^2, 1 + \alpha^3, 0)T, \\ B &= \alpha YZ - 3\alpha^2 Y^2 + g_1(\alpha, \alpha^2, 1 + \alpha^3, 0; 0, Y, Z, T)T, \\ C &= -Y^3 + g(0, Y, Z, T)T. \end{aligned}$$

Докажите, что существуют нормированный «результант»-многочлен $R_{27}(\alpha)$ от α степени 27 со свободным членом 1, такой, что

$$R(\alpha) = 0 \Leftrightarrow A = B = C = 0 \text{ имеют общий нуль } (\eta: \xi: \tau) \text{ в } \mathbb{P}^2.$$

(Указание. Разрешая $A = 0$ относительно Z (и получив при этом α^3 в знаменателе), подставляем выражение для Z в B и C , чтобы получить бинарные квадрат и куб от Y и Z . Затем, используя детерминант Сильвестра, исключаем Y и Z . Трудность этого случая состоит в том, что детерминант из старших членов обращается в нуль. Это происходит из-за того, что A, B, C имеют тривиальный общий нуль $Q = P_\alpha = (0, 0, 1, 0)$, когда $\alpha = 0$ или ∞ . А rg детерминант имеет члены $\alpha^{18}, \dots, \alpha^{-15}$ и нужно вычислить четыре первых и четыре последних коэффициента, чтобы доказать, что на самом деле он имеет вид $-1\alpha^{15} + \dots - 1\alpha^{-12}$.)

§ 8. Заключительные комментарии

Студент не обязан готовить этот заключительный параграф к экзамену, но тем не менее отдельные места могут представлять для него интерес.

История и социологический аспект современной алгебраической геометрии

(8.1) Введение. Алгебраическая геометрия за последние 30 лет заняла в математике приблизительно такое же положение, какое занимает сама математика в окружающем мире. Ее уважают и боятся куда больше, чем понимают. В то же время те «практические» вопросы, которые мне задают английские коллеги или старшекурсники Уорикского университета, обычно настолько элементарны, что покрываются либо этой книжкой, либо книгой [Атья, Макдональд]. Дальнейшее описание современного развития предмета — всего лишь попытка объяснить этот парадокс. При этом я никак не претендую на объективность.

(8.2) Предыстория. Алгебраическую геометрию в XIX в. питали несколько разных источников. Прежде всего это — собственно геометрическая традиция, т. е. проективная геометрия (и начертательная геометрия, представлявшая во времена Наполеона большой интерес для военных), изучение кривых и поверхностей как таковых, геометрия конфигураций. Затем это — теория функций комплексного переменного, представление о компактной римановой поверхности как об алгебраической кривой и ее чисто алгебраическое построение через поле функций. Над всем этим — глубокая аналогия между алгебраическими кривыми и кольцом целых чисел числового поля, а также потребность в алгебраическом и геометрическом языке для теории инвариантов, сыгравшей важную роль в развитии абстрактной алгебры в начале XX столетия.

Первые десятилетия XX в. ознаменовались глубоким расколом. С одной стороны, геометрическая традиция изучения кривых и поверхностей плодотворно развивалась работами блистательной итальянской школы (наряду со своими собственными вполне впечатляющими достижениями она сыграла значительную роль в развитии топологии и дифференциальной геометрии), однако доказательства все более настойчиво апеллировали к «геометрической интуиции», и даже *Maestri* не были в состоянии проводить рассуждения на должном уровне строгости. С другой стороны, недавно сформировавшиеся полки коммутативной алгебры заклады-

вали фундамент и новую технику доказательств. Примером различия между этими двумя подходами является спор между Чжоу и ван дер Варденом, с одной стороны (им удалось доказать существование алгебраического многообразия, параметризующего пространство кривых заданного рода и степени), и Севери, с другой стороны, который всю свою жизнь творчески использовал такие пространства и в преклонных годах горько сетовал на вторжение алгебраистов (да еще и не итальянцев!) в свою область. Особенно его задевали неявные намеки на то, что работам его собственной школы не хватает строгости.

(8.3) Строгость, первая волна. Вслед за введением абстрактной алгебры Гильбертом и Эмми Нётер строгие основания алгебраической геометрии были заложены в 20-е и 30-е годы ван дер Варденом, Зарисским и Вейлем (обычно заслуги ван дер Вардена замалчивают, по-видимому, из-за того, что большое число математиков послевоенной поры, включая некоторых ведущих алгебраических геометров, считало его коллаборационистом).

Центральной задачей их программы было построение алгебраической геометрии над любым полем. Ключевая трудность здесь заключается в том, что многообразие нельзя определить просто как множество точек. А именно, когда вы начинаете с рассмотрения многообразия $V \subset \mathbb{A}_k^n$ над заданным полем k , то оно является не просто подмножеством в k^n . Вам придется также рассмотреть все K -значные точки многообразия V , где $k \subset K$ — расширение полей (см. обсуждения в (8.13 (с))). Это одна из причин использования символа $\mathbb{A}_k^n$ для обозначения k -значных точек многообразия $\mathbb{A}^n$, которое хотелось бы считать существующим независимо от конкретного поля k .

Необходимость смены основного поля в ходе рассуждений сильно увеличивает технические и концептуальные трудности (не говоря уж об обозначениях). Тем не менее около 1950 г. вейлевская система оснований геометрии вошла в употребление настолько, что традиционные геометры (например Ходж и Пидо) были вынуждены использовать ее в своих книгах, что существенно затруднило (по моему мнению) восприятие этих книг.

(8.4) Эра Гротендика. В период примерно между 1955 и 1970 гг. в алгебраической геометрии господствовали парижские математики, вначале Серр, а затем главным образом Гротендик и его школа. Важно не впасть в недооценку влияния подхода Гротендика, особенно теперь, когда он уже до некоторой степени вышел из моды. Это

был период, когда были сделаны огромные идейные и технические продвижения, и благодаря систематическому использованию понятия схемы (более общего, чем многообразие, см. (8.12)–(8.14) ниже) алгебраическая геометрия получила возможность впитать в себя практически все достижения топологии, гомологической алгебры, теории чисел и т. д. и даже сыграть важную роль в их развитии. Сам Гротендик удалился со сцены около 1970 г., когда ему было едва за сорок, что следует расценивать как трагическую утрату (все началось с того, что он покинул Институт высших исследований (IHES), протестуя против финансирования науки военными.) Любопытный алгебраический геометр хорошо знаком с большими фрагментами созданной в тот период мощной техники, многие из которых еще нуждаются в доступном изложении.

