Ж.Серр

АЛГЕБРАИЧЕСКИЕ ГРУППЫ И ПОЛЯ КЛАССОВ

Книга известного французского математика Ж. Серра стала одной из классических книг по алгебраической геометрии. Она не требует больших предварительных знаний и вводит читателя в круг современных вопросов. С большим педагогическим мастерством в ней излагается ряд основных понятий алгебраической геометрии (алгебраические кривые и поверхности, теорема Римана — Роха, якобиевы многообразия кривых и т. д.).

Книга рассчитана на научных работников, аспирантов и студентов старших курсов университетов и педагогических институтов.

Содержание

Указатель

ОТ РЕДАКТОРА ПЕРЕВОДА

Курс лекций, который читался Серром в Коллеж де Франс, посвящен изложению работ Розенлихта об обобщенных якобиевых многообразиях, Ленга об абелевых расширениях полей алгебраических функций, а также Барсотти, Розенлихта и Серра о расширениях и когомологиях алгебраических групп.

Для русского издания автором любезно были присланы некоторые замечания и дополнения. Они внесены в соответствующие места.

С. ДЕМУШКИН

Декабрь 1967 г.

ГЛАВА

I

СВОДКА ОСНОВНЫХ РЕЗУЛЬТАТОВ

Этот курс посвящен изложению недавних работ Розенлихта и Ленга. Начнем с краткого изложения результатов Розенлихта.

1. Обобщенные якобиевы многообразия

Пусть X — проективная неприводимая алгебраическая кривая без особенностей, $f: X \to G$ — рациональное отображение X в алгебраическую коммутативную группу G. Множество S точек кривой X, в которых f нерегулярно, есть конечное множество. Пусть D — дивизор, равный нулю на S (т. е. дивизор вида $D = \sum n_i P_i$, где $P_i \notin S$). Положим $f(D) = \sum n_i f(P_i) \in G$.

В случае когда G — *абелево многообразие*, $S = \varnothing$ и $f(D) = 0$ при D, равном дивизору (φ) рациональной функции φ на X; в этом случае $f(D)$ зависит лишь от *класса* дивизора D относительно линейной эквивалентности.

В общем случае приходится изменить понятие класса (так же как и в теории чисел для изучения разветвленных накрытий) следующим образом.

Назовем *модулем с носителем* S функцию, ставящую в соответствие каждой точке $P_i \in S$ целое число $n_i > 0$. Пусть $\mathfrak{m}$ — модуль с носителем S, а φ — рациональная функция. Говорят, что φ „сравнима с 1 по модулю $\mathfrak{m}$“, и пишут $\varphi \equiv 1 \pmod{\mathfrak{m}}$, если $v_i(1-\varphi) \geqslant n_i$ для всех i, где v_i обозначает нормирование, определенное точкой P_i. Поскольку $n_i > 0$, такая функция φ регулярна в точках P_i и принимает в них значение 1; таким образом, дивизор (φ) такой функции равен нулю на S.

Теорема 1. *Для всякого рационального отображения $f: X \to G$, регулярного вне S, существует модуль $\mathfrak{m}$ с носителем S, такой, что $f(D) = 0$ для любого дивизора $D = (\varphi)$, где $\varphi \equiv 1 \pmod{\mathfrak{m}}$.*

(Доказательство см. в гл. III, § 2.)

Обратно, по заданному модулю $\mathfrak{m}$ можно восстановить если не саму группу G, то по крайней мере „универсальную" группу для группы G.

Теорема 2. *Для всякого модуля $\mathfrak{m}$ существуют алгебраическая коммутативная группа $J_{\mathfrak{m}}$ и рациональное отображение $f_{\mathfrak{m}}: X \to J_{\mathfrak{m}}$, такие, что выполняется следующее свойство:*

для всякого рационального отображения $f: X \to G$, удовлетворяющего условиям теоремы 1 относительно модуля $\mathfrak{m}$, существует (аффинный) рациональный гомоморфизм $\theta: J_{\mathfrak{m}} \to G$, определяемый единственным образом, такой, что $f = \theta \circ f_{\mathfrak{m}}$.

(Доказательство см. в гл. V, п. 9.)

Можно уточнить структуру $J_{\mathfrak{m}}$ точно так же, как в случае обыкновенных якобиевых многообразий (получаемых, если положить $\mathfrak{m} = 0$). Для этого рассмотрим группу $C_{\mathfrak{m}}$ классов дивизоров, равных нулю на S, по модулю дивизоров вида $D = (\varphi)$, где $\varphi \equiv 1 \pmod{\mathfrak{m}}$; пусть $C_{\mathfrak{m}}^0$ - подгруппа группы $C_{\mathfrak{m}}$ классов дивизоров степени 0. Если обозначить через C^0 группу классов (в обычном смысле) дивизоров нулевой степени, то получим сюръективный гомоморфизм $C_{\mathfrak{m}}^0 \to C^0$. Ядро $L_{\mathfrak{m}}$ этого гомоморфизма состоит из классов $C_{\mathfrak{m}}$ дивизоров вида (φ), где φ обратима во всех точках $P_i \in S$. Но для каждого $P_i \in S$ обратимые элементы с точностью до элементов, сравнимых с 1 по модулю $\mathfrak{m}$, образуют алгебраическую коммутативную группу $R_{\mathfrak{m}, i}$ размерности n_i; пусть $R_{\mathfrak{m}}$ — произведение этих групп. По теореме о независимости нормирований можно найти функцию, соответствующую произвольным элементам $r_i \in R_{\mathfrak{m}, i}$. Отсюда следует, что $L_{\mathfrak{m}}$ изоморфна факторгруппе $R_{\mathfrak{m}}/G_m$, где через G_m обозначена мультипликативная группа основного поля, естественным образом вложенная в $R_{\mathfrak{m}}$. Полагая $J = C^0$, получаем в итоге точную последовательность

$$0 \to R_{\mathfrak{m}}/G_{\mathfrak{m}} \to C^0_{\mathfrak{m}} \to J \to 0.$$

Заметим, что на J имеется естественная структура *алгебраической группы*, поскольку J является якобиевым многообразием кривой X. То же самое относится к $C^0_{\mathfrak{m}}$. Эта структура продолжается и на $R_{\mathfrak{m}}/G_{\mathfrak{m}}$, как показывает

Теорема 3. *Отображение $f_{\mathfrak{m}}: X \to J_{\mathfrak{m}}$ определяет при распространении его на классы дивизоров биекцию $C^0_{\mathfrak{m}}$ на $J_{\mathfrak{m}}$. Если отождествить $C^0_{\mathfrak{m}}$ с $J_{\mathfrak{m}}$ посредством этой биекции, то группа $J_{\mathfrak{m}}$ будет расширением (в смысле алгебраических групп) группы J с помощью группы $R_{\mathfrak{m}}/G_{\mathfrak{m}}$.*

(Доказательство см. в гл. V, § 3.)

Группы $J_{\mathfrak{m}}$ являются *обобщенными якобиевыми многообразиями* кривой X.

2. Абелевы накрытия

Пусть G — связная коммутативная алгебраическая группа и θ: $G' \to G$ — *изогения* (группа G' также предполагается связной). Это означает, что θ — сюръективный гомоморфизм (в смысле алгебраических групп) с конечным ядром. Предположим далее, что расширение полей, соответствующее гомоморфизму θ, сепарабельно. В этом случае мы будем говорить, что отображение θ *сепарабельно*. Если $\mathfrak{g}$ обозначает ядро θ, то группа G отождествляется с фактором $G'/\mathfrak{g}$ и G' является неразветвленным накрытием G, имеющим в качестве группы Галуа абелеву группу $\mathfrak{g}$.

Пусть теперь U — алгебраическое многообразие и $f: U \to G$ — регулярное отображение. Определим *прообраз* $U' = f^{-1}(G')$ группы G' при отображении f как подмногообразие многообразия $U \times G'$, образованное парами (x, g'), такими, что $f(x) = \theta(g')$. Проекция $U' \to U$ превращает U' в (неразветвленное) накрытие U с группой Галуа $\mathfrak{g}$.

Вообще пусть $f: X \to G$ — рациональное отображение неприводимого многообразия X в группу G и $X' \to X$ — накрытие X с группой Галуа $\mathfrak{g}$. Если существует открытое непустое множество U, на котором f регулярно, и если накрытие U', индуцированное накрытием X' на U, изоморфно $f^{-1}(G')$, то мы будем говорить, что X' — *прообраз* изогении $G' \to G$ при отображении f (т. е. понятие прообраза имеет бирациональный характер).

Имеет место

Теорема 4. *Всякое абелево накрытие неприводимого алгебраического многообразия является прообразом некоторой изогении.*

Наметим идею доказательства (подробности см. в гл. VI, § 2). Мы ограничимся случаем неприводимого накрытия $X' \to X$. Можно, очевидно, считать, что $\mathfrak{g}$ — циклическая группа порядка n, где n или взаимно просто с p, или равно p^m.

1) *Группа $\mathfrak{g}$ циклическая порядка n, где $(n, p) = 1$.*

Пусть G_m — мультипликативная группа и $\theta_n : G_m \to G_m$ — изогения, задаваемая эндоморфизмом $\lambda \to \lambda^n$. Если отобразить группу $\mathfrak{g}$ на мультипликативную группу корней n-й степени из единицы, то образующая σ группы Галуа $\mathfrak{g}$ перейдет в примитивный корень из единицы ε, при этом ядро отображения θ_n отождествляется с группой $\mathfrak{g}$. Покажем, что всякое абелево накрытие с группой Галуа $\mathfrak{g}$ является прообразом θ_n. Действительно, пусть L/K — расширение полей, соответствующее данному накрытию $X' \to X$. Поскольку норма ε в L/K равна 1, из классической „теоремы 90“ Гильберта следует существование элемента $g \in L^*$, такого, что $g^\sigma = \varepsilon g$. Имеем $L = K(g)$ (элемент g называется „образующей Куммера“). Далее, $f = g^n \in K$. Отображение $g: X' \to G_m$ коммутирует с операциями $\mathfrak{g}$ и определяет при переходе к фактору отображение $f: X \to G_m$. Это показывает, что $X' = f^{-1}(G_m)$.

2) *Группа $\mathfrak{g}$ циклическая порядка p^m.*

Предположим сначала, что $m = 1$. Пусть G_a — аддитивная группа и $\wp$: $G_a \to G_a$ — изогения, задаваемая эндоморфизмом $\wp(\lambda) = \lambda^p - \lambda$. Ядром этой изогении является группа $\mathbf{Z}/p\mathbf{Z}$ целых чисел по модулю p; после выбора образующей $\mathfrak{g}$ его можно отождествить с $\mathfrak{g}$. Мы увидим, что всякое абелево накрытие с группой Галуа $\mathfrak{g}$ является прообразом изогении $\wp$. Действительно, пусть, как и выше, L/K — расширение, соответствующее нашему накрытию. Поскольку след 1 в L/K равен 0, из аддитивного варианта „теоремы 90“ вытекает существование элемента $g \in L$, такого, что $g^\sigma = g + 1$ (элемент g называется „образующей Артина — Шрейера“). Имеем $f = \wp(g) = g^p - g \in K$. Как и выше, это означает, что данное накрытие является прообразом $\wp$ при отображении g.

В случае $m > 1$ следует заменить группу G_a на группу W_m *векторов Витта* длины m (см. Витт [1]).

Объединяя теорему 4 с теоремами 1 и 2, получаем

Следствие. *Пусть $X' \to X$ — абелево накрытие алгебраической кривой X. Существует такая сепарабельная изогения $\theta: G' \to J_\mathfrak{m}$, где $J_\mathfrak{m}$ — обобщенное якобиево многообразие кривой X, что X' изоморфно $f_\mathfrak{m}^{-1}(G')$.*

Далее мы докажем следующие результаты (см. гл. VI, § 2).

а) Для заданных X' и $J_\mathfrak{m}$ изогения $\theta: G' \to J_\mathfrak{m}$ определяется единственным образом.

б) Модуль $\mathfrak{m}$ можно выбрать так, чтобы его носитель S был в точности равен множеству точек ветвления данного накрытия $X' \to X$. В частности, неразветвленным накрытиям соответствуют изогении якобиевого многообразия.

Применением а) и теоремы о „спуске основного поля“ Вейля [11] доказывается следующая теорема (см. гл. VI, § 4).

Теорема 5. *Если абелево накрытие $X' \to X$ определено и абелево над конечным полем k, то изогению $\theta: G' \to J_\mathfrak{m}$ из следствия теоремы 4 можно определить над k.*

Так, с помощью k-изогений обобщенных якобиевых многообразий $J_\mathfrak{m}$, соответствующих рациональным над полем k модулям $\mathfrak{m}$, можно получить конструкцию абелевых расширений поля $k(X)$. Как показал Ленг, эта конструкция дает возможность легко построить теорию полей классов для поля $k(X)$ (см. гл. VI, § 6). В частности, закон взаимности Артина сводится к формальному вычислению изогении θ. „Явные законы взаимности“ находятся с помощью „локальных символов“ и теоремы 1 (см. гл. III, § 1, а также гл. VI, п. 30).

3. Другие результаты

а) Теория полей классов была распространена Ленгом на многообразия произвольной размерности. Отображения $f_{\mathfrak{m}}$: $X \to J_{\mathfrak{m}}$ заменяются при этом на „максимальные“ отображения (см. гл. VI, § 3). Наиболее интересным является пример канонического отображения кривой X в ее *многообразие Альбанезе*, с помощью которого получаются „почти все“ неразветвленные абелевы расширения X (см. гл. VI, п. 20). Отметим, что кроме этого случая и случая кривых очень мало имеется фактов о максимальных отображениях; ничего не известно об „обобщенных многообразиях Альбанезе“, которые призваны играть роль $J_{\mathfrak{m}}$.

б) Обобщенные якобиевы многообразия помимо их арифметических приложений интересны еще и тем, что они дают нетривиальные примеры *расширений* абелева многообразия с помощью линейной группы. Пусть, например, $P \in X$. Положим $\mathfrak{m} = 2P$. После выбора локальной униформизующей t_P в P группа $L_{\mathfrak{m}}$ из п. 1 отождествляется с аддитивной группой G_a. Многообразие $J_{\mathfrak{m}}$ превращается таким образом в расширение обыкновенного якобиева многообразия J с помощью G_a. В силу результата Розенлихта (см. гл. VII, п. 6) это расширение можно рассматривать как главное расслоенное пространство с базой J и группой G_a. Оно определяет, следовательно, элемент $j_P \in H^1(J, \mathfrak{G}_J)$. Пусть j'_P — образ j_P при гомоморфизме $H^1(J, \mathfrak{G}_J)$ в $H^1(X, \mathfrak{G}_X)$, определенном отображением $f_{\mathfrak{m}}$. Имеет место

Теорема 6. *При отождествлении $H^1(X, \mathfrak{G}_X)$ с классами распределений на X* (см. гл. V, п. 5) *элемент $j'_P \in H^1(X, \mathfrak{G}_X)$ отождествляется с классом распределения* $1/t_P$.

Как мы увидим, эта теорема позволяет определить группу $H^1(J, \mathfrak{G}_J)$ и вообще группу $H^q(A, \mathfrak{G}_A)$ для любого абелева многообразия A и любого целого числа q (гл. VII, § 4).

Библиографические замечания

Приведенные выше результаты излагаются в последующих главах этого курса; в конце каждой главы имеются краткие библиографические замечания. Здесь отметим лишь, что построение обобщенных якобиевых многообразий вместе с выяснением их свойств было проведено Розенлихтом [2], [3]; арифметические результаты п. 2 принадлежат Ленгу [2], [3]. Оба автора опираются на теорию абелевых многообразий, разработанную Вейлем [5]. Определение когомологий абелевых многообразий принадлежит по существу Розенлихту [4] и Барсогти [3], [4]; см. также Серр [6].

ГЛАВА

II

АЛГЕБРАИЧЕСКИЕ КРИВЫЕ

В этой главе, как и в двух следующих, не рассматриваются вопросы рациональности. Поэтому предполагается, что основное поле k есть алгебраически замкнутое поле (произвольной характеристики). Определения и элементарные результаты, относящиеся к алгебраическим многообразиям и пучкам, см. в моей работе о когерентных пучках (Серр [1]), которая сокращенно обозначается далее АКП. Эта работа легко переводится на язык Вейля ([3], Ленг [4]), или язык схем (Картан и Шевалле [1]).

1. Алгебраические кривые

Пусть X — алгебраическая кривая, т. е. алгебраическое многообразие размерности 1; мы предполагаем, что X — *неприводимая неособая* и *полная* кривая.

Пусть $k(X)$ — поле рациональных функций на X. Это поле является конечно-порожденным расширением поля k степени трансцендентности 1. Обратно, каждому такому расширению F/k соответствует единственная кривая X (с точностью до изоморфизма).

Покажем сначала *существование* кривой X. Пусть $x_1, \ldots, x_r$ — образующие расширения F/k и $A = k[x_1, \ldots, x_r]$ — подалгебра F, порожденная элементами x_i; она является аффинной алгеброй, соответствующей замкнутому подмногообразию Y аффинного пространства k^r. Его замыкание $\overline{Y}$ в проективном пространстве $\mathbf{P}_r(k)$ будет полной неприводимой кривой с полем рациональных функций F. В качестве искомой кривой X достаточно взять *нормальную модель* $\overline{Y}$; действительно, как известно, нормальная кривая — неособая. Более того, метод проективной нормализации (см., например, Самюэль [3], стр. 25—26, или Ленг [4], стр. 133—146) показывает, что X *можно погрузить в проективное пространство.*

Единственность кривой X следует из явного определения ее топологии Зарисского и ее локальных колец (см. п. 2); впрочем, известно, что знание локальных колец неприводимого многообразия X произвольной размерности определяет его топологию Зарисского (см. [17], сообщения 1 и 2).

Замечание. Единственность X может быть также выведена из следующего факта: всякое рациональное отображение неособой кривой в полное многообразие всюду регулярно.

Изучение кривой X, таким образом, *эквивалентно* изучению расширения F/k в противоположность многообразиям размерности $\geqslant 2$. Следовательно, для случая кривых нет оснований говорить о различии между методами „алгебраическим“ и „геометрическим“.

2. Локальные кольца

Пусть P — точка кривой X. Известно, что́ такое *локальное кольцо* $\mathfrak{O}_P$ кривой X в точке P. Если предположить, что кривая X вложена в проективное пространство $\mathbf{P}_r(k)$, то это есть множество функций, индуцированных рациональными функциями вида R/S, где R и S — однородные полиномы одной и той же степени и $S(P) \neq 0$. Это кольцо является подкольцом поля $k(X)$. В силу общих свойств алгебраических многообразий, это *локальное нётерово кольцо*, максимальный идеал которого $\mathfrak{m}_P$ состоит из функций f, обращающихся в нуль в точке P; при этом $\mathfrak{O}_P/\mathfrak{m}_P = k$. Элементы кольца $\mathfrak{O}_P$ называются *регулярными* функциями в точке P.

Воспользуемся теперь предположениями относительно кривой X. Так как X — кривая, то $\mathfrak{O}_P$ — локальное кольцо *размерности* 1 (в смысле теории размерности для локальных колец): оно не имеет простых идеалов, отличных от 0 или $\mathfrak{m}_P$. Так как P — простая точка кривой X, локальное кольцо, кроме того, *регулярно*: его максимальный идеал может быть порожден одним элементом. Этот элемент называется *локальным параметром* в точке P. В силу известной (и элементарной) теоремы из предыдущих свойств вытекает, что

$\mathcal{O}_P$ — *кольцо дискретного нормирования*. Соответствующее нормирование обозначается через v_P. Если f — ненулевой элемент поля $k(X)$, то равенство $v_P(f) = n$, $n \in \mathbf{Z}$, означает, что f может быть представлен в виде $f = t^n u$, где t — локальный параметр в точке P, а u — обратимый элемент в кольце $\mathcal{O}_P$. Кольца $\mathcal{O}_P$ являются единственными кольцами нормирований, содержащими поле k. Действительно, если U — такое кольцо, то U содержит $\mathcal{O}_P$ (так как X предполагается полным; это одно из определений полного многообразия, см. [11]) и, следовательно, совпадает с $\mathcal{O}_P$, потому что $\mathcal{O}_P$ — кольцо нормирования.

Как и для любого алгебраического многообразия, кольца $\mathcal{O}_P$ в данном случае образуют *пучок колец* на кривой X при условии, что в X введена *топология Зарисского* [АКП, гл. II]. Напомним, что замкнутые подмножества в этой топологии — это конечные подмножества и вся кривая X. Пучок колец $\mathcal{O}_P$ будет обозначаться через $\mathcal{O}_X$ или просто $\mathcal{O}$. Этот пучок является подпучком постоянного пучка $k(X)$.

3. Дивизоры, линейная эквивалентность, линейные системы

Элемент свободной абелевой группы, порожденной точками $P \in X$, называется *дивизором*. Таким образом, дивизор D записывается в виде $D = \sum_{P \in X} n_P P$, где $n_P \in \mathbf{Z}$ и $n_P = 0$ для почти всех P (за исключением конечного числа). Коэффициенты n_P в D обозначаются через $v_P(D)$. *Степень* дивизора D определяется равенством

$$\deg(D) = \sum n_P = \sum v_P(D).$$

Дивизор считают *положительным*, если все $v_P(D) \geqslant 0$. Отсюда очевидна структура упорядочивания в группе $D(X)$ всех дивизоров кривой X.