С другой стороны, культ личности Гротендика имел серьезные побочные эффекты. А именно, многие математики, посвятившие большую часть своей жизни освоению вейлевских оснований, были вытеснены из алгебраической геометрии или подверглись насмешкам. Насколько мне известно, лишь один или два из них сумели адаптироваться к новому языку. Кроме того, целое поколение студентов (преимущественно французских) пребывало в глупой уверенности, что если задачу нельзя облачить в рафинированный абстрактный формализм, то ею не стоит заниматься, и тем самым лишили себя естественного для математика пути развития, когда он начинает с маленьких задач, которые ему по силам, и, опираясь на них, развивает свою деятельность. (Я знаю реальный случай, когда диссертация по арифметике кубических поверхностей вначале не была принята, поскольку «естественно строить конструкцию над общими локально нётеровыми окольцованными топосами». Это не шутка.) Многие из тогдашних студентов не представляли себе более достойного занятия, чем «*étudier les EGAs*». Начало изучения теории категорий как таковой (являющееся, согласитесь, одним из наиболее бесплодных интеллектуальных занятий) также относится к этому периоду. Впрочем, не следует сваливать всю вину на Гротендика, так как сам он применял теорию категорий к решению задач вполне успешно.

С той поры мода переменилась. На недавней конференции во Франции я, комментируя изменение ситуации, получил в ответ саркастическое замечание: «Однако скрученная кубика является прекрасным примером про-представимого функтора». Я понимаю, что некоторые из математиков, имеющие в настоящее время отношение к финансированию науки, пострадали в тот период интеллектуального терроризма, и в результате заявки для создания научных про-

ектов составляются так, чтобы максимально уменьшить их связь с алгебраической геометрией.

Помимо очень небольшого числа его собственных студентов, которым удалось выдержать гонку и выжить, люди, которые извлекли наибольшую пользу из идей Гротендика и развивали их наиболее успешно, испытывали его влияние на расстоянии. К ним относятся гарвардская школа (через Зарисского, Мамфорда и М. Артина), московская школа Шафаревича и, может быть, также японская школа коммутативных алгебраистов.

(8.5) Большой взрыв. История не закончилась в начале 70-х гг., и алгебраическая геометрия не стала с той поры менее подверженной колебаниям моды. В 70-е гг., хотя ряд крупных школ имел свои собственные специальные интересы (Мамфорд и компактификация пространства модулей, гриффитсовские школы теории Ходжа и алгебраических кривых, Делинь и «веса» в когомологиях многообразий, Шафаревич и $K3$ -поверхности, Иитака с последователями и классификация многомерных многообразий и т. д.), мне казалось, что все мы в основном верили, что занимаемся одним предметом и что алгебраическая геометрия остается монолитным зданием (и в действительности завоевывает смежные территории). Может быть, это объяснялось наличием одного или двух специалистов, владеющих всем кругом вопросов.

В середине 80-х гг. ситуация изменилась, и в настоящее время кажется, что алгебраическая геометрия распалась на дюжину или более школ, которые друг с другом мало взаимодействуют: кривые и абелевы многообразия, алгебраические поверхности и теория Дональдсона, трехмерные многообразия и классификация в высших размерностях, K -теория и алгебраические циклы, теория пересечений и исчислительная геометрия, обобщенные теории когомологий, теория Ходжа, характеристика p , арифметическая алгебраическая геометрия, теория особенностей, уравнения математической физики, теория струн, применения компьютерной алгебры и т. д.

Дополнительные замечания и «высоконаучные» комментарии

В этом параграфе перемешаны элементарные и сложные темы. Так как он отчасти является напутствием для университетских преподавателей, использующих эту книгу как учебник, а также должен привлечь заинтересованных студентов в дебри алгебраической геометрии, то какая-то часть материала может показаться трудной.

(8.6) Выбор тем. Темы и примеры, рассмотренные в этой книге, частично подбирались из прагматических соображений, чтобы степени были поменьше, а вычисления попроще, а также чтобы дать представление о «классификации многообразий». Так, материал о кониках применим до известной степени к любой рациональной кривой, а кубические поверхности являются наиболее важными примерами рациональных поверхностей дель Пеццо. Кубические кривые с групповым законом являются примерами абелевых многообразий. Утверждение в разд. (2.2) о том, что неособая кубика не является рациональной кривой — это самый первый шаг классификации. Пересечение двух плоских коник в разд. (1.12)—(1.14) и пересечение двух квадрик в $\mathbb{P}_k^3$, используемое в упр. 5.6, также укладываются в похожую схему, причем пересечение двух квадрик в $\mathbb{P}_k^4$ задает другой класс поверхностей дель Пеццо, а семейство прямых на пересечении двух квадрик в $\mathbb{P}_k^5$ является двумерным абелевым многообразием.

Род кривой и деление на 3 класса, приведенные в таблице на с. 50—51, являются эскизом классификации многообразий. Мне хотелось бы включить побольше материала о роде кривой, в частности, как его вычислять через топологическую эйлерову характеристику или через индекс пересечений в алгебраической геометрии. Это — важные упражнения для молодых геометров. Однако этот материал вполне составил бы отдельный лекционный курс для начинающих, так же как и комплексно-аналитическая теория эллиптических кривых.

(8.7) Вычисления и теория. Другим обстоятельством, на которое следует обратить внимание, является то, что в этой книге основной упор делается на случаи, которые можно разобрать с помощью явных вычислений. Когда из общей теории вытекает существование некоторой конструкции, то получение для нее явных координатных выражений является полезным упражнением, позволяющим сохранить ощущение реальности, что вполне уместно для начального курса. Однако это не должно скрывать тот факт, что в действительности теория предназначена для изучения трудных случаев, когда выписывание явных формул, как правило, ничего не дает.

(8.8) $\mathbb{R}$ и $\mathbb{C}$. Читатель, которого интересует вещественный случай, возможно, будет разочарован тем, что после рассмотрений над $\mathbb{R}$ в § 1—2 мы переходим в § 3 к рассмотрению над произвольным полем k , которое сразу же предполагается алгебраически замкну-

тым. Я рекомендую таким читателям проявить настойчивость, так как имеется много взаимосвязей между вещественной и комплексной геометрией и некоторые из них весьма удивительны. Вопрос о вещественных точках вещественного многообразия является очень трудным и в основном представляет большой интерес для немногих специалистов по вещественной алгебраической геометрии. В любом случае получение всей информации о множестве комплексных точек, как правило, является важной подготовительной частью. Другой очевидной взаимосвязью геометрии над $\mathbb{R}$ и $\mathbb{C}$ является то, что n -мерное неособое комплексное многообразие является $2n$ -мерным вещественным дифференцируемым многообразием. Например, алгебраические поверхности — это главный источник построения гладких четырехмерных многообразий.

Наряду с этими довольно очевидными связями имеется ряд не столь очевидных: (а) из особенностей плоских кривых $C \subset \mathbb{C}^2$ при пересечении с границей маленького шара возникают узлы в S^3 и (б) в конструкции твисторов Пенроуза четырехмерное многообразие (с римановой метрикой специального типа) рассматривается как множество вещественных точек четырехмерного комплексного многообразия, параметризующего рациональные кривые на комплексном трехмерном многообразии (так, вещественная четырехмерная сфера S^4 , на которой мы существуем, отождествляется с совокупностью вещественных точек комплексного грассманиана $\text{Gr}(2, 4)$ прямых в $\mathbb{P}^3_{\mathbb{C}}$).

(8.9) Регулярные функции и пучки. Читатель, который правильно усвоил понятие рациональной функции $f \in k(X)$ на многообразии X и понятие регулярности функции f в точке $P \in X$ (разд. (4.7) и (5.4)), уже имеет достаточно хорошее интуитивное представление о пучке $\mathcal{O}_X$. Для каждого открытого подмножества $U \subset X$ множество всех регулярных функций $U \rightarrow k$

$$\mathcal{O}_X(U) = \{f \in k(X) \mid f \text{ регулярна во всех точках } P \in U\} = \bigcap_{P \in U} \mathcal{O}_{X,P}$$

является подкольцом в поле $k(X)$. Пучок $\mathcal{O}_X$ есть просто семейство колец $\mathcal{O}_X(U)$, где U пробегает все открытые подмножества в X . Очевидно, что любой элемент локального кольца $\mathcal{O}_{X,P}$ (см. определения в разд. (4.7) и (5.4)) является регулярным в некоторой окрестности U точки P , так что $\mathcal{O}_{X,P} = \bigcap_{P \in U} \mathcal{O}_X(U)$. Вот и все: имеется фиксированная совокупность рациональных сечений, и сечения пуч-

ка над открытым множеством U просто являются рациональными сечениями, регулярными во всех точках $P \in U$.

Этот язык адекватно описывает любой пучок без кручения на неприводимом многообразии с топологией Зарисского. Конечно, если многообразие X приводимо или если вы захотите работать с более сложными пучками либо воспользоваться комплексной топологией, то потребуется настоящее определение пучков.

(8.10) Глобально определенные регулярные функции. Если X — проективное многообразие, то единственными рациональными функциями $f \in k(X)$, которые регулярны во всех точках $P \in X$, являются константы. Это общее свойство проективных многообразий, аналогичное теореме Лиувилля для функций одного комплексного переменного. Для многообразий над $\mathbb{C}$ оно вытекает из компактности и принципа максимума (многообразие $X \subset \mathbb{P}^n_{\mathbb{C}}$ компактно в комплексной топологии, поэтому модуль глобально голоморфной функции на X должен достигать максимума), но непосредственное доказательство в алгебраической геометрии оказывается на удивление трудным (см., например, [Хартсхорн I. 3. 4]). Постоянство регулярной функции на проективном многообразии в действительности — теорема конечности, связанная с конечномерностью когомологий когерентных пучков).

(8.11) Удивительная универсальность проективной алгебраической геометрии. В разд. (0.4) кратко упоминалось о вейлевском определении абстрактного многообразия (аффинные алгебраические множества склеиваются по изоморфным открытым подмножествам). С ним легко работать в терминах пучков. Если исходить из этого, то желание работать с многообразиями, вложенными в фиксированное пространство $\mathbb{P}^N_k$, может показаться с первого взгляда слишком ограничительным. Я хочу кратко изложить современную точку зрения на это обстоятельство.

(а) Поляризация и положительность. Прежде всего многообразия, как правило, рассматриваются с точностью до изоморфизма, т. е. говоря, что многообразие X проективно, мы подразумеваем, что X может быть вложено в некоторое $\mathbb{P}^N$, т. е. изоморфно замкнутому подмногообразию $X \subset \mathbb{P}^N$, как в (5.1)–(5.7). *Квазипроективность* означает изоморфизм с локально замкнутым подмногообразием в $\mathbb{P}^N$, т. е. с открытым плотным подмножеством проективного многообразия. Проективность включает в себя свойство *полноты*, т. е. X не может быть вложено в качестве открытого плотного множества ни в какое большее многообразие.

Собственно выбор настоящего вложения $X \hookrightarrow \mathbb{P}^N$ (или очень обильного расслоения $\mathcal{O}_X(1)$, сечения которого будут однородными координатами в $\mathbb{P}^N$) часто называют *поляризацией* и пишут $(X, \mathcal{O}_X(1))$ для указания того, что этот выбор сделан. Кроме условия полноты проективные многообразия $X \subset \mathbb{P}^N$ удовлетворяют условию «положительности степени». А именно, если $V \subset X$ есть k -мерное многообразие, то V пересекается с общим линейным подпространством $\mathbb{P}^{N-k}$ в положительном конечном числе точек. И наоборот, критерий Клеймана утверждает, что некоторая степень линейного расслоения на полном многообразии X может задать проективное вложение многообразия X , если его степень на каждой кривой $C \subset X$ непременно больше нуля (т. е. $\geq \varepsilon \cdot$ (любая разумная мера кривой C)). Положительность такого типа тесно связана с выбором келеровой метрики на комплексном многообразии (римановой метрики с правильным условием согласования с комплексной структурой). Поэтому мы понимаем проективность как условие типа «положительной определенности».