Если f — ненулевой элемент поля $k(X)$, то *дивизор функции* f, обозначаемый (f), определяется формулой

$$(f) = \sum_{P \in X} v_P(f) P.$$

В силу очевидного равенства $(fg) = (f) + (g)$, эти дивизоры образуют подгруппу $P(X)$ группы $D(X)$ (f пробегает $k(X)^*$). Факторгруппа $C(X) = D(X)/P(X)$ называется *группой классов* дивизоров (по линейной эквивалентности). Два дивизора из одного и того же класса называются линейно эквивалентными.

Предложение 1. *Если* $D \in P(X)$, *то* $\deg(D) = 0$.

Этот результат является немедленным следствием теоремы Римана — Роха в первой форме (см. п. 4), которая будет доказана без использования этого предложения. Но можно дать и непосредственное доказательство. Пусть $D = (f)$, где $f \in k(X)^*$ и отлична от константы (в противном случае $D = 0$). Функция f определяет тогда отображение кривой X в проективную прямую $\mathbf{P}^1(k)$ и (f) — не что иное, как дивизор $f^{-1}(0) - f^{-1}(\infty)$, где 0 и ∞ — точки в $\mathbf{P}^1(k)$, а операция f^{-1} понимается в смысле теории пересечений. Но известно (из той же теории), что для всех точек $a \in \mathbf{P}^1(k)$ степень дивизора $f^{-1}(a)$ равна степени проекции f, т. е. $[k(X): k(f)]$. Отсюда и вытекает предложение с дополнительным уточнением (которое показывает, например, что ни $f^{-1}(0)$, ни $f^{-1}(\infty)$ не сводятся к 0 для непостоянной функции; иначе говоря, неравенство $(f) \geqslant 0$ означает, что f — константа).

Из предложения 1 следует, что можно говорить о степени класса дивизоров, в частности, о группе $C^0(X)$ классов дивизоров степени 0. Имеем

$$C(X)/C^0(X) = \mathbf{Z}.$$

Объединяя линейную эквивалентность с отношением порядка дивизоров, мы получаем понятие *линейной системы*.

Пусть D — произвольный дивизор. Рассмотрим положительные дивизоры D', линейно эквивалентные D. Для каждого такого дивизора можно записать $D' = D + (f)$, где $f \in k(X)^*$; мы должны иметь $D + (f) \geqslant 0$, т. е. $(f) \geqslant -D$. Функции, удовлетворяющие этому условию, образуют вместе с нулем векторное пространство, которое обозначается через $L(D)$. Мы убедимся далее (предложение 2), что $L(D)$ — конечномерное пространство. Каждый элемент $f \neq 0$ из $L(D)$ определяет дивизор $D' = D + (f)$, отвечающий нашему требованию, и две функции f и g определяют один и тот же дивизор тогда и только тогда, когда $f=\lambda g$, где $\lambda \in k^*$. Таким образом, множество $|D|$ положительных дивизоров, линейно эквивалентных дивизору D, находится в биективном соответствии с *проективным пространством* $\mathbf{P}(L(D))$, соответствующим векторному пространству $L(D)$. Когда мы заменяем D на линейно эквивалентный ему дивизор, структура проективного пространства, соответствующего $|D|$, не изменяется. Непустое множество F положительных дивизоров D называется *линейной системой*, если существует дивизор D, такой, что F является подпространством пространства $|D|$. В случае $F=|D|$ говорят, что линейная система F *полная*. Линейная система F, содержащаяся в $|D|$, соответствует векторному подпространству $V\subset L(D)$. Размерность V равна проективной размерности F, увеличенной на единицу. В частности, если $l(D)$ обозначает размерность $L(D)$, то

$$l(D)=\dim|D|+1.$$

Замечание. С каждой линейной системой тесно связано некоторое отображение кривой в проективное пространство. Укажем кратко, каким именно образом.

Пусть $\varphi\colon X\to \mathbf{P}_r(k)$ — регулярное отображение кривой X в проективное пространство. Предположим, что $\varphi(X)$ порождает (в проективном смысле) $\mathbf{P}_r(k)$. При этом предположении, если H обозначает гиперплоскость $\mathbf{P}_r(k)$, дивизор $\varphi^{-1}(H)$ вполне определен. Когда H изменяется, $\varphi^{-1}(H)$ образуют линейную систему F размерности r „без неподвижных точек" (т. е. для всех точек $P\in X$ существует дивизор $D\in F$, такой, что $v_P(D)=0$). Наоборот, все линейные системы без неподвижных точек получаются таким образом, причем однозначно (с точностью до автоморфизма $\mathbf{P}_r(k)$). Более того, для каждой линейной системы F существуют положительный дивизор A и линейная система без неподвижных точек F', такие, что F состоит из дивизоров вида $A+D'$, где D' пробегает F'. Дивизор A называется в этом случае *неподвижной частью* линейной системы F.

Все предыдущее можно с очевидными изменениями перенести на случай, когда X — нормальное многообразие произвольной размерности. Однако в этом случае надо различать

неподвижные компоненты линейной системы F (которые являются подмногообразиями $W \subset X$ коразмерности 1, такими, что $D \geqslant W$ для всех $D \in X$) и *базисные точки* системы F (которые являются точками пересечения носителей дивизоров $D \in F$). Рациональное отображение кривой X в проективное пространство, соответствующее линейной системе F, не меняется, если удалить из F ее неподвижные компоненты. Это отображение регулярно вне базисных точек F. Дальнейшие подробности см., например, у Ленга [4], гл. VI.

4. Теорема Римана — Роха (первая форма)

Пусть D — дивизор на кривой X. В предыдущем пункте было определено векторное пространство $L(D)$. Это множество рациональных функций f, которые удовлетворяют условию $(f) \geqslant -D$, т. е.

$$v_P(f) \geqslant -v_P(D) \quad \text{для всех точек} \quad P \in X.$$

Пусть теперь P — точка кривой X. Обозначим через $\mathscr{L}(D)_P$ множество функций f, удовлетворяющих предыдущему неравенству в точке P. Элементы $\mathscr{L}(D)_P$ образуют *подпучок* $\mathscr{L}(D)$ постоянного пучка $k(X)$. Группа $H^0(X, \mathscr{L}(D))$ совпадает с $L(D)$.

Предложение 2. *Векторные пространства $H^0(X, \mathscr{L}(D))$ и $H^1(X, \mathscr{L}(D))$ конечномерны над k. Для $q \geqslant 2$ имеем $H^q(X, \mathscr{L}(D)) = 0$.*

Согласно АКП (п. 53), имеем $H^q(X, \mathscr{F}) = 0$ при $q \geqslant 2$ для любого пучка $\mathscr{F}$, откуда следует вторая часть предложения. Для доказательства первой части достаточно в соответствии с АКП (п. 66) доказать, что $\mathscr{L}(D)$ — алгебраический когерентный пучок. Итак, пусть P — точка кривой X и φ — функция, для которой $v_P(\varphi) = v_P(D)$. Отсюда получаем, что умножение на φ есть изоморфизм пучка $\mathscr{L}(D)$ на пучок $\mathscr{O}$ в окрестности точки P. Следовательно, пучок $\mathscr{L}(D)$ когерентен, ч. т. д.

Замечания. 1. Если $D' = D + (\varphi)$, то пучок $\mathscr{L}(D)$ изоморфен пучку $\mathscr{L}(D')$, причем изоморфизм определяется умножением на функцию φ.

2. Предложение 2 легко доказать без использования результатов АКП, применяя непосредственно определения $H^0(X, \mathscr{L}(D))$ и $H^1(X, \mathscr{L}(D))$; соответствующая литература приводится в конце главы.

Прежде чем сформулировать теорему Римана—Роха, введем следующие обозначения:

$$I(D) = H^1(X, \mathscr{L}(D)), \quad i(D) = \dim I(D),$$

$$g = i(0) = \dim H^1(X, \mathscr{O}).$$

Целое число g называется *родом* кривой X. Далее будет видно, что предыдущее определение эквивалентно обычному.

Теорема 1 (теорема Римана—Роха; первая форма). *Для всех дивизоров D имеем* $l(D) - i(D) = \deg(D) + 1 - g$.

Убедимся сначала, что эта формула верна для $D = 0$. Действительно, имеем $l(0) = 1$ (так как константы — единственные функции, удовлетворяющие условию $(f) \geqslant 0$). Кроме того, $i(0) = g$ по определению и $\deg(0) = 0$.

Теперь достаточно показать, что если формула верна для дивизора D, то она верна для дивизора $D + P$, и наоборот (P — произвольная точка кривой X), ибо очевидно, что от нулевого дивизора можно перейти к любому дивизору последовательным прибавлением или отниманием по одной точке.

Обозначим левую часть формулы через $\chi(D)$, а правую — через $\chi'(D)$. Имеем $\chi'(D + P) = \chi'(D) + 1$. Поэтому достаточно показать, что такая же формула верна и для $\chi(D)$. Пучок $\mathscr{L}(D)$ является подпучком пучка $\mathscr{L}(D + P)$, что дает возможность записать точную последовательность пучков

$$0 \to \mathscr{L}(D) \to \mathscr{L}(D + P) \to \mathscr{Q} \to 0.$$

Факторпучок $\mathscr{Q}$ — нулевой вне точки P, а его слой $\mathscr{Q}_P$ в точке P является одномерным векторным пространством. Таким образом, $H^1(X, \mathscr{Q}) = 0$, а $H^0(X, \mathscr{Q}) = \mathscr{Q}_P$ — одномерное векторное пространство. Запишем точную последовательность групп когомологий

$$0 \to L(D) \to L(D + P) \to H^0(X, \mathscr{Q}) \to I(D) \to I(D + P) \to 0.$$

Вычисляя альтернированную сумму размерностей векторных пространств, получаем

$$l(D)-l(D+P)+1-i(D)+i(D+P)=0,$$

т. е.

$$\chi(D+P)=\chi(D)+1,$$

ч. т. д.

Замечания. 1. Одной теоремы 1 недостаточно для вычисления $l(D)$. Надо иметь сведения о числе $i(D)$. Эти сведения будут получены в *теореме двойственности* (п. 8). Теорема Римана — Роха примет тогда окончательный вид.

2. Метод доказательства теоремы, состоящий в проверке формулы для одного дивизора, а затем в переходе от этого дивизора к другому с помощью пучка $\mathfrak{G}$, сконцентрированного на подмногообразии, применим также к многообразиям более высокой коразмерности. Например, нетрудно доказать этим способом теорему Римана — Роха для неособой поверхности в виде

$$\chi(D)=\frac{1}{2}D(D-K)+1+p_a,$$

где K обозначает канонический дивизор, а p_a — арифметический род рассматриваемой поверхности (см. гл. IV, п. 8).

5. Классы распределений

Прежде чем перейти к дифференциалам и теореме двойственности, покажем, как можно проинтерпретировать векторное пространство $l(D)$ на языке распределений (или „аделей") Вейля.

Распределение r есть семейство $\{r_P\}_{P\in X}$ элементов поля $k(X)$, таких, что $r_P\in\mathfrak{O}_P$ для почти всех точек $P\in X$. Распределения образуют алгебру R над полем k. Для дивизора D будем обозначать через $R(D)$ векторное подпространство R, состоящее из таких распределений $r=\{r_P\}$, что $v_P(r_P)\geqslant -v_P(D)$. Когда дивизоры D пробегают упорядоченное множество дивизоров кривой X, $R(D)$ образуют возрастающее фильтрованное семейство подпространств R, объединение которых совпадает со всем пространством R.

С другой стороны, если каждому элементу $f \in k(X)$ поставить в соответствие распределение $\{r_P\}$, такое, что $r_P = f$ для всех точек $P \in X$, то получим отображение поля $k(X)$ в алгебру R, которое позволяет отождествить поле $k(X)$ с подкольцом R. Используя эти определения, имеем

Предложение 3. *Для дивизора D кривой X векторное пространство $I(D) = H^1(X, \mathscr{L}(D))$ канонически изоморфно $R/(R(D) + k(X))$.*

Пучок $\mathscr{L}(D)$ — подпучок постоянного пучка $k(X)$. Следовательно, имеем точную последовательность

$$0 \to \mathscr{L}(D) \to k(X) \to k(X)/\mathscr{L}(D) \to 0.$$

Так как кривая X неприводима и пучок $k(X)$ постоянен, имеем

$$H^1(X, k(X)) = 0$$

(ибо нерв всякого покрытия X является симплексом). С другой стороны, так как кривая X связна, то $H^0(X, k(X)) = k(X)$. Точная последовательность групп когомологий, соответствующая предыдущей точной последовательности пучков, записывается следующим образом:

$$k(X) \to H^0(X, k(X)/\mathscr{L}(D)) \to H^1(X, \mathscr{L}(D)) \to 0.$$

Пучок $A = k(X)/\mathscr{L}(D)$ есть „пучок небоскребов“: если s — сечение пучка A над окрестностью U точки P, то существует окрестность $U' \subset U$ точки P, такая, что $s = 0$ на $U' - P$. Отсюда следует, что группа $H^0(X, A)$ отождествляется с прямой суммой групп A_P по точкам $P \in X$, которая, очевидно, изоморфна $R/R(D)$. Точная последовательность, записанная выше, показывает тогда, что $H^1(X, \mathscr{L}(D))$ отождествляется с $R/(R(D) + k(X))$, ч. т. д.

Всюду далее мы отождествляем $I(D)$ и $R/(R(D) + k(X))$.

6. Пространство, двойственное к пространству классов распределений

Здесь используются те же определения, что и в предыдущем пункте. Пусть $J(D)$ — пространство, двойственное к векторному пространству $I(D) = R/(R(D) + k(X))$. Элемент пространства $J(D)$ отождествляется, следовательно, с линейной формой на пространстве R, аннулирующей подпространство $R(D)$ и поле $k(X)$. Для $D' \geqslant D$ имеем $R(D') \supset R(D)$. Это показывает, что $J(D) \supset J(D')$. Объединение $J(D)$ по D, пробегающим множество дивизоров X, будет обозначаться через J. Отметим, что $J(D)$ является убывающим фильтрированным семейством. (Можно интерпретировать J как пространство, *топологически двойственное* пространству $R/k(X)$, снабженному топологией, которая определяется векторными пространствами — образами пространств $R(D)$.)

Пусть $f \in k(X)$ и $\alpha \in J$. Отображение $r \to \langle \alpha, fr \rangle$ есть линейная форма на пространстве R, которая аннулирует поле $k(X)$. Обозначим ее через $f\alpha$. Имеем $f\alpha \in J$. Действительно, если $\alpha \in J(D)$ и $f \in L(\Delta)$, то линейная форма $f\alpha$ аннулирует $R(D-\Delta)$ и, следовательно, принадлежит пространству $J(D-\Delta)$. Операция $(f, \alpha) \to f\alpha$ снабжает J структурой *векторного пространства* над полем $k(X)$.

Предложение 4. *Размерность векторного пространства J над полем $k(X)$ не больше* 1.

Предположим, что α и α' — два элемента пространства J, линейно независимых над полем $k(X)$. Так как J есть объединение множеств $J(D)$, найдется дивизор D, такой, что $\alpha \in J(D)$ и $\alpha' \in J(D)$. Положим $d = \deg(D)$.

Для всех целых $n \geqslant 0$ пусть Δ_n — дивизор степени n (например, $\Delta_n = nP$, где P — фиксированная точка кривой X). Если $f \in L(\Delta_n)$, то $f\alpha \in J(D-\Delta_n)$ в силу того, что говорилось выше; то же самое относится к $g\alpha'$, если $g \in L(\Delta_n)$. Так как α и α' линейно независимы над полем $k(X)$, соотношение $f\alpha + g\alpha' = 0$ выполняется только для $f = g = 0$. Отсюда следует, что отображение

$$(f, g) \to f\alpha + g\alpha'$$

есть взаимно однозначное отображение прямой суммы $L(\Delta_n) + L(\Delta_n)$ в $J(D-\Delta_n)$. В частности,

$$\dim J(D-\Delta_n) \geqslant 2 \dim L(\Delta_n) \text{ для всех } n. \qquad (*)$$

Осталось показать, что неравенство (*) ведет к противоречию, когда $n \to +\infty$. Левая часть равна

$$\dim J(D - \Delta_n) = i(D - \Delta_n).$$

По теореме 1 имеем

$$i(D - \Delta_n) = -\deg(D - \Delta_n) + g - 1 + l(D - \Delta_n) =$$
$$= n + (g - 1 - d) + l(D - \Delta_n).$$

Но для $n > d$ имеем $\deg(D - \Delta_n) < 0$, что, очевидно, дает

$$l(D - \Delta_n) = 0$$

(в противном случае существовал бы положительный дивизор D', линейно эквивалентный дивизору $D - \Delta_n$, что невозможно в силу предложения 1). Поэтому для больших n левая часть (*) равна $n + A_0$, где A_0 — константа.

Но правая часть равна $2l(\Delta_n)$, и теорема 1 показывает, что

$$l(\Delta_n) \geqslant \deg(\Delta_n) + 1 - g = n - g + 1.$$

Таким образом, правая часть (*) не меньше $2n + A_1$, где A_1 обозначает постоянную, и мы получаем противоречие для достаточно больших n.

Замечания. 1. Легко показать, что размерность пространства J равна в точности 1. Достаточно доказать существование ненулевого элемента в J. На самом деле мы докажем далее более точный результат, а именно, что J изоморфно пространству *дифференциалов* на кривой X.

2. Определения и результаты этого параграфа легко перенести на случай нормального проективного многообразия X произвольной размерности r. Если D — дивизор на многообразии X, то пространство $J(D)$ определяется как двойственное к $H^r(X, \mathscr{L}(D))$. Так как все группы H^{r+1} нулевые, точная последовательность групп когомологий показывает, что функтор H^r точен справа, и, если $D' \geqslant D$, имеем, кроме того, вложение $J(D')$ в $J(D)$. Индуктивный предел J пространств $J(D)$ является одномерным векторным пространством над полем $k(X)$. Это получается с помощью рассуждений, аналогичных применявшимся в предложении 4 (вместо Δ_n надо взять кратное сечение многообразия X гиперпло-

скостью). Отдельные результаты из теории пучков, которые используются при этом, элементарны и содержатся в АКП, п. 66. (Подробности см. в докладе Зарисского [3], стр. 139.)

7. Дифференциалы. Вычеты

Напомним кратко общее понятие *дифференциала* на алгебраическом многообразии X.

Прежде всего, если F—коммутативная алгебра над полем k, то известно, что́ такое *модуль k-дифференциалов* на F, обозначаемый через $D_k(F)$. Это F-модуль, снабженный k-линейным отображением

$$d{:}F \to D_k(F),$$

удовлетворяющим обычному условию $d(xy) = x \cdot dy + y \cdot dx$, где элементы $dx\ (x \in F)$ порождают модуль $D_k(F)$, причем $D_k(F)$ является „универсальным" модулем относительно предыдущих свойств (см. Картан и Шевалле [1], сообщение 13 Картье).

Все предыдущее применимо, в частности, к локальным кольцам $\mathcal{O}_P$ и полям рациональных функций $F = k(X)$ алгебраического многообразия X (произвольной размерности r); обращаясь к аффинному случаю, тотчас же проверяем, что модули $\underline{\Omega}_P = D_k(\mathcal{O}_P)$ образуют алгебраический когерентный пучок над X. Кроме того, имеем

$$D_k(F) = D_k(\mathcal{O}_P) \otimes_{\mathcal{O}_P} F.$$

Если P — простая точка многообразия X, а $t_1, \ldots, t_r$ образуют регулярную систему параметров в точке P, то dt_i образуют базис модуля $D_k(\mathcal{O}_P)$. Это видно, например, из следствия теоремы 5 сообщения 17 (Картан и Эйленберг [1]). Таким образом, пучок $\underline{\Omega}$ локально свободен над окрестностями простых точек многообразия X (следовательно, он соответствует расслоенному пространству с векторным слоем, двойственным пространству касательных векторов).

Обращаясь теперь к случаю *кривой* X, удовлетворяющей условиям п. 1, видим, что модуль $D_k(F)$ превращается в векторное пространство размерности 1 над полем $F = k(X)$, а пучок $\underline{\Omega}$ — в подпучок постоянного пучка $D_k(F)$. Если t — локальный параметр в точке P, дифференциал dt образует базис $\mathcal{O}_P$-модуля $\underline{\Omega}_P$, а также базис F-векторного пространства $D_k(F)$. Если $\omega \in D_k(F)$, то можно записать $\omega = f\,dt$, где $f \in F$. Считая, что $\omega \neq 0$, положим теперь

$$v_P(\omega) = v_P(t).$$

Сразу видно, что это определение *инвариантно*, т. е. не зависит от выбора локального параметра t. Оно применимо ко всякому рациональному сечению расслоенного пространства с векторным слоем размерности 1.

Из записи $\omega = f\,dt$ можно получить другой локальный инвариант дифференциала ω — его *вычет*. Пусть $\hat{F}_P$ обозначает пополнение поля F по нормированию v_P. Известно, что $\hat{F}_P$ изоморфно полю $k((T))$ формальных рядов над k, причем изоморфизм определяется отображением t на T. Если отождествить f с его образом в $\hat{F}_P$, то можно записать

$$f = \sum_{n \gg -\infty} a_n T^n, \qquad a_n \in k,$$

где символ $n \gg -\infty$ обозначает, что n принимает конечное число отрицательных значений.

В частности, определен коэффициент a_{-1} при T^{-1} у f. Этот коэффициент называется *вычетом* дифференциала $\omega = f\,dt$ в точке P и обозначается через $\operatorname{Res}_P(\omega)$. Это определение оправдывается следующим предложением.

Предложение 5 (инвариантность вычета). *Предыдущее определение вычета не зависит от выбора локального параметра t.*

Доказательство будет дано далее (п. 11) вместе с перечислением свойств отображения $\omega \to \operatorname{Res}_P(\omega)$. Заметим только, что $\operatorname{Res}_P(\omega) = 0$, если $v_P(\omega) \geqslant 0$, т. е. если у ω нет полюса в точке P. Так как каждый дифференциал имеет лишь конечное число полюсов (поскольку он является рациональным сечением векторного расслоения), то $\operatorname{Res}_P(\omega) = 0$ для почти всех P и сумма $\sum_{P \in X} \operatorname{Res}_P(\omega)$ имеет смысл. В связи с этим справедлив следующий фундаментальный результат.

Предложение 6 (формула вычетов). *Для каждого дифференциала* $\omega \in D_k(F)$ *имеем* $\sum_{P \in X} \operatorname{Res}_P(\omega) = 0$.

Доказательство будет дано далее (пп. 12 и 13). Это доказательство, как и доказательство предложения 5, очень просто в случае нулевой характеристики, но гораздо сложнее в случае характеристики $p > 0$. Однако в последнем случае можно дать совсем другое доказательство, используя операцию Картье (см. [1]).

В случае характеристики 0 можно, разумеется, воспользоваться трансцендентным методом. Действительно, в силу принципа Лефшеца можно предположить, что $k = \mathbf{C}$ ($\mathbf{C}$ — поле комплексных чисел). Кривая X естественным образом наделяется тогда структурой аналитического компактного комплексного многообразия размерности 1. Тотчас же проверяется, что $\operatorname{Res}_P \omega = (1/2\pi i) \oint_P \omega$. Это доказывает предложение 5; предложение 6 следует из формулы Стокса.

8. Теорема двойственности

Пусть ω — ненулевой дифференциал на кривой X. Определим *дивизор* (ω) той же формулой, что и в случае функций:

$$(\omega) = \sum_{P \in X} v_P(\omega) P,$$

где $v_P(\omega)$ определено в предыдущем параграфе.

Для дивизора D обозначим через $\Omega(D)$ векторное пространство, состоящее из 0 и дифференциалов $\omega \neq 0$, таких, что $(\omega) \geqslant D$. Очевидно, $\Omega(D)$ — подпространство пространства $D_k(F)$ всех дифференциалов на X.

Введя эти понятия, определим теперь скалярное произведение $\langle \omega, r \rangle$ между дифференциалом $\omega \in D_k(F)$ и распределением $r \in R$ следующей формулой:

$$\langle \omega, r \rangle = \sum_{P \in X} \operatorname{Res}_P(r_P \omega).$$

Это определение имеет смысл, так как $r_P \omega \in \underline{\Omega}_P$ для почти всех точек P. Определенное скалярное произведение обладает такими свойствами:

а) $\langle \omega, r\rangle = 0$, если $r \in F = k(X)$, в силу формулы вычетов (предложение 6);

б) $\langle \omega, r\rangle = 0$, если $r \in R(D)$ и $\omega \in \Omega(D)$, так как тогда имеем $r_P\omega \in \Omega_P$ для всех точек $P \in X$;

в) если $f \in F$, то $\langle f\omega, r\rangle = \langle \omega, fr\rangle$.

Для каждого дифференциала ω пусть $\theta(\omega)$ — линейная форма на R, которая переводит r в $\langle \omega, r\rangle$. Свойства а) и б) означают, что если $\omega \in \Omega(D)$, то $\theta(\omega) \in J(D)$, так как пространство $J(D)$ по определению двойственно к $R/(R(D) + k(X))$.

Теорема 2 (теорема двойственности). *Для всех дивизоров D отображение θ есть изоморфизм $\Omega(D)$ на $J(D)$ [другими словами, скалярное произведение $\langle \omega, r\rangle$ определяет двойственность векторных пространств $\Omega(D)$ и $I(D) = R/(R(D) + k(X))$].*

Докажем сначала следующую лемму.

Лемма 1. *Если ω — дифференциал, для которого $\theta(\omega) \in J(D)$, то $\omega \in \Omega(D)$.*

Действительно, в противном случае имеем такую точку $P \in X$, что $v_P(\omega) < v_P(D)$. Положим $n = v_P(\omega) + 1$ и пусть r — распределение с компонентами

$$\begin{cases} r_Q = 0 & \text{при} \quad Q \neq P; \\ r_P = \dfrac{1}{t^n}, & \text{где } t \text{ — локальный параметр в точке } P. \end{cases}$$

Имеем $v_P(r_P\omega) = -1$, откуда $\operatorname{Res}_P(r_P\omega) \neq 0$ и $\langle \omega, r\rangle \neq 0$. Но так как $n \leqslant v_P(D)$, имеем $r \in R(D)$, что приводит к противоречию, поскольку $\theta(\omega)$ предполагалось аннулирующим пространство $R(D)$.

Приступим теперь к доказательству теоремы 2. Прежде всего отображение θ *инъективно*. Действительно, если $\theta(\omega) = 0$, то предыдущая лемма показывает, что $\omega \in \Omega(\Delta)$ для всех дивизоров Δ, откуда, очевидно, получаем $\omega = 0$. Далее, отображение θ *сюръективно*. Действительно, в силу в) θ - F-линейное отображение $D_k(F)$ в J. Так как $D_k(F)$ размерности 1 и J размерности $\leqslant 1$ (предложение 4), θ отображает $D_k(F)$ на J. Поэтому если α — произвольный элемент пространства $J(D)$, то существует $\omega \in D_k(F)$, для которого $\theta(\omega) = \alpha$, и предыдущая лемма показывает, что $\omega \in \Omega(D)$.

Следствие. *Имеем* $i(D) = \dim \Omega(D)$. *В частности, род* $g = i(0)$ *равен размерности векторного пространства дифференциальных форм* ω, *таких, что* $(\omega) \geqslant 0$ (*формы „первого рода“*).

Отсюда получаем обычное определение рода.

9. Теорема Римана — Роха (окончательная форма)

Пусть ω и ω' — два ненулевых дифференциала. Так как пространство $D_k(F)$ одномерно над полем F, имеем $\omega' = f\omega$, где $f \in F^*$, откуда $(\omega') = (t) + (\omega)$. Таким образом, все дивизоры дифференциалов линейно эквивалентны и образуют один класс относительно линейной эквивалентности. Этот класс называется *каноническим классом* и обозначается через K. Часто через K обозначается также дивизор, принадлежащий этому классу.

Пусть теперь D — произвольный дивизор. Определим пространство $\Omega(D)$. Если $K = (\omega_0)$ — канонический дивизор, то все дифференциалы записываются в виде $\omega = f\omega_0$. Имеем $(\omega) \geqslant D$ тогда и только тогда, когда $(f) + (\omega_0) \geqslant D$, т. е. если $f \in L(K - D)$. Таким образом,

$$i(D) = \dim \Omega(D) = l(K - D),$$

и, объединяя этот результат с теоремой 1, получаем:

Теорема 3 (теорема Римана — Роха; окончательная форма). *Для всех дивизоров* D *имеем*

$$l(D) - l(K - D) = \deg(D) - g + 1.$$

Положим $D = K$ в этой формуле. Имеем $l(K) = i(0) = g$ и $l(0) = 1$, откуда $g - 1 = \deg K + 1 - g$. Поэтому

$$\deg(K) = 2g - 2.$$

Следствие. а) *Если* $\deg(D) \geqslant 2g - 1$, *то полная линейная система* $|D|$ *имеет размерность* $\deg(D) - g$.

б) *Если* $\deg(D) \geqslant 2g$, *то* $|D|$ *не имеет неподвижных точек.*

в) *Если* $\deg(D) \geqslant 2g+1$, *то система* $|D|$ *регулярна* (*т. е. определяет бирегулярное вложение* X *в проективное пространство*).

Если $\deg(D) \geqslant 2g-1$, то $\deg(K-D) \leqslant -1$, откуда $l(K-D)=0$ и $l(D)=\deg(D)+1-g$, что и доказывает а).

Предположим теперь, что $\deg(D) \geqslant 2g$ и что $|D|$ имеет неподвижную точку P. Тогда существует такая линейная система F, что дивизоры $|D|$ представимы в виде $P+H$, где H пробегает F. Таким образом, $\dim F = \dim|D|$, что противоречит а), так как $\deg(H)=\deg(D)-1$.

Предположим, наконец, что $\deg(D) \geqslant 2g+1$ и пусть $P \in X$. В силу б) линейная система $|D-P|$ есть система без неподвижных точек. Существует, следовательно, дивизор $\Delta \in |D|$, такой, что $v_P(\Delta)=1$. Если $\varphi\colon X \to \mathbf{P}_r(k)$ — отображение, соответствующее линейной системе $|D|$ (см. п. 3), то это означает, что существует гиперплоскость $H \subset \mathbf{P}_r(k)$, для которой $\varphi^{-1}(H)$ содержит точку P с коэффициентом 1. В результате получается, во-первых, что $\varphi\colon X \to \varphi(X)$ — отображение степени 1, а во-вторых, что $\varphi(P)$ — простая точка $\varphi(X)$. Отображение будет, следовательно, изоморфизмом.

Относительно других приложений теоремы Римана — Роха (например, о „точках Вейерштрасса") см. трактат Севери [1].

10. Замечания к теореме двойственности

Из того факта, что $i(K)=l(0)=1$, следует, что векторное пространство $H^1(X, \mathscr{L}(K))$ одномерно. То же самое верно, следовательно, и для $H^1(X, \underline{\Omega})$, поскольку пучок $\underline{\Omega}$ изоморфен пучку $\mathscr{L}(K)$. Действительно, истолковывая последний изоморфизм как двойственность между $H^1(X, \mathscr{L}(K))$ и $\Omega(K)=L(0)$, видим, что группа когомологий $H^1(X, \mathscr{L}(K))$ является *канонической* базой, другими словами, *канонически изоморфна* полю k.

Скалярное произведение $\langle \omega, r \rangle$ между элементами пространств $\Omega(D)=H^0(X, \underline{\Omega}(D))$ и $I(D)=H^1(X, \mathscr{L}(D))$ можно теперь интерпретировать как $\cup$-*произведение* со значениями в пространстве $H^1(X, \underline{\Omega})$, а теорема двойственности утверждает, что это произведение устанавливает двойственность между двумя пространствами. В этом виде теорему можно распространить на произвольный алгебраический когерентный пучок $\mathcal{F}$. Если положить $\mathcal{F}' = \mathrm{Hom}(\mathcal{F}, \underline{\Omega})$, то $\cup$-произведение отображает $H^1(X, \mathcal{F}) \times H^0(X, \mathcal{F}')$ в $H^1(X, \underline{\Omega})$ и устанавливает двойственность между двумя первоначальными пространствами.

Отметим, что теорема 2, как и ее доказательство, без больших изменений распространяется на нормальные многообразия произвольной размерности r. Пучок $\underline{\Omega}$ надо тогда заменить пучком $\underline{\Omega}^r$ дифференциальных форм степени r, не имеющих полюсов. С помощью рекуррентных соотношений относительно r доказывается, что $H^r(X, \underline{\Omega}^r)$ канонически изоморфно k. Благодаря этому факту $\cup$-произведение определяет скалярное произведение на $H^r(X, \mathcal{L}(D)) \times \times H^0(X, \underline{\Omega}^r(D))$, а следовательно, линейное отображение θ пространства $H^0(X, \underline{\Omega}^r(D))$ в двойственное к $H^r(X, \mathcal{L}(D))$ пространство $J(D)$. Рассуждения теоремы 2 показывают тогда, что θ — изоморфизм. Относительно дальнейших подробностей см. упоминавшийся доклад Зарисского.

11. Доказательство инвариантности вычета

Остальная часть этой главы посвящена доказательству предложений 5 и 6, сформулированных в п. 7. Начнем с предложения 5.

Речь идет о *локальном* вопросе, касающемся дифференциалов поля $\hat{F}_P$. Это поле будет обозначаться через K на всем протяжении этого пункта. Выбор локальной униформизующей t отождествляет K с $k((t))$. Обозначим через v нормирование поля K, через $\mathcal{O}$ — кольцо нормирования (множество $f \in K$, таких, что $v(t) \geqslant 0$) и через $\mathfrak{m}$ — идеал нормирования (множество $f \in K$, таких, что $v(t) > 0$). Очевидно, что $\mathcal{O} = \hat{\mathcal{O}}_P$ и $\mathfrak{m} = \hat{\mathfrak{m}}_P$.

Модуль $D_k(F)$ дифференциалов поля K определяется способом, описанным в п. 7. В силу того, что при этом способе определения не учитывается нормирование поля K, модуль получается (в случае характеристики 0) „слишком большим“ — векторным пространством бесконечной размерности над K. Удобно перейти к ассоциированному сепарабельному модулю (относительно $\mathfrak{m}$-топологии), полагая

$$D'_k(K) = D_k(K)/Q, \quad \text{где} \quad Q = \bigcap_{n \geqslant 0} \mathfrak{m}^n d(\mathfrak{O}).$$

Так получаемый модуль уже не обладает патологическими свойствами:

Лемма 2. *Пусть t — локальный параметр. Для всех элементов $f = \sum_{n \geqslant -\infty} a_n t^n \in K$ положим $f'_t = \sum n a_n t^{n-1}$. Тогда $df = f'_t\, dt$ и dt образует базис $D'_k(K)$ над K.*

Для того чтобы показать, что $df = f'_t\, dt \in D'_k(K)$, достаточно убедиться, что для всех целых $N \geqslant 0$ имеем $df - f'_t\, dt \in \mathfrak{m}^N d(\mathfrak{O}) \subset D_k(K)$. Записав

$$f = f_0 + t^{N+1} f_1, \quad \text{где} \quad f_0 = \sum_{n \leqslant N} a_n t^n, \quad f_1 \in \mathfrak{O},$$

$$f'_t = (f_0)'_t + t^N g, \quad \text{где} \quad g \in \mathfrak{O},$$

получаем

$$df - f'_t\, dt = (N+1) t^N f_1\, dt + t^{N+1}\, df_1 - t^N g\, dt.$$

Так как последние три члена принадлежат $\mathfrak{m}^N d(\mathfrak{O})$, это доказывает первое утверждение леммы.

Таким образом, dt порождает векторное K-пространство $D'_k(K)$. Для доказательства того, что он образует базис, достаточно показать, что $D'_k(K) \neq 0$, т. е. что существует дифференцирование поля K, не равное тождественно нулю, продолжение которого на $D_k(K)$ аннулирует Q. Дифференцирование $D: K \to K$, определенное равенством $Df = f'_t$, удовлетворяет этим условиям. Действительно, оно не равно тождественно нулю и отображает $\mathfrak{m}^{N+1} d(\mathfrak{O})$ в $\mathfrak{m}^N$, причем Q в $\bigcap \mathfrak{m}^N = 0$.

Начиная с этого момента, *дифференциалом* поля K называется элемент из $D'_k(K)$. Если ω — такой дифференциал и t — локальный параметр, то $\omega = f\,dt$, где $f \in K$. Если $f = \sum a_n t^k$, то коэффициент a_{-1} при dt/t называется *вычетом* ω (по отношению к t) и обозначается через $\operatorname{Res}_t(\omega)$. Предложение 5 можно теперь переформулировать следующим образом.

Предложение 5′. *Если t и u — два локальных параметра поля K, то $\operatorname{Res}_t(\omega) = \operatorname{Res}_u(\omega)$ для всех дифференциалов $\omega \in D'_k(K)$.*

Отметим сначала некоторые свойства операции $\operatorname{Res}_t(\omega)$:

1) $\operatorname{Res}_t(\omega)$ *k-линейна относительно* ω;

2) $\operatorname{Res}_t(\omega) = 0$ *при* $v(\omega) \geqslant 0$ (*т. е. при* $\omega \in \mathfrak{O}\,dt$);

3) $\operatorname{Res}_t(dg) = 0$ *для всех* $g \in K$;

4) $\operatorname{Res}_t(dg/g) = v(g)$ *для всех* $g \in K^*$.

Свойства 1), 2), 3) очевидны. Чтобы доказать свойство 4), положим $g = t^n w$, где $n = v(g)$, откуда $v(w) = 0$. Имеем

$$dg/g = n\,dt/t + dw/w,$$

откуда $\operatorname{Res}_t(dg/g) = n + \operatorname{Res}_t(dw/w)$ в соответствии с 2).

Перейдем теперь к доказательству предложения 5′. Запишем дифференциальную форму ω в виде

$$\omega = \sum_{n \geqslant 0} a_n\,du/u^n + \omega_0, \quad \text{где} \quad v(\omega_0) \geqslant 0.$$

Имеем $\operatorname{Res}_u(\omega) = a_1$ и $\operatorname{Res}_t(\omega) = \sum a_n \operatorname{Res}_t(du/u^n)$.

Так как $\operatorname{Res}_t(du/u) = 1$ в силу 4), то остается доказать следующую формулу:

5) $\operatorname{Res}_t\left(\dfrac{du}{u^n}\right) = 0$ *для* $n \geqslant 2$.

В случае поля k характеристики нуль имеем $du/u^n = dg$, где $g = -1/(n-1)\,n^{n-1}$, и формула 5) есть простое следствие формулы 3). Это рассуждение неприменимо к случаю характеристики $p > 0$, так как может случиться, что $n - 1 \equiv 0 \pmod p$. Однако случай характеристики p можно свести к случаю характеристики нуль следующим способом.

Прежде всего можно предположить, умножив u на скалярный множитель, что

$$u = t + a_2 t^2 + a_3 t^3 + \ldots = t(1 + a_2 t + a_3 t^2 + \ldots),$$

откуда получаем

$$\frac{1}{u^n} = \frac{1}{t^n}(1 - na_2t + \ldots + b_it^i + \ldots),$$

где b_i — полиномы от $a_2, \ldots, a_{i+1}$ с коэффициентами в $\mathbf{Z}$, не зависящие от характеристики (целое число n фиксировано). При умножении на $du = dt + 2a_2t\,dt + \ldots + ia_it^{i-1}\,dt + \ldots$ получаем

$$\frac{du}{u^n} = \frac{dt}{t^n}\sum_{i=0}^{\infty} c_it^i,$$

где коэффициенты c_i, как и прежде, суть полиномы от $a_2, \ldots, a_{i+1}$ с коэффициентами из $\mathbf{Z}$, не зависящие от характеристики.

В частности, $c_{i-1} = \mathrm{Res}_t(du/u^n)$. Поскольку формула 5) верна в случае характеристики нуль, полиномы $c_{n-1}(a_2, \ldots, a_n)$ равны нулю, когда аргументы a_i берутся из поля характеристики нуль. В силу *принципа продолжения алгебраических тождеств* (Бурбаки Н., Алгебра, гл. IV, § 2, п. 5) этот полином равен тождественно нулю, откуда следует 5) в общем случае. Предложение 5′ доказано.

Замечание. Ссылку на принцип продолжения алгебраических тождеств легко заменить „*функториальным*“ рассуждением. Вводя для всех коммутативных колец A алгебру $K_A = A((t))$ и ее модуль дифференциалов $D'_A(K_A)$, имеем гомоморфизм Res_t: $D'_A(K_A) \to A$, коммутирующий с гомоморфизмом $A \to B$. Тогда доказываем формулу 5) для $u = t + \sum_{i \geqslant 2} a_it^i$ в три этапа:

а) для случая когда A — поле характеристики 0 (методом, изложенным в тексте);

б) для случая когда A — область целостности характеристики нуль [погружением A в поле частных и использованием а)];

в) для произвольного A (записывая A как факторкольцо полиномов над $\mathbf{Z}$ и применяя б) к последнему кольцу).

Восстановление всех деталей этого доказательства предоставляем читателю.

12. Доказательство формулы вычетов

Начнем с проверки формулы в частном случае.

Лемма 3. *Формула вычетов верна в случае, когда X — проективная прямая.*

В этом случае тождественное отображение $X \to X$ есть функция t на X и $k(X) = k(t)$. Все дифференциалы ω на X записываются в виде $\omega = f(t)\,dt$, где $f(t)$ — рациональная функция от t. Раскладывая f на простейшие дроби (Бурбаки, Алгебра, гл. VII, § 2, п. 3), видим, что можно считать $f = t^n$ или $f = 1/(t-a)^n$.

В первом случае единственный полюс ω — бесконечно удаленная точка. Если положить $u = 1/t$, то $\omega = -du/u^{n+2}$, откуда $\operatorname{Res}_\infty(\omega) = 0$, и сумма вычетов равна нулю.