(b) **Универсальность.** Удивительным обстоятельством является то, что многие проблемы алгебраической геометрии решаются в рамках проективных многообразий. Конструкция многообразий Чжоу, упоминавшаяся в разд. (8.2), является одним из таких примеров. Другим служит работа Мамфорда 60-х гг., в которой он построил многообразия Пикара и многие пространства модулей как квазипроjektивные многообразия (схемы). Теория Мори (благодаря которой были достигнуты важные принципиальные продвижения в классификации многообразий, имеющих отношение к рациональности, см. [Kollár]) является наиболее свежим примером. Ее идеи и техника являются по сути своей проективными.

(c) **Узость абстрактных многообразий.** Кривые и неособые поверхности автоматически являются квазипроjektивными. Но существуют абстрактные многообразия, не являющиеся квазипроjektивными (особые поверхности или неособые многообразия размерности ≥ 3). Однако если вам потребуются эти конструкции, то почти наверняка захочется также рассмотреть многообразия Мойшезона (алгебраические пространства М. Артина), которые являются объектами алгебраической геометрии, более общими, чем абстрактные многообразия; они получаются при более свободной трактовке «склеивания локальных кусков».

Теоремы об абстрактных многообразиях часто доказываются сведением к квазипроjektивному случаю. Так что будут ли доказательства в терминах квазипроjektивных многообразий или подробности процесса редукции к квазипроjektивному случаю полезными,

важными и интересными или окажутся только средством легко получить пригодную для публикации работу, зависит от конкретной задачи, индивидуальных интересов и потребностей студента. Недавно было доказано, что неквазипроjektивное неособое абстрактное многообразие, или многообразие Мойшезона, обязательно содержит рациональную кривую. Однако доказательство (принадлежащее Дж. Коллару) проведено с помощью теории Мори и является «махровой» проективной алгебраической геометрией.

(8.12) **Аффинные многообразия и схемы.** Координатное кольцо $k[V]$ аффинного многообразия V над алгебраически замкнутым полем k (определение (4.1)) удовлетворяет двум условиям:

- (i) оно является конечно порожденной k -алгеброй;
- (ii) оно является областью целостности.

Кольцо, удовлетворяющее этим двум условиям, очевидно, имеет вид $k[V]$ для некоторого многообразия V и называется *геометрическим кольцом* (или *геометрической k -алгеброй*).

В гл. 2 содержатся два ключевых теоретических результата. Одним из них является теорема (4.4), утверждающая в точности, что отображение $V \mapsto k[V] = A$ есть эквивалентность между категорией аффинных алгебраических многообразий и категорией, двойственной к категории геометрических k -алгебр (хотя я вымарал все упоминания о категориях как непригодные для юных читателей). Другим является Nullstellensatz (3.10), утверждающая, что простые идеалы в $k[V]$ находятся в биективном соответствии с неприводимыми подмногообразиями в V . Точки многообразия V соответствуют максимальным идеалам.

Эти результаты в совокупности отождествляют аффинные многообразия V с аффинными схемами геометрических колец (ср. также с определением (4.6)).

Простой спектр $\text{Spec } A$ определен для произвольного кольца (коммутативного и с единицей) и является множеством всех простых идеалов кольца A . Он снабжен топологией Зарисского и структурным пучком. Это и есть *аффинная схема*, соответствующая кольцу A (см. детали в [Mumford, Introduction] или [Хартсхорн, гл. II]). Имеется несколько различных причин, вследствие которых аффинные схемы являются более общим понятием, чем аффинные многообразия. Каждая из них важна, и мы кратко остановимся на них в разд. (8.14).

Важно понимать, что для геометрического кольца $A = k[V]$ простой спектр $\text{Spec } A$ содержит в точности ту же информацию, что и многообразие A , и ни граммом больше. Nullstellensatz обеспечи-

вает нас большим запасом максимальных идеалов (m_v для всех точек $v \in V$), а любой другой простой идеал $P \subset A$ является пересечением максимальных идеалов по всем точкам неприводимого подмногообразия $Y \subset V$:

$$P = I(Y) = \bigcap_{v \in Y} m_v.$$

Полезно и (по крайней мере, грубо говоря) допустимо игнорировать различие между многообразиями и схемами и писать $V = \text{Spec } A$, v вместо m_v и представлять себе простой идеал $P = I(Y)$ («общую точку») как своего рода метку для прачечной, пришитую всюду плотно на материи подмногообразия Y .

(8.13) Что такое точка? Большинству студентов никогда не понадобится никаких сведений о схемах, выходящих за пределы материала из разд. (8.9) и (8.12). Следует только помнить, что понятие «общая точка» используется в различных технических смыслах и часто означает нечто совсем иное, чем выражение «достаточно общая точка».

Этот раздел предназначен для читателя, перед которым стоит проблема чтения современной литературы; здесь даются некоторые пояснения к различным понятиям точки в теории схем, что, вероятно, является одним из основных камней преткновения для начинающих.

(а) Теоретико-схемные точки многообразия. Предположим, что k — поле (не обязательно алгебраически замкнутое), $I \subset k[X_1, \dots, X_n]$ — идеал и $A = k[X_1, \dots, X_n]/I$. Положим $V = V(I) \subset K^n$, где $k \subset K$ — выбранное алгебраическое замыкание. Точки из $\text{Spec } A$ ненамного сложнее, чем в случае геометрического кольца из разд. (8.12). Согласно очевидному усилению Nullstellensatz, максимальный идеал в A определяется точкой $v = (a_1, \dots, a_n) \in V \subset K^n$, т. е. имеет вид

$$m_v = \{f \in A \mid f(P) = 0\} = (x_1 - a_1, \dots, x_n - a_n) \cap A.$$

Легко показать, что различные точки $v \in V \subset K^n$ соответствуют одному и тому же максимальному идеалу m_v в кольце A тогда и только тогда, когда они сопряжены над k в смысле теории Галуа (так как A состоит из многочленов с коэффициентами из k). Таким образом, максимальным спектром $\text{Spec } A$ является многообразие V «с точностью до сопряжения» (т. е. факторпространство по действию группы $\text{Gal } K/k$ на V). Каждый простой идеал P в A соответствует,

как в разд. (8.12), неприводимому подмногообразию $Y = V(P) \subset V$ (с точностью до сопряжения над k). Идеал $P \in \text{Spec } A$ называется теоретико-схемной *общей точкой* многообразия Y и к нему по-прежнему можно относиться как к метке на Y . Топология Зарисского на $\text{Spec } A$ организуется таким образом, что P всюду плотна в Y . Максимальные идеалы в A называются для отличия *замкнутыми точками*. Если $C: (f = 0) \subset \mathbb{A}_C^2$ — неприводимая кривая, то у нее имеется ровно одна теоретико-схемная общая точка, соответствующая идеалу (0) в $C[X, Y]/(f)$, в то время как у поверхности S наряду с собственной общей точкой, плотной в S , имеется по одной общей точке для каждой неприводимой кривой $C \subset S$.

Теоретико-схемные точки важны при определении $\text{Spec } A$ как множества с топологией и пучком колец (а также в коммутативной алгебре и при изучении в алгебраической геометрии таких понятий, как окрестность общей точки неприводимого подмногообразия; см. п. (i) разд. 8.14). Однако точки многообразия $V \subset K^n$ со значениями в алгебраическом замыкании $k \subset K$ больше соответствуют геометрическому представлению о точке и называются *геометрическими точками*. Это напоминает ситуацию с топологией Зарисского многообразия V , которая служит скорее «сферой обитания» структурного пучка $\mathcal{O}_V$, чем полноправным геометрическим объектом.

(б) Точки со значениями в поле в теории схем. Если P — простой идеал кольца A (а значит, $P \in \text{Spec } A$ — точка), то поле вычетов в точке P является полем частных области целостности A/P и обозначается через $k(P)$. Оно является алгебраическим расширением основного поля k тогда и только тогда, когда идеал P максимален. Точка многообразия V с коэффициентами из расширения $k \subset L$ (точка $(a_1, \dots, a_n) \in V(I) \subset L^n$), очевидно, соответствует гомоморфизму $A \rightarrow L$ (заданному формулой $X_i \mapsto a_i$), ядром которого является простой идеал P в A , или, что эквивалентно, вложению $k(P) \hookrightarrow A$. Если $P = m_v$ — максимальный идеал и $L = K$ — алгебраическое замыкание поля k , то именно выбор вложения $A/m_v = k(v) \hookrightarrow K$ определяет координаты соответствующей точки многообразия $V \subset K^n$, или, другими словами, выделяет эту точку из набора сопряженных по Галуа. Это — геометрические точки многообразия V .

Для любого расширения $k \subset L$ гомоморфизм k -алгебр $A \rightarrow L$, соответствующий L -значной точке многообразия V , можно приукрасить так, чтобы он выглядел более оправданным. Напомним прежде всего, что многообразие — это больше, чем множество точек. Даже если оно состоит из одной единственной точки, необходимо

указать, над каким полем оно определено. Так,

$$\text{Spec } L = \frac{L}{\cdot} = \text{pt}_L$$

является многообразием, состоящим из единственной точки, определенной над L . В силу эквивалентности категорий (4.4) морфизм $\text{Spec } L \rightarrow V$ (включение точки, определенной над L) должен быть гомоморфизмом k -алгебр $A = k[V] \rightarrow L = k[\text{pt}_L]$.

Подводя итог связи между теоретико-схемными точками и точками со значениями в поле, можно сказать, что точка $P \in \text{Spec } A = V$ является простым идеалом кольца A и тем самым соответствует гомоморфизму факторизации $A \rightarrow A/P \subset \text{Quot}(A/P) = k(P)$ в поле. Если L — произвольное поле, то L -значная точка в V — это гомоморфизм $A \rightarrow L$. Теоретико-схемная точка P соответствует тавтологическим образом точке со значениями в поле, но это поле $k(P)$ меняется от точки к точке. Если K — алгебраическое замыкание поля k , то K -значные точки многообразия $V \subset K^n$ являются в точности геометрическими точками; K -значная точка v «сидит» в замкнутой теоретико-схемной точке m_v и имеет заданное включение $A/m_v = k(v) \hookrightarrow K$.

(с) Общие точки в основаниях Вейля. В разд. (8.3) упоминалось об особых свойствах точек в основаниях Вейля. А именно, многообразию V , определенному над полем k , разрешается иметь L -значные точки для любого расширения $k \subset L$. Это свойство, очевидно, проистекает из теории чисел, но имеет следствия также и в геометрии. Например, если C — окружность $x^2 + y^2 = 1$, определенная над полем $k = \mathbb{Q}$, то точка

$$P_\pi = (2\pi/(\pi^2 + 1), (\pi^2 - 1)/(\pi^2 + 1))$$

является $\mathbb{C}$ -значной точкой C . Так как π трансцендентно над $\mathbb{Q}$, то любой многочлен $f \in \mathbb{Q}[x, y]$, обращающийся в нуль в точке P_π , кратен $x^2 + y^2 - 1$. Таким образом, P_π является $\mathbb{Q}$ -общей точкой кривой C , т. е. она не лежит ни в каком меньшем подмногообразии в C , определенном над $\mathbb{Q}$. Другими словами, сопряженные к P_π относительно действия группы $\text{Aut } \mathbb{C} (= \langle \text{Gal}(\mathbb{C}/\mathbb{Q}) \rangle)$ точки плотны в C . Так как P_π — это $\mathbb{Q}$ -общая точка, то, если о точке P_π доказывалось утверждение, в котором используются только рациональные многочлены, то это утверждение будет справедливо и для всех точек кривой C .