Во втором случае, если $n = 1$, $\omega = dt/(t-a)$ имеет полюсы a и ∞ с вычетами 1 и -1 соответственно. Если $n \geqslant 2$, точка a — единственный полюс с нулевым вычетом. Следовательно, формула вычетов проверена во всех случаях.

Пусть теперь X — произвольная кривая. Выберем функцию φ на X, отличную от константы. Если X' обозначает проективную прямую $\mathbf{P}_1(k)$, то можно рассматривать φ как отображение $X \to X'$ (на X'). Это отображение превращает X в „накрытие“ кривой X', возможно разветвленное. Если положить $E = k(X')$ и $F = k(X)$, то отображение φ определяет погружение поля E в поле F. Поле E отождествляется, таким образом, с полем $k(\varphi)$, порожденным φ. Так как кривая X имеет размерность 1, имеем $[F : F^p] = p$. Если F' обозначает максимальное сепарабельное расширение E, содержащееся в F, то, следовательно, существует такое целое n, что $F' = F^{p^n}$. Расширение F/E *сепарабельно* тогда и только тогда, когда $n = 0$, другими словами, если $\varphi \notin F^p$. В дальнейшем это всегда будет предполагаться.

Если f — элемент поля F, то определен его *след* в F/E. Это элемент поля E, обозначаемый через $\operatorname{Tr}_{F/E}(t)$. Операция взятия следа может быть распространена на дифференциалы F следующим образом.

Отображение $E \to F$ определяет гомоморфизм $D_k(E)$ в $D_k(F)$. Так как $d\varphi$ есть E-база $D_k(E)$ и $\varphi \notin F^p$, предыдущий гомоморфизм инъективен и продолжается до изоморфизма $D_k(E) \underset{E}{\otimes} F$ на $D_k(F)$. С другой стороны, операция $\mathrm{Tr}_{F/E}\colon F \to E$ E-линейна. Применяя этот гомоморфизм ко второму члену в $D_k(F) \underset{E}{\otimes} F$, видим наконец, что отображение $\mathrm{Tr}_{F/E}\colon D_k(F) \to D_k(E)$ E-линейно. Можно пояснить это отображение таким образом: если ω — дифференциал кривой X, записанный в виде $\omega = f\,d\varphi$, то

$$\mathrm{Tr}_{F/E}(\omega) = \left(\mathrm{Tr}_{F/E}(f)\right) d\varphi.$$

Итак, всем дифференциалам ω кривой X соответствуют дифференциалы $\mathrm{Tr}(\omega)$ кривой $X' = \mathbf{P}_1(k)$. Эта операция обладает следующим свойством:

Лемма 4. *Для всех точек $P \in X'$ имеем*

$$\sum_{Q \to P} \mathrm{Res}_Q(\omega) = \mathrm{Res}_P(\mathrm{Tr}(\omega)),$$

причем сумма распространяется на все точки $Q \in X$, такие, что $\varphi(Q) = P$.

Из лемм 3 и 4 вытекает формула вычетов. Действительно, если ω — дифференциал на X, то лемма 4 показывает, что

$$\sum_{Q \in X} \mathrm{Res}_Q(\omega) = \sum_{P \in X'} \mathrm{Res}_P(\omega'),$$

где $\omega' = \mathrm{Tr}(\omega)$, а из леммы 3 следует, что последняя сумма равна нулю.

Остается доказать лемму 4. Наше высказывание „полулокальное“, т. е. локальное относительно X', но не X. Начнем со сведе́ния доказательства к чисто локальному утверждению.

Пусть $\widehat{E}_P$ — пополнение E по нормированию v_P, а $\widehat{F}_Q$ — пополнения F по нормированиям v_Q, соответствующим точкам Q, проектирующимся в P. Нормирования v_Q продолжают v_P в следующем смысле: существуют целые числа e_Q, такие, что $v_Q = e_Q v_P$ на E. Наоборот, все нормирования поля F, продолжающие v_P, совпадают с одним из нормирований v_Q. Мы оказались, таким образом, в ситуации, типичной для „разложения" нормирования; $\hat{F}_Q$ — расширение поля $\hat{E}_P$ степени e_Q и имеется канонический изоморфизм (см., например, Шевалле [1], стр. 113)

$$F \underset{E}{\otimes} \hat{E}_P \cong \prod_{Q \to P} \hat{F}_Q.$$

Этот изоморфизм немедленно дает формулу для следов

$$\mathrm{Tr}_{F/E}(t) = \sum_{Q \to P} \mathrm{Tr}_Q(t), \qquad f \in F,$$

где Tr_Q обозначает след расширения $\hat{F}_Q/\hat{E}_P$. Отсюда получаем в силу аддитивности вычетов

$$\mathrm{Res}_P(\mathrm{Tr}(f)\,d\varphi) = \sum_{Q \to P} \mathrm{Res}_P(\mathrm{Tr}_Q(f)\,d\varphi).$$

Последняя формула сводит лемму 4 к следующей:

Лемма 5. *Для всех* $f \in \hat{F}_Q$ *имеем*

$$\mathrm{Res}_Q(f\,d\varphi) = \mathrm{Res}_P(\mathrm{Tr}_Q(f)\,d\varphi).$$

Доказательство этой леммы см. в следующем пункте.

Замечания. 1. В предыдущей редукции совсем не используется предположение о том, что X' — проективная прямая; тем самым дается доказательство леммы 4, годное для любого сепарабельного накрытия $X \to X'$.

2. Следуя Хассе, мы вывели формулу вычетов из леммы 4. Отметим, что возможно обратное: из формулы вычетов (доказанной трансцендентным методом, либо с использованием операции Картье, либо каким-нибудь другим методом) легко вывести лемму 4. Можно даже распространить ее на несепарабельные накрытия при помощи подходящего определения следа дифференциала (использованное выше определение уже не годится). Мы возвратимся к этому в гл. III, п. 3.

13. Доказательство леммы 5

Как и в предложении 5, вопрос носит *локальный* характер. Имеем поле формальных рядов K и конечное сепарабельное расширение L/K. Если t (соответственно u)

обозначает локальный параметр поля L (соответственно K), то надо установить формулу

$$\mathrm{Res}_t(f\,du) = \mathrm{Res}_u(\mathrm{Tr}(f)\,du) \quad \text{для всех} \quad f \in L. \qquad (*)$$

Впрочем, можно ограничиться случаем, когда f имеет вид t^n, где $n \in \mathbf{Z}$.

Предположим сначала, что *характеристика поля K равна нулю*. Если обозначить через e степень L/K, то $v_L(u) = e$. Это показывает, что $u = w^e$, где w — локальный параметр поля L. Заменяя t на w, видим, что *можно предполагать* $u = t^e$. Таким образом, мы имеем дело с циклическим расширением, в котором вычисление следа не представляет труда. Имеем

$$\mathrm{Tr}(t^n) = \begin{cases} 0 & \text{при} \quad n \not\equiv 0 \pmod e; \\ eu^{n/e} & \text{при} \quad n \equiv 0 \pmod e. \end{cases}$$

Отсюда

$$\mathrm{Res}_u(\mathrm{Tr}(t^n)\,du) = \begin{cases} 0 & \text{при} \quad n \neq -e; \\ e & \text{при} \quad n = -e. \end{cases}$$

С другой стороны, имеем

$$\mathrm{Res}_t\left(t^n\,du\right) = \mathrm{Res}_t\left(et^{n+e-1}\,dt\right) = \begin{cases} 0 & \text{при} \quad n \neq -e; \\ e & \text{при} \quad n = -e, \end{cases}$$

что приводит к тому же результату.

Теперь перейдем к общему случаю. Можно записать

$$u = t^e + \sum_{i > e} a_i t^i. \qquad (**)$$

Наоборот, эта формула определяет такое подполе $k((u))$ поля $k((t))$, что $[k((t)) : k((u))] = e$. Расширение $k((t))/k((u))$ сепарабельно тогда и только тогда, когда $u \notin k((t^p))$.

Формула (**) делает очевидным тот факт, что система $\{1, t, t^2, \ldots, t^{e-1}\}$ образует *базис* $k((t))/k((u))$. Для всех $n \in \mathbf{Z}$ можно, таким образом, написать

$$t^n \cdot t^i = \sum_{j=0}^{e-1} b_{n,i,j}(u)\,t^j \,(0 \leqslant i < e-1),$$

где $b_{n,i,j}$ — формальные ряды от u:

$$b_{n,i,j}(u) = \sum b_{n,i,j,k} u^k.$$

Для фиксированного n $b_{n,i,j}$ образуют матрицу, соответствующую t^n в *регулярном представлении* $k((t))/k((u))$. В силу определения следа имеем, следовательно, $\mathrm{Tr}(t^n) = \sum_{i=0}^{e-1} b_{n,i,i}(u)$, и вычет $c_n = \mathrm{Res}(\mathrm{Tr}(t^n)\,du)$ задается формулой

$$c_n = \sum_{i=0}^{e-1} b_{n,i,i-1}.$$

С другой стороны, сразу же видно, что $\mathrm{Res}(t^n\,du) = -na_{-n}$ (положив $a_e = 1$ и $a_i = 0$ при $i < e$). Поэтому доказываемая формула эквивалентна утверждению

$$c_n = -na_{-n} \quad \text{для всех} \quad n \in \mathbf{Z}. \qquad (***)$$

Но предыдущие вычисления можно провести, считая a_i неопределенными величинами. Следовательно, $b_{n\,i,j,k}$ — *полиномы* от a_i с коэффициентами в Z, не зависящие от характеристики. То же самое относится к $c_n + na_{-n}$. Как было показано выше, эти полиномы обращаются в нуль, когда аргументам придаются значения из алгебраически замкнутого поля характеристики нуль. Применяя принцип продолжения алгебраических тождеств, получаем, что эти многочлены тождественно равны нулю. Это дает доказательство леммы 5, а тем самым и формулы вычетов.

Библиографические замечания

Имеется много работ, посвященных алгебраическим кривым Мы ограничимся указанием трудов Севери [1], Г. Вейля [1], Шевалле [1] и А. Вейля [4], которые дают достаточное представление о возможных точках зрения по этому вопросу. Лекции Севери изложены в стиле итальянской геометрической школы; они содержат много интересных результатов о линейных системах, проективных погружениях и автоморфизмах алгебраических кривых. Г. Вейль стоит на точке зрения „аналитической геометрии", выходя тем самым из чисто алгебраических рамок; именно, он доказывает теорему об униформизации, а также то, что всякая компактная риманова поверхность алгебраическая. Известно, что последний результат приводит к нахождению накрытий алгебраической кривой, имеющей заданные ветвления (теорема существования Римана). Алгебро-геометрические методы не дают возможности получить последний результат.

Севери и Г. Вейль ограничиваются классическим случаем, беря за основное поле комплексных чисел C. У Шевалле и А. Вейля основное поле произвольное. Это почти единственное, что есть общего у этих двух авторов: Шевалле пишет в чисто алгебраическом стиле (он всегда говорит о полях, а не о кривых), тогда как А. Вейль использует более геометрический язык „Оснований“ [3].

Какова бы ни была принятая точка зрения, центральной всегда является теорема Римана — Роха. Доказательство, данное нами, использует распределения, которые введены А. Вейлем в письме к Хассе [1]. Это доказательство (довольно короткое) имеет еще то преимущество, что его легко перевести на язык пучков, подготавливая тем самым путь к обобщениям на многообразия произвольной размерности (см. гл. IV, случай поверхностей). Любопытно отметить, что такое доказательство имеется в работе Шевалле [1], а у А. Вейля [4] его нет.

Как мы видели, формула вычетов играет основную роль в отождествлении дифференциалов с линейными формами на распределениях („теорема двойственности“). Первое доказательство этой формулы (для полей произвольной характеристики) принадлежит Хассе [3]; по существу его доказательство и воспроизведено нами. Работа Шевалле [1] содержит другое доказательство, хотя и довольно окольное, но обходящееся без трудоемкой леммы 5 (см. также Ленг [4], гл. X, § 5). Имеется, впрочем, другое доказательство этой леммы в заметке Уэплса [1].

Несмотря на различия, все эти доказательства довольно искусственны. Здесь, как и в других вопросах (см. замечание к гл. IV), по-видимому, нельзя получить действительно естественного доказательства, если не встать на точку зрения общей „теоремы двойственности“ Гротендика [2].

ГЛАВА

III

ОТОБРАЖЕНИЯ КРИВОЙ В КОММУТАТИВНУЮ ГРУППУ

Эта глава посвящена доказательству первой теоремы, сформулированной в гл. I, о существовании модуля, соответствующего рациональному отображению алгебраической кривой в алгебраическую коммутативную группу.

Собственно доказательству посвящен § 2. В § 1 мы проводим общее изучение „локальных символов“ и находим значение этих символов в частных случаях. Наконец, § 3 содержит некоторые вспомогательные результаты, которые более или менее общеизвестны, но на которые трудно дать удовлетворительные ссылки.

§ 1. Локальные символы

1. Определения

Пусть X — алгебраическая кривая (удовлетворяющая условиям гл. II, обозначения которой сохраняются). Если S — конечное подмножество X, то *модулем* с носителем S мы называем задание для всех $P \in S$ целого числа $n_P > 0$. Модуль $\mathfrak{m}$ часто будет отождествляться с положительным дивизором $\sum n_P P$.

Пусть g — рациональная функция на X. Мы пишем

$$g \equiv 1 \bmod \mathfrak{m},$$

если $v_P(1-g) \geqslant n_P$ для всех $P \in S$.

Если предыдущее неравенство выполняется только в точке P, то мы пишем

$$g \equiv 1 \bmod \mathfrak{m} \text{ в } P.$$

Заметим, что если $g \equiv 1 \bmod \mathfrak{m}$, то дивизор (g) не содержит точек из S.

Пусть теперь $f\colon X - S \to G$ — отображение дополнения S в коммутативную группу G. (Заметим, что мы *не предполагаем* ни того, что G — алгебраическая группа, ни того, что f — рациональное отображение.) Отображение f продолжается по линейности до гомоморфизма группы дивизоров, равных нулю на S, в группу G. В частности, если $g \equiv 1 \bmod \mathfrak{m}$, то определен элемент $f((g)) \in G$, и если записывать группу G аддитивно, то

$$f((g)) = \sum_{P \in X-S} v_P(g) f(P).$$

Определение 1. *Мы говорим, что $\mathfrak{m}$ — модуль для отображения f (или что $\mathfrak{m}$ — ассоциирован с f), если $f((g)) = 0$ для всех функций $g \in k(X)$, таких, что $g \equiv 1 \bmod \mathfrak{m}$.*

Мы преобразуем это определение с помощью понятия „локального символа".

Определение 2. *Пусть $\mathfrak{m}$ — модуль с носителем S и f — отображение $X - S$ в G. „Локальным символом", соответствующим f и $\mathfrak{m}$, мы называем задание для всех $P \in X$ и всех $g \in k(X)^*$ элемента из G, обозначаемого $(f, g)_P$, удовлетворяющего следующим четырем условиям:*

1) $(f, gg')_P = (f, g)_P + (f, g')_P$;

2) $(f, g)_P = 0$ *при* $P \in S$ *и* $g \equiv 1 \bmod \mathfrak{m}$ *в* P;

3) $(f, g)_P = v_P(g) f(P)$ *при* $P \in X - S$;

4) $\sum_{P \in X} (f, g)_P = 0$.

Примеры таких символов будут приведены в пп. 3 и 4.

Предложение 1. *Для того чтобы $\mathfrak{m}$ был модулем для отображения f, необходимо и достаточно, чтобы существовал локальный символ, ассоциированный с f* и $\mathfrak{m}$, *причем этот символ определен тогда однозначно.*

Предположим, что локальный символ существует, и пусть g — такая функция, что $g \equiv 1 \bmod \mathfrak{m}$. Имеем

$$f((g)) = \sum_{P \notin X} v_P(g) f(P) =$$

$$= \sum_{P \notin S} (f, g)_P \qquad \text{по свойству } 3),$$

$$= -\sum_{P\in S}(f, g)_P \quad \text{по свойству} \quad 4),$$
$$= 0 \quad \text{по свойству} \quad 2).$$

Обратно, предположим, что $\mathfrak{m}$ — модуль для f. Попытаемся определить локальный символ $(f, g)_P$. Если $P \notin S$, то условие 3) дает $(f, g)_P = v_P(g)\, f(P)$. Предположим теперь, что $P \in S$. Всегда можно найти вспомогательную функцию g_P, такую, что $g_P \equiv 1 \bmod \mathfrak{m}$ в точках $Q \in S - P$ и $g/g_P \equiv 1 \bmod \mathfrak{m}$ в P (существование g_P следует, например, из теоремы о независимости нормирований)[1]. Определим $(f, g)_P$ формулой

$$(f, g)_P = -\sum_{D\notin S} v_Q(g_P)\, f(Q). \qquad (*)$$

Правая часть не зависит от выбора вспомогательных функций g_P. Действительно, можно умножать g_P лишь на функцию h, такую, что $h \equiv 1 \bmod \mathfrak{m}$, а это не изменяет суммы в силу того, что $f((h)) = 0$.

Формула (*), следовательно, однозначно определяет $(f, g)_P$ при $P \in S$. Остается убедиться теперь, что выполняются свойства 1) — 4).

Проверка свойства 1). Если g_P и g'_P — вспомогательные функции для g и g' соответственно, то можно принять $g_P g'_P$ за вспомогательную функцию для gg', чем формула тотчас же проверяется.

Проверка свойства 2). Если $g \equiv 1 \bmod \mathfrak{m}$ в P, то $g_P \equiv 1 \bmod \mathfrak{m}$, и правая часть в (*) равна $-f((g_P)) = 0$, поскольку $\mathfrak{m}$ — модуль для f.

Проверка свойства 3). Это следует из определения $(f, g)_P$ при $P \notin S$.

---

[1]) Эта теорема утверждает следующее: если $P_1, \ldots, P_n$ — конечный набор точек кривой X, а $m_1, \ldots, m_n$ — целые числа, то существует функция $f \in k(X)$, такая, что $v_{P_i}(t) = m_i$ для всех P_i (см. Шевалле [1], гл. I, § 6). — *Прим. перев.*

Проверка свойства 4). Имеем

$$\sum_{P\in S}(f,\ g)_P = -\sum_{P\in S}\ \sum_{Q\notin S} v_Q(g_P)\, f(Q) =$$
$$= -\sum_{Q\notin S} v_Q(h)\, f(Q),\ \text{где}\ h = \prod_{P\in S} g_P.$$

Если положить $g/h = k$, то очевидно, что $k \equiv 1 \pmod{\mathfrak{m}}$. Отсюда

$$\sum_{Q\notin S} v_Q(k)\, f(Q) = 0,$$

поскольку $\mathfrak{m}$ — модуль для f. Верхнее равенство можно поэтому записать в виде

$$\sum_{P\in S}(f,\ g)_P = -\sum_{Q\notin S} v_Q(g)\, f(Q) + \sum_{Q\notin S} v_Q(k)\, f(Q) =$$
$$= -\sum_{Q\notin S} v_Q(g)\, f(Q) =$$
$$= -\sum_{Q\notin S} (f,\ g)_Q\ \text{по свойству 3)}.$$

Таким образом, выражение (*) — локальный символ, соответствующий $\mathfrak{m}$ и f. Этот символ единственно возможный, так как

$$(f,\ g)_P = (f,\ g_P)_P,$$

и в силу 2) — 4) $(f,\ g_P)_P$ должен быть равен правой части формулы (*). Следовательно, предложение 1 доказано.

Замечание. Если отображение $f\colon X - S \to G$ имеет модуль $\mathfrak{m}$, то оно имеет также и другие модули (например, $\mathfrak{m}' \geqslant \mathfrak{m}$), но соответствующие локальные символы будут те же самые. Действительно, можно ограничиться случаем, когда $\mathfrak{m}' \geqslant \mathfrak{m}$. В этом случае локальный символ для $\mathfrak{m}$ совпадает с символом для $\mathfrak{m}'$ по доказанному свойству единственности. Таким образом, локальный символ, если он существует, *зависит только от* f.

Интерпретация в терминах иделей. Предыдущее изложение легко переводится на язык „иделей“ Шевалле. Укажем, каким образом это делается.

Пусть I — группа иделей X, т. е. мультипликативная группа обратимых элементов кольца распределений R (гл. II, п. 5). Обозначим через F поле $k(X)$ и для любого $P \in X$ пусть U_P — подгруппа F^*, образованная функциями g, такими, что $v_P(g)=0$. Для $n \geqslant 1$ обозначим через $U_P^{(n)}$ подгруппу U_P, образованную такими функциями, что $v_P(1-g) \geqslant n$. При этих обозначениях идель a есть семейство $\{a_P\}_{P \in X}$ элементов F^*, таких, что $a_P \in U_P$ для почти всех P. Пусть $(f, g)_P$ — локальный символ. Положим для иделя a

$$\theta(a) = \sum (f, a_P)_P, \text{ где } a = \{a_P\}_{P \in X}.$$

Из того, что $a_P \in U_P$ для почти всех P, следует, что эта сумма конечна. Получим, таким образом, гомоморфизм θ: $I \to G$. Задание этого гомоморфизма, впрочем, *эквивалентно* заданию локального символа $(f, g)_P$, с которого мы начали. Условия 2) и 3) означают, что $\theta = 0$ на подгруппе $I_\mathfrak{m} \subset I$, определяемой формулой

$$I_\mathfrak{m} = \prod_{P \in S} U_P^{(n_P)} \times \prod_{P \notin S} U_P, \quad \text{если} \quad \mathfrak{m} = \sum n_P P.$$

Условие же 4) означает, что θ аннулирует подгруппу $F^* \subset I$, образованную главными иделями. Таким образом, θ — гомоморфизм $I/I_\mathfrak{m}F^*$ в G (и наоборот, всего моморфизмы $I/I_\mathfrak{m}F^*$ в G получаются таким способом). Легко видеть, используя теорему о независимости нормирований, что группа $I/I_\mathfrak{m}F^*$ канонически изоморфна группе $C_\mathfrak{m}$, введенной в гл. I, п. 1; это, впрочем, является содержанием предложения 1.

2. Основные свойства локальных символов

а) *Функториальный характер.* Пусть f: $X - S \to G$ — отображение $X - S$ в коммутативную группу G и θ: $G \to G'$ — гомоморфизм G в коммутативную группу G'. Тогда имеет место

Предложение 2. *Если $\mathfrak{m}$ — модуль для f, то он будет также модулем для $\theta \circ f$ и соответствующие локальные символы удовлетворяют формуле*

$$(\theta \circ f, g)_P = \theta((f, g)_P).$$

Достаточно проверить, что $\theta((f, g)_P)$ — **локальный символ**, ассоциированный с $\theta \circ f$ и $\mathfrak{m}$, другими словами, что выполняются свойства 1) — 4). Это делается непосредственно.

б) *Локальный символ следа.* Рассмотрим опять f: $X - S \to G$ и предположим, что π: $X \to X'$ — отображение X на другую кривую X' (можно, следовательно, рассматривать X как „разветвленное накрытие“ X'; ср. гл. II, п. 12). Положим $S' = \pi(S)$ и для всех $P' \in X'$ обозначим через $\pi^{-1}(P')$ дивизор X, являющийся прообразом P' при π. Имеем

$$\pi^{-1}(P') = \sum_{P \to P'} e_P P,$$

где e_P обозначает индекс ветвления нормирования v_P по отношению к нормированию $v_{P'}$.

Если $P' \in S'$, то дивизор $\pi^{-1}(P')$ равен нулю на S [1]), и выражение $f(\pi^{-1}(P'))$ имеет смысл. Имеем, таким образом, отображение

$$\mathrm{Tr}_\pi f\colon\ X' - S' \to G,$$

которое будет называться *следом* отображения f.

Предложение 3. *Если f обладает модулем $\mathfrak{m}$, то отображение $f' = \mathrm{Tr}_\pi f$ обладает модулем $\mathfrak{m}'$ и*

$$(\mathrm{Tr}_\pi f, g')_{P'} = \sum_{P \to P'} (f, g' \circ \pi)_P, \quad P' \in X', \ g' \in k(X')^*.$$

Необходимо показать, что выражение $(f', g')_{P'}$, определенное выше, удовлетворяет условиям 1) — 4) для f' и подходящего модуля $\mathfrak{m}'$. Выполнение 1) очевидно. Чтобы доказать 2), положим

$$\mathfrak{m} = \sum_{P \in S} n_P P$$

и для всех $P' \in S'$ выберем целое $n_{P'}$, большее всех отношений n_P/e_P при $P \in S \cap \pi^{-1}(P')$. Если $v_{P'}(1 - g') \geqslant n_{P'}$, то

$$v_P(1 - g' \circ \pi) \geqslant e_P n_P \geqslant n_P, \quad \text{если } P \to P' \text{ и } P \in S.$$

[1]) То есть носитель дивизора не пересекается с S. — *Прим. перев.*

Поэтому в этом случае $(f,\ g' \circ \pi)_P = 0$. Если $P \notin S$, то $v_P(g' \circ \pi) = 0$ дает $(f,\ g' \circ \pi)_P = 0$. Итак, условие 2) выполняется для модуля

$$\mathfrak{m}' = \sum_{P' \in S'} n_{P'} P'.$$

Для проверки 3) надо вычислить $(\mathrm{Tr}_\pi f,\ g')_{P'}$ при $P' \in S'$. Имеем в этом случае

$$\begin{aligned}(\mathrm{Tr}_\pi f,\ g')_{P'} &= \sum_{P \to P'} v_P(g' \circ \pi) f(P) \quad (\text{поскольку } P \in S),\\ &= v_{P'}(g') \sum_{P \to P'} e_P f(P)\\ &= v_{P'}(g') f'(P') \text{ по определению } f'.\end{aligned}$$

Условие 3), следовательно, выполняется. То же самое очевидно относительно условия 4).

в) *Локальный символ нормы.* Пусть π: $X \to X'$ — разветвленное накрытие, S' — конечное подмножество X' и f': $X' - S' \to G$ — отображение $X' - S'$ в коммутативную группу G. Положим $S = \pi^{-1}(S')$. С другой стороны, если $g \in k(X)^*$, обозначим через $N_\pi g$ норму g в расширении $k(X)/k(X')$, определяемом π. Тогда имеет место следующее предложение, аналогичное предложению 3, в котором роли f и g поменялись местами.

Предложение 4. *Если f' обладает модулем $\mathfrak{m}'$ и отображение $f' \circ \pi$ — модулем $\mathfrak{m}$, то*

$$(f',\ N_\pi g)_{P'} = \sum_{P \to P'} (f' \circ \pi,\ g)_P, \quad P \in X', \quad g \in k(X)^*.$$

Заметим сначала, что существует модуль $\mathfrak{m}$ с носителем S, такой, что из $g \equiv 1 \bmod \mathfrak{m}$ следует $N_\pi g \equiv 1 \bmod \mathfrak{m}'$. Действительно, это хорошо известный результат для нормы (отображение нормы „непрерывно"), который можно доказать, например, погружая расширение $k(X)/k(X')$ в нормальное расширение. С другой стороны, если $g \in k(X^*)$, то, как известно, $(N_\pi g) = \pi((g))$. Применяя это к случаю $g \equiv 1 \bmod \mathfrak{m}$, мы видим, что $f' \circ \pi((g)) = f'(N_\pi g) = 0$. Это показывает, что $\mathfrak{m}$ — модуль для $f' \circ \pi$.

Осталось установить формулу, связывающую локальные символы f' и $f' \circ \pi$. Если $P' \in X - S'$, то эта формула выражает просто тот факт, что $v_{P'}(N_\pi g) = \sum_{P \to P'} v_P(g)$, т. е. что $(N_\pi g) = \pi((g))$. Предположим поэтому, что $P' \in S'$, и выберем функцию h, такую, что $g/h \equiv 1 \bmod \mathfrak{m}$ в точках, проектирующихся в P', и $h \equiv 1 \bmod \mathfrak{m}$ в точках $P \in S$, не проектирующихся в P. Тогда $N_\pi g / N_\pi h \equiv 1 \bmod \mathfrak{m}'$ в P' и $N_\pi h \equiv \equiv 1 \bmod \mathfrak{m}'$ на $S' - P'$. Отсюда

$$(f', N_\pi g)_{P'} = (f', N_\pi h)_{P'} = - \sum_{Q' \notin S'} (f', N_\pi h)_{Q'} =$$
$$= \sum_{P \notin S} (f' \circ \pi, h)_P = \sum_{P \to P'} (f' \circ \pi, h)_P = \sum_{P \to P'} (f' \circ \pi, g)_P.$$

3. Пример локального символа: случай аддитивной группы

Начиная с этого пункта, будем считать, что коммутативная группа G есть связная *алгебраическая* группа, а отображение f: $X - S \to G$ *регулярно*. Тогда f можно рассматривать как рациональное отображение X в G, регулярное во всех точках, за исключением S. Мы предположим, что S — минимальное подмножество точек G с этим свойством; другими словами, S — множество точек, где f нерегулярно.

Теорема Розенлихта, которую мы собираемся доказать в конце этой главы, формулируется так (ср. гл. I, теорема 1):

Теорема 1. *Отображение f обладает модулем $\mathfrak{m}$ с носителем S.*

Мы проверим эту теорему в частном случае, когда G — аддитивная группа G_a[1]), и дополним ее явным вычислением локального символа $(f, g)_P$.

Предложение 5. *Теорема 1 верна для группы G_a, причем соответствующий локальный символ $(f, g)_P = = \mathrm{Res}_P(f\, dg/g)$.*

---

[1]) G_a обозначает аддитивную группу поля k. — *Прим. перев.*

(Последняя формула имеет смысл, так как f — скалярная функция на X, имеющая S в качестве множества полюсов.)

Если P входит в S, мы полагаем $n_P = 1 - v_P(f)$. В силу того, что P — полюс f, имеем $n_P \geqslant 1$. Проверим, что $\mathrm{Res}_P(f\,dg/g)$ — локальный символ, соответствующий f, и $\mathfrak{m} = \sum n_P P$.

Свойство 1) очевидно, так как

$$\frac{d(gg')}{gg'} = \frac{dg}{g} + \frac{dg'}{g}.$$

Переходя к 2), заметим, что при $v_P(1-g) \geqslant n_P$

$$v_P(dg) \geqslant n_P - 1 \geqslant -v_P(f).$$

Так как $v_P(g) = 0$, это дает $v_P(f\,dg/g) \geqslant 0$, откуда $\mathrm{Res}_P(f\,dg/g) = 0$.

Для доказательства 3) заметим, что dg/g имеет *простой* полюс в P, что верно также и для $f\,dg/g$ $\left(\text{поскольку } P \notin S\right)$, и, следовательно, можно записать

$$\mathrm{Res}_P\left(f\frac{dg}{g}\right) = f(P)\,\mathrm{Res}_P\left(\frac{dg}{g}\right) = f(P)\,v_P(g),$$

применив формулу 4) из гл. II, п.11.

Наконец, формула 4)

$$\sum_{P \in X} \mathrm{Res}\left(f\frac{dg}{g}\right) = 0$$

есть формула вычетов, примененная к дифференциальной форме $\omega = f\,dg/g$.

Доказательство предложения **5**, таким образом, закончено.

Следствие. *В случае характеристики* $p > 0$ *имеем*

$$\mathrm{Res}_P\left(f^p\frac{dg}{g}\right) = \left[\mathrm{Res}_P\left(f\frac{dg}{g}\right)\right]^p.$$

Действительно, отображение $x = x^p$ является гомоморфизмом $G_a \to G_a$; с другой стороны, известно, что локальные символы функториальны (предложение 2).

(Конечно, нетрудно проверить предыдущую формулу и непосредственным вычислением.)

Можно применить также предложение 3 к рассматриваемому случаю. Напишем формулу для вычета следа (гл. II, п. 12, лемма 4):

$$\sum_{P \to P'} \operatorname{Res}_P(\omega) = \operatorname{Res}_{P'}(\operatorname{Tr}(\omega)).$$

Эта формула следует из предложения 4, если учесть формулу

$$\frac{d(N_\pi g)}{N_\pi g} = \operatorname{Tr}_\pi\left(\frac{dg}{g}\right).$$

Замечание. Предложение 5 распространяется на *группы Витта* W_n произвольной размерности. Рациональное отображение X в W_n — это вектор Витта $\vec{f}$ длины n с компонентами в $k(X)$. За $(\vec{f}, g)_P$ нужно брать символ, определенный Виттом ([1], § 2), и использовать формулу, аналогичную формуле вычетов (Витт [1], § 9; см. также Кавада и Сатаке [1]).

4. Пример локального символа: случай мультипликативной группы

Предположим теперь, что G—мультипликативная группа G_m поля k. Рациональное отображение f может быть снова отождествлено с функцией на X, а S состоит из множества нулей и полюсов f.

Предложение 6. *Отображение f обладает модулем $\mathfrak{m} = \sum_{P \in S} P$, причем соответствующий локальный символ есть*

$$(f, g)_P = (-1)^{nm} \frac{f^n}{g^m}(P), \quad \text{где} \quad n = v_P(g), \quad m = v_P(f).$$

(Эта формула имеет смысл, так как функция $h = f^n/g^m$ такова, что $v_P(h) = 0$, а следовательно, она имеет вполне определенное значение, отличное от нуля в точке P.)

Снова нам надо проверить свойства 1) — 4) локального символа,

1) Пусть $g'' = gg'$. Имеем $n'' = n + n'$, откуда

$$(f, g'')_P = (-1)^{(n+n')m} \frac{f^{(n+m')}}{g^m g'^m}(P) = (f, g)_P (f, g')_P.$$

2) Предположим, **что** $v_P(1-g) \geqslant 1$. Тогда $n = 0$, откуда

$$(f, g)_P = \frac{1}{g^m}(P) = 1, \quad \text{поскольку} \quad g(P) = 1.$$

3) Предположим, что $P \notin S$, т. е. что $m = v_P(f) = 0$. Тогда будем иметь $(f, g)_P = f(P)^{v_P(g)}$.

Итак, осталось только проверить следующую формулу („формулу произведения"):

4) $$\prod_{P \in X} (f, g)_P = 1.$$

Мы поступим так же, как для формулы вычетов, приводя все к случаю, когда X — проективная прямая Λ. Функцию g можно рассматривать как отображение $g\colon X \to \Lambda$. Если g — постоянное отображение, равное a, то левая часть 4) равна $a^{-\Sigma v_P(f)} = a^{-\deg((f))} = 1$ и формула 4) в этом случае верна. Значит, можно предполагать, что g — не константа. Тогда g отображает X на Λ, так как X — накрытие (разветвленное) Λ. Полагая $F = k(x)$ и $E = k(\Lambda)$, имеем расширение F/E, где $E = k(g)$. Определена операция *нормы* $N_{F/E}\colon F^* \to E^*$. Обозначая через t тождественное отображение $\Lambda \to \Lambda$, рассматриваемое как элемент $k(\Lambda)$, имеем две следующие леммы.

Лемма 1. *Для всех точек $P \in \Lambda$ имеем*

$$\prod_{g(Q)=P} (f, g)_Q = (N_{F/E} f, t)_P.$$

Лемма 2. *Для всех функций f' на Λ имеем*

$$\prod_{P \in \Lambda} (f', f)_P = 1.$$

Ясно, что формула 4) следует из леммы 1 и леммы 2, примененной к $f' = N_{F/E} f$. Итак, остается доказать эти две леммы.

Доказательство леммы 2. Запишем f' в виде $f'=\mu\prod(t-\lambda)^{n_\lambda}$. Так как символ $(f', t)_P$ мультипликативен по f', можно ограничиться случаем $f'=(t-\lambda)$. Имеем две возможности: $\lambda=0$ и $\lambda\neq 0$.

а) $\lambda=0$. Тогда $(t, t)_P=1$ для $P\neq 0, \infty$, $(t, t)_0=-1$, $(t, t)_\infty=-1$ и произведение равно единице.

б) $\lambda\neq 0$. Тогда $(t-\lambda, t)_P=1$ для $P\neq 0, \lambda, \infty$; $(t-\lambda, t)_0= =-\lambda$, $(t-\lambda, t)_\lambda=1/\lambda$, $(t-\lambda, t)_\infty=-1$ и произведение опять равно единице.

Доказательство леммы 1. Сведем ее к локальной задаче, как это было сделано в гл. II, п 12 для леммы 4. Заметим сначала, что символ $(f', t)_P$ сохраняет смысл, если f' и t — произвольные элементы поля $K=\widehat{E}_P$, пополнения поля E по нормированию v_P. Получаемый таким образом символ будет обозначаться через $(f', t)_K$. Он снова мультипликативен по f' и t. То же самое можно проделать для локального поля $L=\widehat{F}_Q$. Кроме того, известно[1]), что имеет место формула

$$N_{F/E}f=\prod_{Q\to P}N_Q f,\quad \text{где}\quad N_Q=N_{\widehat{F}_Q/\widehat{E}_P}.$$

Второй член доказываемой формулы записывается, следовательно, в виде $\prod\limits_{Q\to P}(N_Q f, t)_K$, и все сводится к доказательству следующего результата.

Лемма 3. *Если* $f\in L^*$, $g\in K^*$, *то* $(f, g)_L=(N_Q f, g)$.

(В этой лемме поле K отождествляется с подполем поля L, из чего следует, что t отождествляется с g.)

Достаточно провести доказательство для случая, когда f — униформизующая поля L. Действительно, $(f, g)_L$ и $(Nf, g)_K$ оба мультипликативны по f, а группа L^* порождается теми из своих элементов, которые являются униформизующими (поскольку любая „единица“ есть частное двух униформизующих). Следовательно, $L=k((f))$. Можно пред-

[1]) См., например, Шевалле [1], гл. IV, § 5, теорема 6, следствие 1. — *Прим. перев.*

полагать также, что g — униформизующая K, откуда $K = ((g))$. Вычисляя $v_P(Nf) = v_Q(f)$, получаем единицу, что дает

$$(Nf, g)_K = -\frac{Nf}{g}(P).$$

С другой стороны, если положить $e = [L : K]$, то $v_Q(g) = e$, откуда

$$(f, g)_L = (-1)^e \frac{f^e}{g}(Q).$$

Все свелось, следовательно, к тому, чтобы доказать, что функция Nf/fe принимает значение $(-1)^{e-1}$ в точке P (или в точке Q, что все равно). Для этого запишем минимальное уравнение f над K

$$f^e + a_1 f^{e-1} + \ldots + a_e = 0, \qquad a_i \in K.$$

Очевидно, что $a_e = (-1)^e Nf$. С другой стороны, если $a_i \neq 0$, то

$$v_L(a_i f^{e-i}) = e \cdot v_K(a_i) + e - i \equiv -i \bmod e.$$

Отсюда следует, что все одночлены предыдущего уравнения имеют различные порядки, исключая, может быть, f^e и a_e. Элементарные свойства нормирований показывают, что тогда должно быть

$$v_L(f^e) = v_L(a_e) > v_L(a_i f^{e-i}) \quad \text{при} \quad 1 \leqslant i \leqslant e-1.$$

После деления на f^e имеем $v_L(1 + a_e/f_e) > 0$. Это означает, что a_e/f_e принимает значение -1 в P, а следовательно, Nf/f^e принимает значение $(-1)^{e-1}$.

Замечание. Как и символ $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$ нормированного вычета Гильберта, символ $(f, g)_P$ обладает следующими свойствами (которые проверяются прямым вычислением):

$$(f, g)_P (g, f)_P = 1,$$
$$(-f, f)_P = 1,$$
$$(1 - f, f)_P = 1.$$

Отметим также следующий результат.

Предложение 7. *Если* (f) *и* (g) — *два дивизора, носители которых не пересекаются, то* $f((g)) = g((f))$.

Записывая $\prod\limits_{P \in X} (f, g)_P = 1$ и принимая во внимание, что $(f, g)_P$ равно либо $f(P)^{v_P(g)}$, либо $g(P)^{-v_P(f)}$, получаем $f((g))\, g(-(f)) = 1$, откуда и следует предложение 7.

§ 2. Доказательство теоремы 1

5. Основная редукция

Возвращаясь к ситуации п. 2б), предположим, что дано накрытие $\pi: X \to X'$. Для произвольного отображения $f: X - S \to G$ множества $X - S$ в коммутативную группу G было определено отображение

$$\mathrm{Tr}_\pi f: X' - S' \to G,$$

где $S' = \pi(S)$.

Предложение 8. *Если* G — *алгебраическая группа и* f — *регулярное отображение, то отображение* $\mathrm{Tr}_\pi f$ *регулярно.*

Пусть n — степень накрытия $X \to X'$ и $X^{(n)}$ — *n-кратное симметрическое произведение* X (ср. п. 14). Для всех $P' \in X'$ дивизор

$$\pi^{-1}(P') = \sum_{P \to P'} e_P P \qquad \text{(ср. п. 2)}$$

положителен и степени n, а следовательно, может быть отождествлен с точкой из $X^{(n)}$. Определенное таким образом отображение $\pi^{-1}: X' \to X^{(n)}$ *регулярно* (ср. п. 15, предложение 22). Положим, с другой стороны, $Y = X - S$. Множество Y является открытым подмножеством в X. Если положить

$$F(y_1, \ldots, y_n) = f(y_1) + \ldots + f(y_n),$$

то получается регулярное отображение Y^n в G, инвариантное относительно перестановок y_i. В силу определения симметрического произведения это отображение определяет отображение $F'\colon Y^{(n)} \to G$. Но $Y^{(n)}$ открыто в $X^{(n)}$ и π^{-1} отображает $Y' = X' - S'$ в $Y^{(n)}$, откуда следует, что $F' \circ \pi^{-1}\colon X' - S' \to G$ — регулярное отображение. Так как последнее отображение совпадает с $\mathrm{Tr}_\pi f$, предложение доказано.