В действительности это уже учитывается понятием L -значной точки, описанным в п. (b), и геометрический смысл общих точек наиболее ясно может быть выражен на этом языке. Например, поле

$\mathbb{Q}(\pi)$ просто является чисто трансцендентным расширением, так что $\mathbb{Q}(\pi) \cong \mathbb{Q}(\lambda)$, и морфизм $\text{Spec } \mathbb{Q}(\lambda) \rightarrow C$ — рациональная параметризация кривой C , обсуждавшаяся в разд. (1.1). Грубо говоря, разрешается вместо трансцендентного или неизвестного π подставлять любые «достаточно общие» значения. Вообще, конечно порожденное расширение $k \subset L$ является полем функций многообразия W над k . Предположим, что $\varphi: \text{Spec } L \rightarrow V = \text{Spec } A$ — точка, соответствующая гомоморфизму k -алгебр $A \rightarrow L$ с ядром P . Тогда φ продолжается до рационального отображения $f: W \rightarrow V$, образ которого плотен в подмногообразии $Y = V(P) \subset V$, так что φ или $\varphi(\text{Spec } L)$ является общей точкой в Y со значениями в поле.

(d) Точки как морфизмы в теории схем. Обсуждения п. (с) показывают, что L -значная точка многообразия V неявно содержит рациональное отображение $W \rightarrow V$, где W — многообразие, бирационально эквивалентное $\text{Spec } L$ (т. е. $L = k(W)$). Геометр может представлять себе это как множество точек, параметризованное многообразием W .

Вообще, S -значная точка (где S — произвольная схема) интересующего нас многообразия X (или схемы) может быть определена просто как морфизм $S \rightarrow X$. Если $X = V(I) \subset \mathbb{A}_k^n$ — аффинное подмногообразие с координатным кольцом $k[X]$ и $S = \text{Spec } A$, то S -значная точка соответствует, согласно (4.4), гомоморфизму k -алгебр $k[X] \rightarrow A$, т. е. n -набору $(a_1, \dots, a_n) = \mathbf{a}$ элементов из A , удовлетворяющему для всех $f \in I$ соотношению $f(\mathbf{a}) = 0$.

С высоконаучной точки зрения это — апофеоз определений многообразия. А именно, если точкой многообразия X называется просто морфизм, то само X является просто функтором

$$S \mapsto X(S) = \{\text{морфизмы } S \rightarrow X\}$$

на категории схем. (Суэта, которую я развел вокруг обозначения $\mathbb{A}^n$ в примечании на с. 56, уже отражает это обстоятельство. И хотя это может показаться странным, приведенные метафизические заклинания очень полезны в техническом отношении, и многообразие, определяемое как функтор, является основным понятием при современном подходе к пространствам модулей. Если рассматривается геометрический объект, который может «алгебраически зависеть от параметров» (такой, как пространственные кривые данной степени и рода), то естественно возникает желание наделить множество всех допустимых объектов структурой алгебраического многообразия. Более того, вас может заинтересовать поиск семейства объектов над пространством параметров, которое является

«универсальным» или «содержит все допустимые объекты». Многообразие параметров этого универсального семейства обычно наиболее непосредственно определяется как функтор (однако требуется еще доказать, что это многообразие существует). Например, упоминавшееся в разд. (8.2) многообразие Чжоу представляет функтор

$$S \mapsto \{\text{семейство кривых, параметризованных многообразием } S\}.$$

(8.14) Как схемы обобщают многообразия? Теперь я отдельно обсужу три причины, по которым аффинные схемы являются более общими объектами, чем аффинные многообразия. В патологических случаях эти обстоятельства могут встречаться в любых комбинациях, а также вместе с глобальными трудностями, обсуждавшимися в разд. (8.11) или даже вместе с такими новыми явлениями, как p -адическая сходимости или эрмитова метрика Аракелова. К счастью, соображение объема спасает меня от необходимости углубляться дальше в эти пленительные сюжеты.

(i) Алгебры не исчерпываются конечно порожденными. Предположим, что $C \subset S$ — кривая на неособой аффинной поверхности (над C , если угодно). Кольцо

$$\mathcal{O}_{S,C} = \{f \in k(S) \mid f = g/h, \text{ где } h \notin I_C\} \subset k(S),$$

называется локальным кольцом поверхности S относительно кривой C . Элементы $f \in \mathcal{O}_{S,C}$ регулярны на открытом множестве в S , содержащем открытое плотное подмножество кривой C . Теория делимости в этом кольце просто великолепна и связана с геометрическим понятием нулей и полюсов мероморфных функций. А именно, C локально определяется одним уравнением ($y = 0$), где $y \in I_C$ — локальная образующая, и любой ненулевой элемент $f \in \mathcal{O}_{S,C}$ имеет вид $f = y^n f_0$, где $n \in \mathbb{Z}$, а f_0 — обратимый элемент кольца $\mathcal{O}_{S,C}$. Кольцо с таким свойством называется *кольцом дискретного нормирования* в честь дискретного нормирования $f \mapsto n$, которое вычисляет порядок нуля функции f вдоль кривой C ($n < 0$ соответствует полюсам). Элемент y называется *локальным параметром кольца* $\mathcal{O}_{S,C}$.

Теория схем позволяет нам теперь непосредственно рассматривать $\text{Spec } \mathcal{O}_{S,C}$ как геометрический объект, а именно как топологическое пространство $(\cdot, \text{—})$, состоящее только из двух точек: замкнутой точки — максимального идеала (y) (т. е. общей точки кривой C) и незамкнутой точки — нулевого идеала (т. е. общей точки поверхности S). Получаемое преимущество имеет не только технический характер, так как несложная коммутативная алгебра колец дискретного нормирования, конечно, использовалась для получения

алгебро-геометрических результатов и результатов теории функций комплексного переменного (например, об идеалах функций или о локальном поведении над кривой C разветвленного накрытия $T \rightarrow S$ в терминах расширений полей $k(S) \subset k(T)$) задолго до изобретения схем. Более важно, что теория схем дает нам здесь точный геометрический язык и простую картину в локальной алгебре.