Все предыдущее применимо, в частности, к случаю рациональной функции g на X, не являющейся константой, причем g рассматривается как отображение X в проективную прямую Λ. Пусть $\mathfrak{m} = \sum n_P P$ $(n_P > 0)$ — модуль с базой S. Условимся писать $g \equiv 0 \bmod \mathfrak{m}$, если $v_P(g) \geqslant n_P$ для всех $P \in S$. При этих условиях имеем $g(P) = 0$ для всех $P \in S$ и множество $S' = g(S)$ сводится, следовательно, к точке $\{0\}$ проективной прямой Λ. Отображение $\mathrm{Tr}_g f$ в силу предыдущего предложения является, следовательно, *регулярным отображением* $\Lambda - \{0\}$ *в* G.

Предложение 9. *Пусть* $\mathfrak{m} = \sum\limits_{P \in S} n_P(P)$ $(n_P > 0)$ — *модуль с носителем* S. *Для того чтобы* $\mathfrak{m}$ *был модулем для* f, *необходимо и достаточно, чтобы для всех непостоянных функций* g *с* $g \equiv 0 \bmod \mathfrak{m}$ *отображение* $\mathrm{Tr}_g f$ *было постоянным.*

Положим $f' = \mathrm{Tr}_g f$, где g — функция, не являющаяся константой и такая, что $g \equiv 0 \bmod \mathfrak{m}$. Если a — точка Λ, отличная от 0, то $f'(a) = f(g^{-1}(a))$ по определению f'. Если $a = \infty$, то $g^{-1}(\infty)$ есть дивизор $(g)_\infty$ полюсов функции g. Если $a \neq \infty$, то $g^{-1}(a)$ есть дивизор $(g)_a$ нулей функции $g - a$. Во всех случаях имеем, следовательно,

$$f'(a) = f((g)_a), \qquad a \in \Lambda - \{0\}.$$

Предположим теперь, что $\mathfrak{m}$ — модуль для f. Для всех $a \neq 0, \infty$ можно записать $g - a = -a(1 - a^{-1}g) = b \cdot h$, где b — постоянная, отличная от нуля, и $h \equiv 1 \bmod \mathfrak{m}$. Отсюда следует в силу предположения относительно $\mathfrak{m}$, что $f((g - a)) = 0$, откуда

$$f((g)_a) = f((g)_\infty),$$

т. е.

$$f'(a) = f'(\infty).$$

Это показывает, что f' — постоянное отображение.

Обратно, предположим, что f — постоянное отображение для всех функций $g \equiv 0 \bmod \mathfrak{m}$, причем g — не константа. Если $h \equiv 1 \bmod \mathfrak{m}$, то $h = 1 - g$, где $g \equiv 0 \bmod \mathfrak{m}$. Если g—константа, то таковой же будет и h, и $f((h)) = f(0) = 0$. Если g — не константа, то $(h) = (g)_1 - (g)_\infty$, откуда $f((h)) = f'(1) - f'(\infty) = 0$. Предложение доказано.

6. Доказательство в случае характеристики нуль

Пусть, как и прежде, $f\colon X - S \to G$ — регулярное отображение $X - S$ в алгебраическую коммутативную группу G. Обозначим через r размерность G, и пусть $\{\omega_1, \ldots, \omega_r\}$ — база векторного пространства дифференциальных форм степени 1, *инвариантных относительно трансляций на* G (относительно свойств этих форм см. п. 11). Положим $\alpha_i = f^*(\omega_i)$ $(1 \leqslant i \leqslant r)$. Элементы α_i — прообразы ω_i относительно f и, следовательно, регулярные формы на $X - S$. Для $P \in S$ выберем целое $n_P > 0$, такое, что $v_P(\alpha_i) \geqslant n_P$ при $1 \leqslant i \leqslant r$.

Предложение 10. *В случае характеристики* 0 *модуль* $\mathfrak{m} = \sum n_P P$, *определенный выше, является модулем для* f.

Мы применим критерий предложения 9. Пусть g — рациональная функция на X, не являющаяся константой и удовлетворяющая условию $g \equiv 0 \bmod \mathfrak{m}$. Мы должны показать, что $f' = \mathrm{Tr}_g f\colon \Lambda - \{0\} \to G$ — постоянное отображение. Обозначим это отображение через f'. *Достаточно доказать, что* $f'^*(\omega_i) = 0$ *для* $1 \leqslant i \leqslant r$. Действительно, поскольку ω_i линейно независимы в каждой точке G, линейное отображение, касательное к f', всюду равно нулю. Отсюда следует, поскольку характеристика равна нулю, что f' постоянно.

Прежде всего имеет место

Лемма 4. *Для* $1 \leqslant i \leqslant r$ $f'^*(\omega_i) = \mathrm{Tr}(\alpha_i)$.

(След берется относительно накрытия $g\colon X \to \Lambda$; см. гл. II, п. 12.)

Пусть Y — накрытие Галуа прямой Λ, превосходящее X (см. п. 13), и пусть π — проекция $Y \to X$. Так как $g \circ \pi$: $Y \to \Lambda$ — *сепарабельное* накрытие, отображение

$$\omega \to (g \circ \pi)^* (\omega) = \pi^* g^* (\omega)$$

является *инъективным* отображением множества дифференциальных форм на Λ в множество дифференциальных форм на Y. Таким образом, достаточно доказать формулу

$$\pi^* g^* f'^* (\omega_i) = \pi^* g^* \operatorname{Tr} (\alpha_i). \qquad (*)$$

Правую часть равенства (*) можно записать в виде

$$\sum_{j=1}^{j=n} \sigma_j^* \pi^* (\alpha_i),$$

где σ_j обозначают некоторые элементы группы Галуа $\mathfrak{g}$ накрытия $Y \to \Lambda$ (см. п. 13). С другой стороны, имеем равенство

$$f' \circ g \circ \pi = \sum_{j=1}^{n} f \circ \pi \circ \sigma_j, \qquad \text{(см. п. 13)}$$

и вследствие аддитивности операции $f^* (\omega)$ (п. 11, предложение 17) левая часть равенства (*) может быть записана в виде

$$\pi^* g^* f'^* (\omega_i) = \sum_{j=1}^{n} \sigma_j^* \pi^* f^* (\omega_i) = \sum_{j=1}^{n} \sigma_j^* \pi^* (\alpha_i),$$

т. е. получаем тот же результат.

[Заметим, что предыдущее доказательство справедливо для случая произвольной характеристики, лишь бы только g не была p-й степенью. Вероятно, что на самом деле лемма 4 верна без всяких ограничений на g (см. Барсотти [4], теорема 4.2).]

Лемма 5. *Для всех i $(1 \leqslant i \leqslant r)$ дифференциальная форма $f'^* (\omega_i)$ имеет в 0 не более чем простой полюс.*

Надо доказать, что $v_0(f'^* (\omega_i)) \geqslant -1$. Предположим, что $v_0(f'^* (\omega_i)) = -m - 1$ с $m \geqslant 1$. Если t: $\Lambda \to \Lambda$ обозначает тождественное отображение, рассматриваемое как рациональная функция на Λ, то

$$v_0\left(t^m f'^*(\omega_i)\right)=1, \quad \text{откуда} \quad \mathrm{Res}_0\left(t^m f'^*(\omega_1)\right)\neq 0.$$

В силу леммы 4 дифференциальная форма $t^m f'^*(\omega_i)$ является следом формы $g^m\alpha_i$. Применяя лемму 4 из гл. II, п. 12, получим, следовательно,

$$\sum_{P\to 0}\mathrm{Res}_P(g^m\alpha_i)\neq 0, \qquad 1\leqslant i\leqslant r.$$

Но форма $g^m\alpha_i$ регулярна во всех точках P, в которых $g(P)=0$. Действительно, если $P\notin S$, то g и α_i регулярны в этой точке; если же $P\in S$, то

$$v_P(g^m\alpha_i)=mv_P(g)+v_P(\alpha_i)\geqslant mn_P-n_P\geqslant 0.$$

Предположение $m\geqslant 1$ ведет, следовательно, к противоречию, что и доказывает лемму 5.

Теперь легко закончить доказательство предложения 10. Действительно, поскольку f' регулярна на $\Lambda-\{0\}$, то же самое можно сказать и про $f'^*(\omega_i)$. В силу леммы 5 этот дифференциал имеет в 0 не более чем простой полюс. Формула вычетов тогда показывает, что вычет в этой точке равен 0 и $f'^*(\omega_i)$ — дифференциал первого рода на Λ. Но поскольку Λ — кривая рода 0, этот дифференциал равен нулю. Предложение доказано.

7. Доказательство в случае характеристики $p>0$. Сведение задачи к двум случаям

Нам понадобятся некоторые сведения о *структуре* алгебраических коммутативных групп.

Приведем следующие два результата.

Предложение 11 („теорема Шевалле"). *Всякая связная алгебраическая группа G содержит инвариантную подгруппу R, такую, что*

а) *R — линейная связная группа;*

б) *G/R — абелево многообразие.*

(Определение факторгрупп см. Шевалле [3], сообщение 8.)

Предложение 12. *Всякая линейная связная коммутативная алгебраическая группа изоморфна прямому произведению некоторого числа мультипликативных групп G_m и группы U, изоморфной подгруппе группы треугольных матриц, имеющих* 1 *на диагонали.* (Такая группа U называется *„унипотентной“*.)

Применим предложение 11 к группе G. Имеем $G/R = A$, где A — абелево многообразие. С другой стороны, предложение 12 позволяет разложить R в прямое произведение унипотентной группы и групп G_m. Предположим, что $R = R_1 \times R_2$. Тогда группа G погружается как подгруппа в $G/R_1 \times G/R_2$. Если $\mathfrak{m}_i$ — модуль для составного отображения

$$X - S \xrightarrow{f} G \longrightarrow G/R_i \quad (i = 1,2),$$

то ясно, что $\mathfrak{m} = \operatorname{Sup}(\mathfrak{m}_1, \mathfrak{m}_2)$ — модуль для f. Следовательно, можно ограничиться доказательством теоремы 1 для групп G/R_1 и G/R_2, которые являются расширениями R_1 и R_2 с помощью A. Поступая последовательно таким образом, мы сводим доказательство теоремы 1 к двум следующим случаям:

а) *G — расширение группы G_m с помощью абелева многообразия A*;

б) *G — расширение унипотентной группы U с помощью абелева многообразия A.*

Мы рассмотрим случай а) в следующем пункте, а случай б) в пп. 9 и 10.

Замечание. Таким образом, мы использовали теорему Шевалле для доказательства теоремы 1. Наоборот, как заметил Розенлихт, доказав теорему 1 непосредственно, можно получить новое доказательство теоремы Шевалле с помощью теории якобиевых многообразий (см. гл. VII, п. 13).

8. Доказательство теоремы в случае характеристики $p > 0$. Случай а)

Нам потребуются две следующие элементарные леммы.

Лемма 6. *Всякое регулярное отображение проективной прямой с выколотой точкой в мультипликативную группу G_m постоянно.*

Можно считать, что выколотая точка — бесконечно удаленная. В этом случае рассматриваемое отображение есть рациональная функция, не имеющая ни нулей, ни полюсов в конечной области. Следовательно, это полином без нулей, т. е. константа.

Лемма 7. *Пусть V — неособое многообразие и $\underline{\Omega}$ — его пучок дифференциальных форм степени* 1 (см. гл. II, п. 7). *Предположим, что для всех $P \in V$ $\mathfrak{O}_P$-модуль $\underline{\Omega}_P$ порождается элементами $H^0(V, \underline{\Omega})$. Тогда всякое регулярное отображение f проективной прямой Λ в V постоянно.*

Пусть $\omega \in H^0(V, \underline{\Omega})$. Дифференциальная форма $f^*(\omega)$ всюду регулярна на Λ и, следовательно, равна нулю. В силу предположения относительно V отсюда следует, что линейное отображение, касательное к f, всюду равно нулю. В случае характеристики 0 это сразу дает постоянство f. В случае характеристики $p > 0$ это показывает, что f представляется в виде $f = g \circ F$:

$$\Lambda \xrightarrow{F} \Lambda \xrightarrow{g} V, \text{ где } \Lambda \xrightarrow{F} \Lambda \text{ — отображение } \lambda \to \lambda^p.$$

Применяя то же рассуждение к g, получаем представимость f в виде $f = h \circ F^n$, где n — произвольное целое число, что может быть только в том случае, когда f — постоянное отображение. (Действительно, в противном случае образ прямой Λ при отображении f будет кривой C и обязательно $p^n \leqslant [k(\Lambda) : k(C)]$.)

Следствие. *Всякое рациональное отображение Λ в абелево многообразие постоянно.*

Действительно, поскольку абелево многообразие полно, такое отображение всюду регулярно[1]; с другой стороны, очевидно, что абелево многообразие (вообще всякая алгебраическая группа; см. п. 11) удовлетворяет условию леммы.

---

[1]) См., например, Ленг [5]. — *Прим. перев.*

(Заметим, что та же лемма дает доказательство теоремы Люрота[1]): достаточно взять за V кривую рода >0.)

Перейдем теперь к доказательству случая а) теоремы 1.

Предложение 13. *Предположим, что G — расширение мультипликативной группы G_m с помощью абелева многообразия A. Если положить $\mathfrak{m}=\sum\limits_{P\in S} P$, то $\mathfrak{m}$ будет модулем для f.*

Мы применим критерий предложения 9. Пусть g — рациональная функция на X, такая, что

$$g\equiv 0 \bmod \mathfrak{m}, \quad \text{т. е.} \quad g(P)=0 \text{ для } P\in S.$$

Тогда $\mathrm{Tr}_g f$ — регулярное отображение $\Lambda - \{0\}$ в G. Умножая это отображение на проекцию $G\to A$, получаем рациональное отображение Λ в A, которое постоянно в силу леммы 7. Таким образом, $\mathrm{Tr}_g f$ принимает значения в классе по модулю G_m, бирегулярно изоморфном G_m. Применяя лемму 6, заключаем, что отображение $\mathrm{Tr}_g f$ постоянно.

Замечание. Если $G=G_m$, то предыдущее доказательство заново доказывает первую половину предложения 6 (определение модуля $\mathfrak{m}$), но не вторую (явное значение локального символа).

9. Доказательство в случае характеристики $p>0$. Сведение случая б) к случаю унипотентной группы

Предположим теперь, что G содержит унипотентную подгруппу U, такую, что $G/U=A$ — абелево многообразие. Если закон композиции в U записывать аддитивно, то существует целое число r, такое, что $p^r u=0$ для всех $u\in U$. Это видно или из того, что U — кратное расширение групп G_a, или из того, что, записав u в виде $1+n$, где n — нильпотентная матрица из $\mathbf{GL}_m$, будем иметь

$$(1+n)^{p^r}=1+n^{p^r}=1, \quad \text{как только} \quad p^r\geqslant m.$$

[1]) Теорема Люрота утверждает, что любое подполе поля рациональных функций от одной переменной является полем рациональных функций от одной переменной. Эта теорема распространяется на случай двух переменных. Для трех и более переменных теорема не доказана. — *Прим. перев.*

С другой стороны, по теореме Вейля ([5], стр. 127) имеем $p^r A = A$. Положим тогда $u' = G/p^r G$, $G' = A \times U'$, и пусть θ: $G \to G'$ — отображение, равное произведению канонических отображений $G \to A$ и $G \to U'$. Группа U' *унипотентна*. Действительно, она удовлетворяет условию $p^r U' = 0$, а следовательно, не имеет ни подгруппы, изоморфной G_m, ни факторгруппы, изоморфной ненулевому абелеву многообразию. Нужное утверждение следует теперь из теорем о строении алгебраических групп в п. 7. Далее, *ядро* θ *конечно*. Действительно, это ядро равно $U \cap p^r G$, а $p^r G$ — абелево многообразие (поскольку $p^r U = 0$, отображение p^r: $G \to G$ разлагается в $G \to A \to G$). Следовательно, $U \cap p^r G$ — пересечение аффинного многообразия с полным многообразием и, значит, конечное множество.

Мы уже доказали теорему в случае абелевого многообразия (это по существу содержится в следствии к лемме 7). Предположим, что она верна и для унипотентной группы. Тогда она будет верна и для G', а следовательно, и для G в силу следующего предложения.

Предложение 14. *Пусть* θ — *гомоморфизм* (в смысле алгебраических групп) *алгебраической коммутативной группы G в алгебраическую коммутативную группу G'. Предположим, что ядро θ конечно. Если $\mathfrak{m}$ — модуль для $\theta \circ f$, то он будет также модулем для f.* (Это обращение предложения из п. 2.)

Применим критерий предложения 9. Если g — рациональная функция на X, непостоянная и такая, что $g \equiv 0 \bmod \mathfrak{m}$, то

$$\mathrm{Tr}_g(\theta \circ f)\colon \Lambda - \{0\} \to G'$$

есть постоянное отображение. Но это отображение можно записать в виде $\theta \circ \mathrm{Tr}_g f$. Это показывает, что $\mathrm{Tr}_g f$ принимает значения в классе по модулю ядра θ, т. е. в *конечном* множестве. Так как $\Lambda - \{0\}$ связно, отсюда следует, что $\mathrm{Tr}_g f$ постоянно. Предложение доказано.

Итак, остается доказать теорему 1 для случая, когда G — унипотентная группа. Это будет сделано в следующем пункте

10. Окончание доказательства. Случай, когда G — унипотентная группа

Предположим, что G — *унипотентная коммутативная, связная группа*. Таким образом, ее можно считать вложенной в линейную группу $\mathbf{GL}_r(k)$, причем так, что каждый из ее элементов записывается в виде $I+N$, где $N=(n_{ij})$ — матрица с $n_{ij}=0$ для $i \geqslant 1$.

В частности, можно считать G вложенной в векторное пространство $\mathbf{M}_r(k)$ всех матриц порядка r над k. Всякое рациональное отображение g кривой Y в группу G определяет, таким образом, r^2 рациональных функций g_{ij}, $i, j=1, \ldots, r$ (и определяется ими). Если Q — точка Y, то мы полагаем

$$w_Q(g)=\operatorname{Sup}(0, -v_Q(g_{ij})) \quad (i, j=1, \ldots, r). \tag{1}$$

В частности, это относится к $f: X-S \to G$. Выберем теперь такое целое n, что

$$n > (r-1)\, w_P(f) \quad \text{для всех} \quad P \in S. \tag{2}$$

Предложение 15. *Модуль* $\mathfrak{m}=\sum_{P \in S} nP$ *является модулем для* f.

Применим опять критерий предложения 9. Пусть g — рациональная функция на X, не являющаяся константой и такая, что $v_P(g) \geqslant n$ для всех $P \in S$. Надо показать, что $f'=\operatorname{Tr}_g f$ — постоянное отображение. Для этого достаточно убедиться в том, что

$$w_0(f') < 1. \tag{3}$$

Действительно, это неравенство показывает, что $v_0(f'_{ij}) \geqslant 0$, другими словами, что f' регулярно в точке 0 на Λ. Отображение f', являясь регулярным отображением полного многообразия Λ в аффинное многообразие G, будет постоянным.

Пусть Y — нормальное накрытие Λ над X (см. п. 13) и π — проекция $Y \to X$. Для каждой точки $P \in X$ (соответственно $Q \in Y$) пусть e_P (соответственно e_Q) — индекс ветвления P (соответственно Q) для накрытия g: $X \to \Lambda$ (соответственно для накрытия π: $Y \to X$). Выберем точку $Q \in Y$, проектирующуюся в $P \in S$ и такую, что значение $e=e_Q$ в этой точке максимально по сравнению со всеми точками Q, обладающими этим свойством. Положим $P = \pi(Q)$, $P \in S$. Тогда

$$w_Q(f' \circ g \circ \pi) = e e_P w_0(f'),$$

откуда

$$w_Q(f' \circ g \circ \pi) \geqslant n e w_0(f'), \tag{4}$$

поскольку $e_P = v_P(g) \geqslant n$.

Остается, следовательно, оценить $w_P(f' \circ g \circ \pi)$. Однако если p^k обозначает степень несепарабельности расширения $k(x)/k(\Delta)$, то

$$f' \circ g \circ \pi = p^k \sum f \circ \pi \circ \sigma_j, \tag{5}$$

где σ_j обозначают некоторые элементы группы Галуа накрытия Y (см. п. 13). Теперь можно воспользоваться следующей леммой.

Лемма 8. *Если f^α — рациональные отображения кривой Y в G, то*

$$w_Q\left(\sum f^\alpha\right) \leqslant (r-1) \operatorname*{Sup}_\alpha w_Q\left(f^\alpha\right).$$

Применяя ее к (5), получаем

$$\begin{aligned} w_Q(f' \circ g \circ \pi) &\leqslant (r-1) \operatorname*{Sup}_j \omega_Q(f \circ \pi \circ \sigma_j) \\ &\leqslant (r-1) \operatorname*{Sup}_j w_{Q_j}(f \circ \pi), \text{ где } Q_j = \sigma_j(Q), \\ &\leqslant (r-1) \operatorname*{Sup}_j e_{Q_j} w_{P_j}(f), \text{ где } P_j = \pi(Q_j). \end{aligned} \tag{6}$$

Если $P_j \notin S$, то $w_{P_j}(f) = 0$ и, следовательно, можно ограничиться рассмотрением во втором выражении (6) членов, соответствующих $P_j \in S$. Для них имеем $e_{Q_j} \leqslant e$ и $w_{P_j}(f) \leqslant n/(r-1)$ в силу выбора n. Таким образом, из (6) получаем неравенство

$$w_Q(f' \circ g \circ \pi) < en, \tag{7}$$

которое вместе с (4) и доказывает (3).