Это лишь один пример, относящийся к локализации или к понятию «окрестности общей точки подмногообразия», иллюстрирующий преимущества для обычной геометрии, возникающие из-за рассмотрения более общего спектра кольца, чем конечно порожденная алгебра над полем. Аналогичным примером является рассмотрение общей точки $\text{Spec } k(W)$ многообразия W как многообразия, полученного пересечением всех непустых открытых подмножеств в W (ср. с (8.13 (c))), подобно улыбке чеширского кота, которая остается после исчезновения самой кошачей мордочки.

(ii) Нильпотенты. Кольцо A может содержать нильпотентные элементы. Например, $A = k[x, y]/(y^2 = 0)$ соответствует «двойной прямой» $2l \subset \mathbb{A}_k^2$, которая рассматривается как инфинитезимальная полосообразная окрестность прямой. Элемент кольца A имеет вид $f(x) + \varepsilon f_1(x)$ (где $\varepsilon^2 = 0$). Таким образом, он выглядит как разложение многочлена в ряд Тейлора в окрестности l , оборванное на членах первого порядка. Если вы будете тренироваться по нескольку раз в день, то научитесь представлять себе этот элемент как функцию на двойной прямой $2l$.

Нильпотенты позволяют работать в теории схем с рядами Тейлора, усеченными до любого порядка, т. е. скажем, изучать точки многообразия методами теории рядов. Они являются важными в контексте задач теории модулей, упоминавшейся в конце (8.13 (d)). Например, они обеспечивают точный язык описания деформаций первого порядка геометрических объектов (как объектов над пространством параметров $\text{Spec}(k[\varepsilon]/(\varepsilon^2 = 0))$) и позволяют рассматривать их как касательные векторы к универсальному многообразию параметров. Они также приводят к большому числу явлений, не имеющих классических аналогов, например к связям между несепарабельными расширениями полей и алгебрами Ли векторных полей на многообразиях в характеристике p .

(iii) Долой основное поле. Пусть p — простое число, а $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ — подкольцо, состоящее из рациональных чисел, не содержащих p в знаменателе. $\mathbb{Z}_{(p)}$ является еще одним примером кольца дискретного нормирования с параметром p . В нем есть единственный максимальный идеал $0 \neq p\mathbb{Z}_{(p)}$, полем вычетов которого является $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p = \mathbb{Z}/(p)$. Если $F \in \mathbb{Z}_{(p)}[X, Y]$, то можно рассмот-

реть комплексную кривую $C_C: (F=0) \subset \mathbb{A}_C^2$ или привести функцию F по модулю p , получив в результате f , и рассмотреть, кривую $C_p: (f=0) \subset \mathbb{A}_{F_p}^2$. В какого типа геометрический объект можно включать и комплексную кривую и кривую над конечным полем? Можно ли считать такой объект вполне геометрическим — это уже вопрос точки зрения, но схема $\text{Spec } \mathbb{Z}_{(p)}[X, Y]/(F)$ именно это и позволяет сделать.

И опять, технически эта идея не является новой, так как приведение кривой по модулю p применялось, начиная с XVIII в., а вейлевские основания содержат целую теорию «специализаций», занимающихся этим. Преимуществом является новый взгляд на кривую $\text{Spec } \mathbb{Z}_{(p)}[X, Y]/(F)$ над кольцом дискретного нормирования $\mathbb{Z}_{(p)}$ как на геометрический объект, расслоенный над $\text{Spec } (\mathbb{Z}_{(p)}) (= (\cdot -))$; кривые C_C и C_p являются общим и специальным слоями соответственно.

Аналогично, для $F \in \mathbb{Z}[X, Y]$ схема $\text{Spec } \mathbb{Z}[X, Y]/(F)$ является геометрическим объектом, содержащим для каждого простого p кривую $C_p: (f_p=0) \subset \mathbb{A}_{F_p}^2$ над F_p , где f_p — редукция F по модулю p , и одновременно кривую $C_C: (F=0) \subset \mathbb{A}_C^2$, и называется *арифметической поверхностью*. Кроме того, она содержит еще много других объектов. В частности, для каждой точки $s \in C_C$; координаты которой являются алгебраическими числами, она содержит экземпляр $\text{Spec } \mathbb{Q}[c]$ и, следовательно, почти всю информацию о кольце целых чисел числового поля $\mathbb{Q}(c)$, определяемого точкой c . Каким бы уродливым ни выглядел этот объект с первого взгляда (к тому же к нему можно привыкнуть, если поупражняться), тем не менее он является важнейшей компонентой современной теории чисел и основным объектом, на котором зиждятся работы Аракелова и Фальтингса.

(8.15) Доказательство существования прямых на кубической поверхности. Каждый взрослый алгебраический геометр знаком с традиционным доказательством предложения (7.2) с помощью подсчета размерностей (см., например, [Beauville, Complex algebraic surfaces, p. 50] или [Мамфорд, Алгебраическая геометрия]). Мы коротко напомним его перед тем, как остановиться на его трудностях.

Множество прямых в $\mathbb{P}^3$ параметризуется четырехмерным грассманианом $\text{Gr} = \text{Gr}(2, 4)$, а кубические поверхности — проективным пространством $S = \mathbb{P}^N$ кубических форм от (X, Y, Z, T) (на самом деле размерность N равна 19). Обозначим через $Z \subset \text{Gr} \times S$ подмногообразие инцидентности:

$$Z = \{(l, X), l \in \text{Gr}, X \in S | l \subset X\}.$$

Так как кубические формы, обращающиеся в нуль на заданной прямой l , образуют $\mathbb{P}^{N-4}$, то с помощью проекции на первое слагаемое $Z \rightarrow \text{Gr}$ легко вывести, что Z — рациональное N -мерное многообразие. Вторая проекция $p: Z \rightarrow S$ является морфизмом двух N -мерных многообразий, и, следовательно,

(i) *либо* образ $p(X)$ является N -мерным многообразием в S и, таким образом, содержит открытое плотное подмножество в S , *либо* каждый слой проекции p имеет размерность ≥ 1 .

(ii) Z является проективным многообразием и потому образ $p(Z)$ замкнут в S .