Осталось доказать лемму 8. Перейдем для этого к *мультипликативной* записи закона композиции G. Нужно рассмотреть произведение

$$\prod f^{\alpha} = \prod (1 + n^{\alpha}), \tag{8}$$

где n^{α} — рациональное отображение Y в пространство матриц N с $n_{ij} = 0$ при $i \geqslant j$. Но произведение r таких матриц n равно нулю. Следовательно, можно переписать произведение (8) в виде

$$f = \sum_{0 \leqslant k \leqslant r-1} \sum_{\alpha_1 < \ldots < \alpha_k} n^{\alpha_1} \ldots n^{\alpha_k}. \tag{9}$$

Формула (9) показывает, что компоненты $\left(\prod f^{\alpha}\right)_{ij}$ произведения $\prod f^{\alpha}$ — полиномы от n^{α} полной степени $\leqslant r - 1$. В силу определения w_Q это дает

$$w_Q\left(\prod f^{\alpha}\right) \leqslant (r-1) \operatorname{Sup} w_Q(n^{\alpha}) = \\ = (r-1) \operatorname{Sup} w_Q(f^{\alpha}). \tag{10}$$

Лемма доказана.

Это завершает доказательство предложения 15, а вместе с тем и теоремы 1.

Замечание. Случай унипотентной группы можно также свести к случаю групп Витта (п. 3), используя тот факт, что группа G изогенна произведению групп Витта (см. гл. VII, § 2).

§ 3. Вспомогательные результаты

11. Инвариантные дифференциальные формы на алгебраической группе

Пусть X — неособое алгебраическое многообразие. Через T_X мы обозначаем расслоенное пространство касательных векторов на X, а через T_X^* — двойственное ему расслоенное пространство. Напомним (см. гл. II, п. 7), что T_X^* определяется тем условием, что пучок $\mathcal{S}(T_X^*)$ ростков сечения T_X^*

изоморфен пучку $\underline{\Omega}_X$ дифференциалов $D_k(\mathfrak{O}_P)$ локальных колец точек X.

Если $f\colon X \to Y$ — регулярное отображение мнгообразия X в многообразие Y (X и Y предполагаются неособыми), то f определяет гомоморфизм $\mathfrak{O}_Y \to \mathfrak{O}_X$, откуда, переходя к дифференциалам, получаем гомоморфизм

$$f^*\colon \underline{\Omega}_Y \to \underline{\Omega}_X.$$

В общем случае, если E_X и E_Y — два расслоенных пространства, слои которых — векторные пространства, с базами соответственно X и Y, то любой $\mathfrak{O}_Y$-линейный гомоморфизм $\mathcal{S}(E_Y) \to \mathcal{S}(E_X)$ соответствует гомоморфизму расслоенного пространства E_X^* в расслоенное пространство E_Y^*, совместимому с f, и наоборот. Это проверяется непосредственно с помощью локальных карт. Применяя это рассуждение к $E_X = T_X^*$ и $E_Y = T_Y^*$, видим, что f^* определяет (и определяется им) гомоморфизм

$$df\colon T_X \to T_Y,$$

называемый линейным отображением, касательным к f. Таким образом, по определению имеем

$$\langle df(t),\ \omega\rangle = \langle t,\ f^*(\omega)\rangle,$$

если $t \in T_X(x)$ и $\omega \in T_Y^*(y)$, где $y = f(x)$ [слой расслоенного пространства E в точке x обозначается через $E(x)$].

Другими словами, T_X — *ковариантный функтор* на X. Он обладает, кроме того, следующим свойством: если X и Y — два многообразия без особенностей, то каноническое отображение $T_{X\times Y} \to T_X \times T_Y$ является изоморфизмом. (Действительно, существование вложений $X \to X \times Y$ и $Y \to X \times Y$ показывает, что это отображение $T_{X\times Y}$ *на* $T_X \times T_Y$, а так как оба эти пространства имеют одинаковую размерность, то это есть изоморфизм.)

Указанных элементарных свойств нам будет достаточно. Рассмотрим теперь отображение $h\colon X \times Y \to Z$; для всех $y \in Y$ обозначим через h_y частичное отображение $x \to h(x, y)$. Имеет место

Лемма 9. *Пусть X, Y, Z — неособые многообразия. Отображение*

$$(t, y) \to dh_y(t) \quad (t \in T_X, y \in Y)$$

есть регулярное отображение $T_X \times Y$ в T_Z.

Действительно, это отображение можно разложить следующим образом:

$$T_X \times Y \to T_X \times T_Y = T_{X \times Y} \to T_Z,$$

где $T_{X \times Y} \to T_Z$ есть dh, тогда как $T_X \times Y \to T_X \times T_Y$ — произведение тождественного отображения T_X на себя и отображения Y в T_Y, которое переводит y в 0_y, нейтральный элемент $T_Y(y)$[1]).

Пусть теперь G — алгебраическая группа. Для $g \in G$ обозначим через ρ_g левый перенос $x \to gx$. Это автоморфизм G (относительно структуры алгебраического многообразия). Отсюда следует, что $d\rho_g$: $T_G(x) \to T_G(gx)$ — изоморфизм для всех $x \in G$. Если $t \in T_G(x)$, то мы пишем $g \cdot t$ вместо $d\rho_g(t)$. По предыдущей лемме $g \cdot t$ является регулярной функцией от g и t. В частности, пусть $\{t_1, \ldots, t_n\}$ — базис $T_G(e)$, где e — нейтральный элемент G. Для всех i отображение $g \to g \cdot t_i$ есть регулярное сечение расслоенного пространства T_G и $g \cdot t_i$ образуют базис $T_G(g)$ для всех $g \in G$. Другими словами, имеет место

Предложение 16. *Расслоенное пространство T_G касательных векторов к алгебраической группе G размерности n является тривиальным расслоением, допускающим в качестве репера набор векторов $g \circ t_i$, инвариантных относительно левых переносов.*

Переходя к двойственному расслоению T_G^*, получаем

Следствие 1. *Существует репер T_G^*, образованный n дифференциальными формами ω_i, инвариантными слева.*

Пусть теперь f: $G \to G'$ — гомоморфизм группы G в группу G'. Если $S(G)$ [соответственно $S(G')$] обозначает векторное

---

[1]) Отображение $Y \to T_Y$ есть не что иное, как нулевое сечение расслоенного пространства T_Y. — *Прим. перев.*

пространство дифференциальных форм, инвариантных слева на G (соответственно на G'), над полем k, то $f^*(\omega) \in S(G)$ для всех дифференциальных форм $\omega \in S(G')$. При этих обозначениях имеем

Следствие 2. *Предположим, что f: $G \to G'$ — отображение на G'. Для того чтобы структура алгебраической группы G' была факторструктурой G, необходимо и достаточно, чтобы f^*: $S(G') \to S(G)$ было вложением.*

Так как G' можно заменить на факторгруппу, считаем, что f биективно. Можно также предположить, что G и G' связны. Пусть K/K' — расширение поля, соответствующее f. Поскольку f биективно, это расширение радикально. Следовательно, f — тогда и только тогда изоморфизм, когда K/K' сепарабельно. Однако известно [см. критерий сепарабельности (Картан и Шевалле [1], сообщение 13)], что f сепарабельно тогда и только тогда, когда касательное отображение к f сюръективно на каждом открытом непустом множестве из G. В силу следствия 1 это условие эквивалентно тому, что f^*: $S(G') \to S(G)$ инъективно.

Следствие 3. *Предположим, что f: $G \to G'$ инъективно. Для того чтобы структура алгебраической группы G была индуцирована структурой G', необходимо и достаточно, чтобы f^*: $S(G') \to S(G)$ было отображением на $S(G)$.*

Заменяя G' на подгруппу, можем считать, что f биективно. Это возвращает нас к предыдущему следствию.

Можно определить также линейное представление G, биинвариантные дифференциальные формы, операцию возведения в p-ю степень на алгебре Ли (с характеристикой p) и т. д. Все это не представляет никакого затруднения. Мы ограничимся пояснением одного свойства, использованного в доказательстве предложения 10.

Предложение 17. *Пусть f и g — два регулярных отображения алгебраического многообразия X в алгебраическую коммутативную группу G. Если ω — инвариантный дифференциал на G, то*

$$(f+g)^*(\omega) = f^*(\omega) + g^*(\omega).$$

Обозначим через pr_1 и pr_2 две проекции группы $G \times G$ на G и положим $\rho = \mathrm{pr}_1 + \mathrm{pr}_2$. В силу того, что G — абелева группа, эти отображения — гомоморфизмы и $\overset{*}{\rho}(\omega)$, $\overset{*}{\mathrm{pr}_1}(\omega)$ и $\overset{*}{\mathrm{pr}_2}(\omega)$ — инвариантные дифференциалы на $G \times G$. Так как равенство

$$\overset{*}{\rho}(\omega) = \overset{*}{\mathrm{pr}_1}(\omega) + \overset{*}{\mathrm{pr}_2}(\omega)$$

верно в единичном элементе, оно верно всюду. Пусть (f, g): $X \to G \times G$ — отображение, определенное парой (f, g). Тогда

$$f = \mathrm{pr}_1 \circ (f, g), \quad g = \mathrm{pr}_2 \circ (f, g), \quad f + g = \rho \circ (f, g),$$

откуда

$$\overset{*}{(f+g)}(\omega) = \overset{*}{(f, g)}\,\overset{*}{\rho}(\omega) = \overset{*}{(f, g)}\,\overset{*}{\mathrm{pr}_1}(\omega) + \overset{*}{(f, g)}\,\overset{*}{\mathrm{pr}_2}(\omega) = \\ = f^*(\omega) + g^*(\omega).$$

12. Фактормногообразие по конечной группе автоморфизмов

Пусть V — алгебраическое многообразие и R — отношение эквивалентности на V. Обозначим через V/R фактормножество V по R, и пусть θ: $V \to V/R$ — каноническая проекция V на V/R. Снабдим V/R фактортопологией топологии Зарисского V. Если f — функция, определенная в окрестности точки $w \in V/R$, то будем говорить, что f *регулярна в* w, если $f \circ \theta$ регулярна в окрестности $\theta^{-1}(w)$. Регулярные в ω функции образуют кольцо $\mathcal{O}_{V/R,\, w}$. Таким образом, получается подпучок $\mathcal{O}_{V/R}$ пучка ростков функций на V/R. Если топология и предыдущий пучок удовлетворяют аксиомам алгебраических многообразий [аксиомы (VA_{I}) и (VA_{II}) из АКП, п. 34], то говорим, что алгебраическое многообразие V/R есть *фактормногообразие* V по R. Регулярные отображения V/R в алгебраическое многообразие V' отождествляются с регулярными отображениями V в V', постоянными на классах по модулю R. Структура алгебраического многообразия, таким образом, становится факторструктурой V в смысле Бурбаки (Теория множеств, IV, § 2, п. 6.)

Все предыдущее особенно часто применяется в случае, когда R — отношение эквивалентности, определяемое конечной группой $\mathfrak{g}$, действующей на V. В этом случае мы пишем $V/\mathfrak{g}$ вместо V/R. Мы покажем при достаточно широких предположениях, что $V/\mathfrak{g}$ — алгебраическое многообразие. Изучим сначала частный случай.

Предложение 18. *Предположим, что V — аффинное многообразие с кольцом координат A. Тогда $V/\mathfrak{g}$ - алгебраическое аффинное многообразие, кольцо координат которого отождествляется естественным образом с подкольцом $A^{\mathfrak{g}}$ элементов A, неподвижных при действии $\mathfrak{g}$.*

Кольцо A — K-алгебра, порождаемая конечным числом элементов $x_1, \ldots, x_n$. Эти элементы *целы* относительно $A^{\mathfrak{g}}$, как показывают уравнения целой зависимости

$$\prod_{\sigma \in \mathfrak{g}} (X - X^{\sigma}) = 0.$$

Следующая лемма показывает, что $A^{\mathfrak{g}}$ — k-алгебра конечного типа.

Лемма 10. *Пусть A — алгебра конечного типа над коммутативным нётеровым кольцом k и B — подалгебра A, такая, что любой элемент A цел над B. Тогда B — k-алгебра конечного типа.*

Пусть x_i $(1 \leqslant i \leqslant n)$ — образующие алгебры A. Каждый из этих элементов удовлетворяет уравнению целой зависимости над B. Пусть $f_i(x_i) = 0$ — эти уравнения и $b_1, \ldots, b_r$ — их коэффициенты. Пусть $C = k[b_1, \ldots, b_r]$ — подалгебра в B, порожденная b_j. Тогда x_i целы над C и порождают A. Отсюда следует, что A — C-модуль конечного типа. Но C нётерово, а следовательно, B как C-подмодуль A должен порождаться конечным числом элементов $y_1, \ldots, y_m$ и $B = k[b_1, \ldots, b_r, y_1, \ldots, y_m]$. Лемма доказана.

Вернемся теперь к доказательству предложения 18.

Так как B не имеет нильпотентных элементов, существует аффинное многообразие W, координатное кольцо которого есть B. Вложение $B \to A$ определяет регулярное отображение θ: $V \to W$ на W (поскольку A цело над B[1])), инвари-

[1]) Автор использует в этом месте теорему Коэна — Зайденберга (см., например, Зарисский О. и Самюэль П., Коммутативная алгебра, т. 1, ИЛ, М, 1963, стр. 295, теорема 3). — *Прим. перев.*

антное относительно $\mathfrak{g}$. Кроме того, если v и v' — две точки V, не эквивалентные по модулю $\mathfrak{g}$, то можно найти $f \in A$, такое, что

$$f(v) = 0 \quad \text{и} \quad f(v'^{\sigma}) = 1$$

для всех $\sigma \in \mathfrak{g}$. Функция $F = \prod f^{\sigma}$ принадлежит тогда $A^{\mathfrak{g}}$ и удовлетворяет условию $F(v) = 0$, $F(v') = 1$, а потому $\theta(v) \neq \theta(v')$. Таким образом, θ отождествляет фактормножество $V/\mathfrak{g}$ с W. Проверим, что структура алгебраического многообразия W есть факторструктура V. Прежде всего топология W является фактортопологией V; действительно, достаточно показать, что если V' замкнуто в V, то $\theta(V')$ замкнуто в W. Но если V' определяется нулями функций $f_i \in A$, то ясно, что $\theta(V')$ определяется нулями $F_i = \prod\limits_{\sigma \in \mathfrak{g}} f_i^{\sigma}$, которые входят в $A^{\mathfrak{g}}$. Наконец, если g — инвариантная относительно $\mathfrak{g}$ функция, регулярная на орбите $v \in V$, то можно записать g в виде a/s, где $a \in A$ и $s \neq 0$ на орбите v. Заменяя s на $S = \prod s^{\sigma}$, можно предполагать, что $s \in A^{\mathfrak{g}}$, откуда $a \in A^{\mathfrak{g}}$ (все рассуждения проходят по крайней мере, если V неприводимо; в противном случае необходимо изменить их очевидным образом). Это показывает, что g имеет вид $g' \circ \theta$, где g' регулярна в окрестности $\theta(v)$. Локальные кольца W совпадают, таким образом, с локальными кольцами $V/\mathfrak{g}$. Предложение 18 доказано.

Следствие. а) *Если $\mathfrak{g}$ и $\mathfrak{g}'$ действуют на аффинных многообразиях V и V', то*

$$(V \times V')/\mathfrak{g} \times \mathfrak{g}' = V/\mathfrak{g} \times V'/\mathfrak{g}'.$$

б) *Если V неприводимо, то неприводимо и $V/\mathfrak{g}$ и*

$$k(V/\mathfrak{g}) = k(V)^{\mathfrak{g}}.$$

в) *Если V нормально, то нормально и $V/\mathfrak{g}$.*

Утверждение а) эквивалентно формуле

$$(A \otimes_k A')^{\mathfrak{g} \times \mathfrak{g}'} = A^{\mathfrak{g}} \otimes_k A'^{\mathfrak{g}'},$$

справедливой для произвольных векторных пространств A и A'. Утверждения б) и в) вытекают из классической формулы

$$A^{\mathfrak{g}} = A \cap k(V)^{\mathfrak{g}}.$$

Мы предоставляем читателю их проверку.

Предложение 19. *Пусть $\mathfrak{g}$ — конечная группа, действующая на алгебраическом многообразии V. Предположим, что всякая орбита $\mathfrak{g}$ содержится в открытом аффинном множестве V. Тогда $V/\mathfrak{g}$ — алгебраическое многообразие.*

Если S — орбита $\mathfrak{g}$, то существует открытое аффинное множество U, содержащее S. Если положить $U' = \bigcap U^{\sigma}$, то U' — открытое аффинное множество, инвариантное относительно $\mathfrak{g}$ и содержащее S. Покроем V такими открытыми множествами U'_i. Пусть $U_i = U'_i/\mathfrak{g}$ — их образы в $V/\mathfrak{g}$. Тогда U_i — открытые множества в силу предложения 18. Аксиома (VA_{I}) алгебраических многообразий, таким образом, выполнена. Остается проверить аксиому (VA'_{II}), другими словами, проверить, что множество $\Delta_{V/R} \cap (U_i \times U_j)$ замкнуто в $U_i \times U_j$ ($\Delta_{V/R}$ обозначает диагональ V/R). Но это множество является образом $\Delta_V \cap (U'_i \times U'_j)$ при канонической проекции

$$U'_i \times U'_j \to U_i \times U_j = (U'_i \times U'_j)/(\mathfrak{g} \times \mathfrak{g})$$

(см. предыдущее следствие). Так как V — алгебраическое многообразие, $\Delta_V \cap (U'_i \cap U'_j)$ замкнуто, что верно также и для его образа при предыдущем отображении. Предложение доказано.

Примеры. 1. Условие предложения 19 всегда выполняется, если V — локально замкнутое подмногообразие проективного пространства $\mathbf{P}_r(k)$. Действительно, пусть S — орбита $\mathfrak{g}$ и $\overline{V}$ — замыкание V в $\mathbf{P}_r(k)$. Множество $F = \overline{V} - V$ замкнуто и не пересекается с S. Следовательно, можно найти однородную форму $\varphi(x_0, \ldots, x_r)$, обращающуюся в нуль на F и не равную нулю в точках S. Множество U точек V, где $\varphi(x_0, \ldots, x_r) \neq 0$, открыто в V и удовлетворяет условию предложения 18 (см. АКП, п. 52).

2. То же самое будет в случае, когда V — *групповое многообразие* группы G. Действительно, предположим сначала, что группа G связна, и пусть g_i — точки рассматриваемой орбиты S. Если U_0 — открытое непустое аффинное множество G, то пересечение множеств $g_i^{-1}U_0$ непусто. Пусть g — элемент этого пересечения. Тогда непосредственно проверяется, что $U = U_0 g^{-1}$ удовлетворяют поставленному требованию. Случай, когда G несвязна, сводится к предыдущему.

(Заметим, что, как доказал Барсотти [1], всякое групповое многообразие погружается в проективное пространство; тот же результат справедлив для однородных пространств, согласно Чжоу [2].)

3. Наоборот, Нагата [1] построил алгебраическое многообразие V, на котором действует группа $\mathfrak{g} = \mathbf{Z}/2\mathbf{Z}$, так, что фактормногообразие $V/\mathfrak{g}$ не является алгебраическим многообразием.

Замечания. 1. В силу локального характера следствие предложения 18 остается верным для многообразий (не обязательно аффинных), удовлетворяющих условию предложения 19.

2. Пусть k' — подполе в k. Предположим, что V снабжена структурой k'-многообразия (погруженного в проективное пространство, для конкретности). Если операции $\mathfrak{g}$ определены над k', то $V/\mathfrak{g}$ можно снабдить естественным образом структурой k'-многообразия. Это сразу же видно, если перейти к аффинному случаю и использовать очевидную формулу

$$(A' \underset{k'}{\otimes} k)^{\mathfrak{g}} = A'^{\mathfrak{g}} \underset{k'}{\otimes} k,$$

справедливую для любого векторного пространства A' над полем k'.

3. Отметим, что одно из „интуитивных“ свойств фактормногообразий неверно: если V' — подмногообразие V, инвариантное относительно $\mathfrak{g}$, то фактормногообразие $V'/\mathfrak{g}$ не обязательно отождествляется с подмногообразием $V/\mathfrak{g}$ (отображение $V'/\mathfrak{g} \to V/\mathfrak{g}$ радикально; см. пример в п. 14).

Это свойство всегда имеет место в случае характеристики 0 или в случае, когда $\mathfrak{g}$ не имеет неподвижных точек.

13. Некоторые формулы для накрытий

Хотя приводимые ниже формулы понадобятся нам только для кривых, мы докажем их для многообразий произвольной размерности, так как это не вносит дополнительных трудностей.

Пусть X' — неприводимое *неособое* многообразие, $F' = k(X')$ — поле рациональных функций на нем и F/F' — конечное алгебраическое расширение поля F'. Обозначим через X *нормальную модель* X' в расширении F/F' (см., например, Картан и Шевалле [1], сообщение 7, или Ленг [4], гл. V). Это будет нормальное неприводимое многообразие, снабженное проекцией $g\colon X \to X'$. Имеем $k(X) = F$.