Так как существуют кубические поверхности, на которых имеется только конечное множество прямых, то вторая возможность в п. (i) отпадает, и поэтому любая достаточно общая кубическая поверхность содержит прямые. Значит, из (ii) вытекает, что $p(Z) = S$, и каждая кубическая поверхность содержит прямые.

Это рассуждение кажется мне неподходящим для начального курса по двум причинам: в утверждении (i) используются результаты о размерностях слоев, которые, хотя и являются приемлемыми с интуитивной точки зрения, особенно для студентов, заканчивающих изучение курса), но доказать их строго трудно. Кроме того, (ii) является теоремой о полноте проективного многообразия, что также нуждается в доказательстве (с помощью теории исключения, компактности или с привлечением всей мощи валоативного критерия полноты).

Насколько мне известно, приведенное доказательство предложения (7.2) является новым. Осведомленный читатель заметит его связь с другими традиционными доказательствами, использующими векторные расслоения. А именно, на грассманиане $\text{Gr}(2, 4)$ имеется тавтологическое векторное расслоение ранга 2 (состоящее из линейных форм на прямых в $\mathbb{P}^3$). Ограничение уравнения f кубической поверхности на каждую прямую $l \subset \mathbb{P}^3$ определяет сечение $s(f) \in S^3 E$ третьей симметрической степени расслоения E . И наконец, то, что каждое сечение расслоения $S^3 E$ должно обращаться в нуль, вытекает либо из обильности E , либо из рассуждений с классом Чженя (что также приводит к магическому числу 27).

Вместо предисловия.

(8.16) Благодарности и имена, имена. Попытка перечислить всех математиков, которые внесли вклад в мое образование, была бы тщетной. Я особенно обязан моим официальным руководителям

Пьеру Делиню и Питеру Свиннертону-Дайеру (это было до того, как последний стал преуспевающим политиком и известной личностью). По-видимому, больше всего сведений я почерпнул из книг Давида Мамфорда, а своим пониманием (таким как оно есть) гротендиковского наследия обязан Мамфорду и Делиню. На мое мировосприятие и как математика, и как человека в большой мере повлиял Андрей Тюрин.

Мое представление о том, каким должен быть первоначальный университетский курс по алгебраической геометрии, частично сформировалось под влиянием курса, составленного около 1970 г. Свиннертоном-Дайером для третьекурсников Кембриджа и читавшегося в последующие годы им и Барри Теннисоном. Моя книга является в некоторых аспектах его прямым продолжением, и ряд упражнений был дословно заимствован из списков упражнений Теннисона. С другой стороны, я извлек большую пользу из той свободы в выборе материала, которая принята для курсов лекций в Уорике, а также из философии преподавания (явно сформулированной Кристофером Зиманом), согласно которой опыт исследователя должен быть одним из решающих обстоятельств при выборе того, как и чему следует учить.

«Подмигивающий тор», появляющийся в (2.14), стал мне известен от Джима Йеллса, сообщившего мне, что он узнал его от Х. Хопфа (и что он, по-видимому, восходит к более старой немецкой традиции искусства построения математических моделей и иллюстраций). Я должен поблагодарить Каролину Сериес, Франса Оорта, Джона Джонса, Улфа Персёна, Дэвида Фаулера, анонимного рецензента и Дэвида Транаха из ЦУП за полезные замечания к препринтному варианту этой книги и извиниться за то, что в некоторых местах я либо не смог в полном объеме реализовать их пожелания, либо предпочел следовать своим собственным планам.

Я благодарен Мартине Егер за ряд исправлений к первому изданию, а Исао Вакабаяси — за внимательное чтение текста, позволившее исправить много неточностей. Особенно я признателен Р. Чепмену и Б. Брюсу, указавшим наиболее серьезную ошибку первого издания (я не использовал гессиан в начале доказательства предложения (7.2), ссылаясь на неверное утверждение, вынесенное в упражнениях).

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

- | | |
|---|---|
| Абстрактное многообразие (abstract variety) 12, 88, 89, 131, 132 | Бирациональная эквивалентность (birational equivalence) 96—98, 109, 111, 118, 137 |
| Алгебраически замкнутое поле (algebraically closed field) 24, 58, 62, 73, 86, 129, 133, 134, 136 | Бирациональное отображение (birational map) 96—98, 101, 110 |
| — независимые элементы ($\sim$ independent elements) 67, 98, 106, 111 | Вещественная геометрия (real geometry) 129—130 |
| Алгебраическое (под)множество (algebraic (sub-)set) 56—61, 72, 73, 74, 87, 90—93 | Вложение Серге (Segre embedding) 99 |
| Асимптотическое направление (asymptotic direction) 16, 19, 21, 68 | Геометрическая точка (geometric point) 135 |
| Аффинная замена координат (affine change of coordinates) 20, 31 | — k -алгебра ($\sim k$ -algebra) 133 |
| — кривая ($\sim$ curve) 44, 49, 88 | Геометрическое кольцо (geometric ring) 133 |
| — схема ($\sim$ scheme) 133, 138 | Гессииан (Hessian) 44, 122, 142 |
| Аффинное многообразие (affine variety) 12, 79, 81, 83, 87, 133, 138 | Гиперповерхность (hypersurface) 64, 70—71, 73, 98, 102—104, 109 |
| — накрытие проективного многообразия ($\sim$ covering of projective variety) 93 | Групповой закон на кубике (group law on cubic) 39—42, 44—47, 51, 84 |
| — пространство A_k^n ($\sim$ space) 56, 59, 68, 72, 73, 74, 76, 86, 87, 88, 101, 102, 103, 110, 126, 137 | Декартов лист см. нодальная кубика |
| Аффинные координаты (affine coordinates) 21, 43, 44, 48, 93, 123 | Детерминант Сильвестра (Sylvester's determinant) 32 |
| Аффинный конус над проективным многообразием (affine cone over projective variety) 91, 92 | Диофантовы задачи (Diophantine problems) 8, 16—17, 31, 33, 47, 52 |
| — кусок проективного многообразия ($\sim$ piece of projective variety) 21, 44, 88, 93, 101, 122 | Доминантное отображение (dominant map) 82, 97 |
| Бесконечно удаленная прямая (line at infinity) 21 | Евклидово преобразование (Euclidean transformation) 20 |