Пусть $P' \in X'$. Точек $P \in X$, проектирующихся в P' имеется конечное число. Можно применить теорию пересечений в силу того, что P' — *простая* точка на X'. Эта теория позволяет определить кратность e_P, а поэтому и $g^{-1}(P') = \sum_{P \to P'} e_P P$. Коротко напомним определение целого числа e_P.

Пусть A и A' — локальные кольца точек P и P'. Имеем $A' \subset A$. Максимальный идеал $\mathfrak{m}$ кольца A' порождает в A примарный идеал $\mathfrak{m}'A$. Имеем $e_P = e_A(\mathfrak{m}'A) =$ кратность идеала $\mathfrak{m}'A$ в A в смысле Шевалле — Самюэля (Самюэль [2]). Можно также показать, что e_P равно альтернированной сумме размерностей векторных пространств $\mathrm{Tor}_i^{A'}(A, k)$ над полем k. Это есть частный случай „Tor-формулы“ [1]).

В случае кривых A и A' являются кольцами дискретных нормирований и e_P равно индексу ветвления соответствующего нормирования.

Пусть теперь L — нормальное расширение F', содержа-

---

[1]) См. Серр Ж. Локальная алгебра и теория кратностей, сб. *Математика*, 7: 5 (1963), 3—93. — *Прим. перев.*

щее F, и $\mathfrak{g}$ — группа F'-автоморфизмов L (см. Бурбаки, Алгебра, гл. V. § 10, п. 9). Пусть $\mathfrak{h}$ — подгруппа $\mathfrak{g}$, образованная автоморфизмами, оставляющими инвариантными все элементы F. Если Y — нормальная модель X' в L (или нормальная модель X, что все равно), то имеем проекции

$$Y \xrightarrow{\pi} X \xrightarrow{g} X'.$$

Группа $\mathfrak{g}$ — группа автоморфизмов Y.

Предложение 20. *Для всех* $P \in X$ *имеем* $g^{-1}(g(P)) = [F : F']_i \sum \pi \circ \sigma_i(Q)$, *где* $Q \in Y$ *обладает тем свойством, что* $\pi(Q) = P$, *и* σ_i *обозначают представителей элементов* $\mathfrak{g}/\mathfrak{h}$ в $\mathfrak{g}$.

(Напомним, что $[F : F']_i$ обозначает *несепарабельную* часть степени F/F'.)

Пусть $P' = g(P)$ и $h = g \circ \pi$. Определим цикл $h^{-1}(P')$. Это линейная комбинация $\sum\limits_{\sigma \in \mathfrak{g}} n_\sigma \sigma(Q)$. Так как σ являются автоморфизмами Y, совместимыми с h, числа n_σ равны одному и тому же целому числу n. Формула проекции (см. Самюэль [2], стр.32) показывает, что $h(h^{-1}(P^1)) = [L : F'] P'$, откуда $\deg(h^{-1}(P')) = [L : F']$, что определяет целое число n. Если заметить, что $[L : F']$ равно произведению $[L : F']_i$ на порядок $[\mathfrak{g}]$ группы $\mathfrak{g}$, то получается

$$h^{-1}(P') = [L : F']_i \sum_{\sigma \in \mathfrak{g}} \sigma(Q).$$

Если теперь применить формулу проекции к π, получим

$$\pi(h^{-1}(P')) = [L : F] g^{-1}(P'). \qquad (*)$$

Но сумму $\sum\limits_{\sigma \in \mathfrak{g}} \sigma(Q)$ можно записать в виде $\sum\limits_{\alpha \in \mathfrak{h}} \sum\limits_{i} \alpha \circ \sigma_i(Q)$, и поскольку $\pi \circ \alpha = \pi$ для всех $\alpha \in \mathfrak{h}$, то

$$\pi(h^{-1}(P')) = [L : F']_i [\mathfrak{h}] \sum \pi \circ \sigma_i(Q).$$

Так как $[L : F] = [L : F]_i [\mathfrak{g}]$ и $[L : F']_i = [L : F]_i [F : F']_i$, получаем наконец

$$\pi(h^{-1}(P')) = [L : F] [F : F']_i \sum \pi \circ \sigma_i(Q). \qquad (**)$$

Предложение 20 следует из сравнения (*) и (**).

Замечание. Предположим, что накрытие $g: X \to X'$ *сепарабельно*, т. е. что $[F : F']_i = 1$. Если $f \in k(X)$, то справедлива следующая формула, аналогичная формуле из предложения 20:

$$(\mathrm{Tr}_g f) \circ \pi = \sum f \circ \pi \circ \sigma_i.$$

Та же формула справедлива для дифференциальных форм [так как их можно записать в виде $\sum f_i \omega'_i$, где $f_i \in k(X)$, а ω'_i — дифференциальные формы на X', и применить формулу к функциям f_i].

14. Симметрические произведения

Пусть X — алгебраическое многообразие. В этом и следующем пунктах мы предполагаем, что *любое конечное подмножество в X содержится в открытом аффинном множестве* (см. п. 12). Пусть n — целое число $\geqslant 1$. Обозначим через $\mathfrak{S}_n$ симметрическую группу степени n. Пусть $\mathfrak{S}_n$ действует на X^n, переставляя множители. Тогда пара $(X^n, \mathfrak{S}_n)$ удовлетворяет условиям предложения 19. Фактормногообразие $X^n/\mathfrak{S}_n$ является, таким образом, алгебраическим многообразием, которое называется *симметрическим произведением n экземпляров X* и обозначается через $X^{(n)}$.

Согласно этому определению, точку $M \in X^{(n)}$ можно отождествить с формальной суммой $\sum\limits_{P \in X} n_P P$, где $n_P \geqslant 0$ и $\sum n_P = n$, другими словами, с *положительным 0-мерным циклом степени n*. Легко проверяется, что когда X - проективное многообразие, то $X^{(n)}$ изоморфно многообразию „точек Чжоу" рассматриваемых циклов.

Если X неприводимо, то и $X^{(n)}$ неприводимо. Такую же зависимость получаем для нормальности. Если X — *неособая кривая*, то $X^{(n)}$ без особенностей. В этом можно убедиться либо с помощью явного нахождения пополнений локальных колец $X^{(n)}$, либо с помощью рассмотрения случая проективной прямой [когда $X^{(n)} = \mathbf{P}_n(k)$, которое явно без особенностей], пользуясь тем, что любая кривая является накрытием прямой и что можно вложить это накрытие в неразветвленное в данных точках накрытие. Напротив, если X — многообразие размерности $\geqslant 2$ и $n \geqslant 2$, то симметрическое произведение $X^{(n)}$ всегда обладает особенностями.

Если сопоставить каждой точке $P \in X$ точку $X^{(n)}$, соответствующую циклу nP, то получим инъективное отображение: δ_n: $X \to X^{(n)}$. Это отображение регулярно, поскольку оно является композицией диагонального отображения $X \to X^n$ и канонической проекции $X^n \to X^{(n)}$. По определению топологии $X^{(n)}$ это отображение является гомеоморфизмом X на подмногообразие $X^{(n)}$. В случае когда n взаимно просто с характеристикой p поля констант, легко видеть, что этот гомеоморфизм бирегулярен. Это неверно в общем случае, как показывает

Предложение 21. *Если $n = p^m$, где $m \geqslant 0$, то пучок функций, индуцированных на $\delta_n(X)$ регулярными функциями $X^{(n)}$, совпадает с пучком p^m-х степеней пучка $\mathfrak{O}_X$, перенесенного с помощью δ_n.*

[Пусть X_m — алгебраическое многообразие, получаемое снабжением X пучком p^m-х степеней регулярных функций на X; предыдущее предложение означает, что δ_n — бирегулярный изоморфизм X_m на $\delta_n(X)$, снабженном структурой, индуцированной с $X^{(n)}$.]

Рассматриваемая ситуация локальна, а потому X можно предполагать аффинным. Пусть A — координатное кольцо X. Координатное кольцо X^n есть n-я тензорная степень A (обозначим его через A_n), а координатное кольцо $X^{(n)}$—подкольцо A_n, образованное элементами, инвариантными относительно группы $\mathfrak{S}_n$. Достаточно, таким образом, доказать следующую лемму.

Лемма 11. *Пусть A — коммутативная алгебра над полем k характеристики p и $n = p^m$ — произвольная степень p. Пусть $A_n = A \otimes \ldots \otimes A$ (n раз) и B_n — подалгебра A_n, образованная элементами, инвариантными относительно симметрической группы $\mathfrak{S}_n$. Пусть $u: A_n \to A$ — гомоморфизм, определяемый формулой*

$$u(a_1 \otimes \ldots \otimes a_n) = a_1 \ldots a_n.$$

Тогда $u(B_n) = k \cdot A^n$ и $u(B_n) = A^n$, если k совершенно.

(Для сокращения записи через A^n обозначается множество элементов A, являющихся n-ми степенями; в силу того, что n — степень характеристики, A^n — подкольцо.)

Так как $u(a \otimes \ldots \otimes a) = a^n$, то $u(B_n) \supset A^n$, и поскольку u — гомоморфизм алгебр, это дает включение $u(B_n) \supset k \cdot A^n$. Покажем, что верно и обратное включение $u(B_n) \subset k \cdot A^n$. Пусть a_i — базис A. Произведения $\alpha = a_i \otimes \ldots \otimes a_{i_n}$ образуют базис A_n. Пусть $\mathfrak{t}_\alpha$ — подгруппа $\mathfrak{S}_n$, образованная перестановками, оставляющими на месте α. Положим (как обычно в теории симметрических функций)

$$S(\alpha) = \sum \sigma_i(\alpha),$$

где σ_i пробегают систему представителей $\mathfrak{S}_n/\mathfrak{t}_\alpha$. Ясно, что $S(\alpha)$ образуют базис B_n, и, следовательно, достаточно доказать, что $u(S(\alpha)) \in A^n$ для всех α. Но

$$u(S(\alpha)) = n_\alpha \cdot a_{i_1}, \ \ldots, \ a_{i_n}, \text{ где } n_\alpha = (\mathfrak{S}_n : \mathfrak{t}_\alpha).$$

Рассмотрим два случая:

1) $a_{i_1} = \ldots = a_{i_n} = a$. Тогда $\mathfrak{t}_\alpha = \mathfrak{S}_n$ и $u(S(\alpha)) = a^n$.

2) a_{ij} не все равны между собой. В этом случае $\mathfrak{t}_\alpha$ является произведением симметрических групп степеней $< n = p^m$. Индекс $\mathfrak{t}_\alpha$ в $\mathfrak{S}_n$ делится в этом случае на n. Действительно, в противном случае p-подгруппа Силова $\mathfrak{t}_\alpha$ будет также p-подгруппой Силова $\mathfrak{S}_n$. Однако $\mathfrak{S}_n$ содержит циклическую подгруппу порядка p^m, тогда как $\mathfrak{t}_\alpha$ ее не содержит. Поскольку p делит $(\mathfrak{S}_n : \mathfrak{t}_\alpha)$, то $u(S(\alpha)) = 0$, что и завершает доказательство.

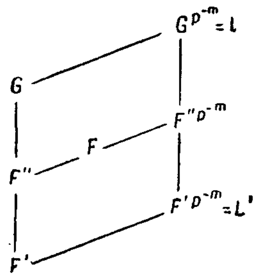
15. Симметрические произведения и накрытия

Пусть g: $X \to X'$ — накрытие, удовлетворяющее условиям п. 13. Таким образом, многообразие X' неприводимо и без особенностей, а многообразие X является его нормальной моделью в конечном расширении F/F' его поля функций. Для всех $P' \in X'$ определен цикл $g^{-1}(P')$. Его степень r равна $[F : F']$, а следовательно, его можно рассматривать как элемент симметрического произведения $X^{(r)}$. Обозначим его через $g^*(P')$.

Предложение 22. *Отображение g^*: $X' \to X^{(r)}$ всюду регулярно.*

Положим $n = [F : F']_i$ и $s = [F : F']_s$, $ns = r$. Целое число n равно степени характеристики p^m. Мы начнем с построения некоторого нормального расширения L поля F', содержащего F и дающего возможность применить предложение 20.

Пусть F'' — максимальное сепарабельное расширение F', содержащееся в F, и пусть G — нормальное расширение F', содержащее F'' (см. диаграмму ниже).



Положим $L = G^{p^{-m}}$. Отображение $x \to x^{p^{-m}}$ показывает, что L — нормальное расширение поля $L' = F'^{p^{-m}}$, имеющее ту же группу Галуа $\mathfrak{g}$, что и расширение G/F. Следовательно, это расширение будет нормальным расширением F'. Кроме того, поскольку

$$[F : F']_i = [F : F''] = p^m,$$

то $F \subset F''^{p^{-m}} \subset L$.

Пусть Y — (соответственно Y') нормальная модель X' в расширении L/F' (соответственно L'/F'). Проекция h: $Y \to X'$ разлагается в $Y \xrightarrow{\pi} X \xrightarrow{g} X'$, а также в $Y \to Y' \to X'$. По построению $Y' = Y/\mathfrak{g}$ и $X' = Y'_m$ (заметим, что Y'_m — многообразие, получаемое из Y' с помощью пучка p-х степеней его локальных колец, см. п. 14).

Применим теперь предложение 20: если $\mathfrak{h}$ обозначает подгруппу $\mathfrak{g}$, соответствующую полю F'', и σ_i — представители в $\mathfrak{g}$ элементов $\mathfrak{g}/\mathfrak{h}$, то

$$g^{-1}(P') = p^m \sum_{i=1}^{i=s} \pi \circ \sigma_i (Q), \quad \text{где} \quad h(Q) = P'.$$

Отбросим сначала множитель p^m и рассмотрим отображение $Q \to \sum \pi \circ \sigma_i (Q)$. Это регулярное отображение Y в симметрическое произведение $X^{(s)}$. Действительно, его можно разложить в регулярные отображения $Y \to Y^s \to X^s \to X^{(s)}$. Кроме того, это отображение инвариантно относительно $\mathfrak{g}$ и, следовательно, определяет при переходе к фактору регулярное отображение α: $Y/\mathfrak{g} = Y' \to X^{(s)}$. Положим $Z = X^{(s)}$ и пусть Z_m — многообразие, получаемое наделением Z пучком p^m-степеней его локальных колец. Отображение α определяет регулярное отображение α_m: $Y'_m \to Z_m$. С другой стороны, предложение 21, примененное к Z, дает регулярное отображение δ'_n: $Z_m \to Z^{(n)}$. Многообразие $Z^{(n)} = \left(X^{(s)}\right)^{(n)}$ есть фактор $X^{ns} = X^r$ по подгруппе $\mathfrak{S}_r$. Следовательно, имеется каноническая проекция $(X^{(s)})^{(n)} \xrightarrow{\gamma} X^{(r)}$.

Беря композицию

$$X' \xrightarrow{\alpha_m} Z_m \xrightarrow{\gamma'_n} (X^{(s)})^{(n)} \xrightarrow{\gamma} X^{(r)},$$

получаем регулярное отображение, и предложение 20 означает, что это отображение совпадает с g^*.

Замечания. 1. Предположение, что X без особенностей, нужно только для того, чтобы $g^{-1}(P')$ имело смысл. В самом деле, если g: $X \to X'$ — некоторое накрытие (причем X и X' — нормальные многообразия), то можно *определить* $g^{-1}(P')$ для $P' \in X'$ с помощью формулы предложения 20, и по-прежнему справедливо доказательство, которое только что было проведено.

2. В случае кривых имеем $F = F''^{p-m}$, что немного упрощает доказательство. Из всех случаев достаточно рассмотреть два: сепарабельный случай, который немедленно ис-

следуется с помощью теории Галуа, и радикальный случай, который следует из предложения 21.

Библиографические замечания

Теорема 1, являющаяся главным результатом главы, доказана Розенлихтом [3]. Его доказательство приведено в этой главе без существенных изменений.

Локальные символы § 1 возникли из символов в полях классов (см. Шмид [1]), которые, впрочем, переоткрываются в гл. VI, § 6.

Локальные символы относительно групп G_m описаны Тейтом (не опубликовано). Формула взаимности $f((g)) = g((f))$ известна давно. Она фигурирует в заметке А. Вейля 1940 г. о гипотезе Римана [2], а в 1956 г. Игуза дал прямое доказательство этой формулы [3]. Недавно Ленг доказал, что ее можно рассматривать как частный случай общей формулы взаимности для абелевых многообразий (см. Ленг [5], гл. VI, § 4).

„Теорема Шевалле“, сформулированная в п. 7, доказана Барсотти [2] и Розенлихтом [4]. Сам Шевалле никогда не публиковал своего доказательства. Разложение линейной связной коммутативной группы в произведение тора и унипотентной группы (предложение 12) принадлежит Колчину [1] (см. также Борель [2]). Было бы интересно обойтись без теорем о структуре алгебраических групп, как это можно сделать в случае характеристики 0.

Касательные вектора и дифференциальные формы вообще рассматриваются в литературе с „бирациональной“ точки зрения, что недостаточно. Мы ограничились сообщением некоторых элементарных результатов, которые нам были нужны (см. также Розенлихт [5]).

Фактормногообразия $V/\mathfrak{g}$ можно определить в нормальном случае с помощью „точек Чжоу“. Относительно общего случая см. Серр [5], где имеются некоторые дополнительные результаты об их локальных кольцах.

Соотношения между симметрическими произведениями и накрытиями почти эквивалентны „теореме о симметрических функциях“ А. Вейля ([5], § 1). В обоих случаях существо дела заключается в лемме 11.

ГЛАВА

IV

АЛГЕБРАИЧЕСКИЕ КРИВЫЕ С ОСОБЕННОСТЯМИ

Основная цель этой главы — подготовка к построению в следующей главе *обобщенных якобиевых многообразий.* Некоторые результаты имеют, впрочем, самостоятельный интерес ввиду их приложений в теории поверхностей.

Здесь опять не рассматриваются вопросы рациональности. Мы предполагаем, что основное поле k алгебраически замкнуто.

§ 1. Строение кривой с особенностями

1. Нормальная модель алгебраического многообразия

Начнем с краткого изложения построения и элементарных свойств нормальной модели алгебраического многообразия. Детали можно найти у Картана — Шевалле [1] или у Ленга [4].

Пусть X' — неприводимое алгебраическое многообразие, $\mathcal{O}'$ — пучок его локальных колец и $k(X') = K$ — поле рациональных функций на X. Для всех точек $Q \in X'$ мы обозначаем через $\mathcal{O}_Q$ *целое замыкание* кольца $\mathcal{O}'_Q$ в его поле частных K. Если U' — открытое аффинное множество в X' и $A' = H^0(U', \mathcal{O}')$ — соответствующее координатное кольцо, то целое замыкание A кольца A' в K есть A'-модуль конечного типа, соответствующий нормальному аффинному многообразию U с канонической проекцией p: $U \to U'$. После склеивания многообразий U мы получаем нормальное алгебраическое многообразие X, которое называется *нормальной моделью* для X'. Сразу же проверяется, что для всех $Q \in X'$ имеем $\mathcal{O}_Q = \bigcap_{P \to Q} \mathcal{O}_P$, где $\mathcal{O}_P$ обозначает локальное кольцо точки $P \in X$, проектирующейся в Q (таких точек имеется конечное число). Пучок $\mathcal{O}$[1]) на X' является, таким образом, *прямым образом*[2]) $p(\mathcal{O}_X)$ пучка локальных колец $\mathcal{O}_X$ на X.

Аннулятор $\mathfrak{c}$ пучка модулей $\mathcal{O}/\mathcal{O}'$[2]) называется *кондуктором* $\mathcal{O}$ в $\mathcal{O}'$. Это когерентный пучок идеалов на X'. Его многообразие S' является множеством точек X', локальные кольца которых нецелозамкнуты. Если положить $S = p^{-1}(S')$, то проекция p есть *бирегулярный изоморфизм* $X - S$ на $X' - S'$. Если Q — точка X', то локальный идеал $\mathfrak{c}_Q$ является множеством элементов $f \in \mathcal{O}'_Q$, таких, что из $g \in \mathcal{O}_Q$ следует $fg \in \mathcal{O}'_Q$. Можно также сказать, что $\mathfrak{c}_Q$ — наибольший идеал в $\mathcal{O}'_Q$, являющийся в то же время идеалом $\mathcal{O}_Q$. Имеем включения

$$\mathcal{O}_Q \supset k + \mathfrak{r}_Q \supset \mathcal{O}'_Q \supset k + \mathfrak{c}_Q, \tag{1}$$

где $\mathfrak{r}_Q$ обозначает *радикал* полулокального кольца $\mathcal{O}_Q$, другими словами, множество $f \in \mathcal{O}_Q$, принимающих нулевое значение во всех точках P, проектирующихся в Q.

2. Случай алгебраической кривой

Если X и X' — *алгебраические кривые*, то множества S и S' имеют нулевую размерность, другими словами, являются конечными подмножествами X и X'. Более того, S' есть множество *особых* точек X'. Действительно, известно, что если $\mathfrak{o}$ — целое локальное кольцо размерности 1, то условия „$\mathfrak{o}$ целозамкнуто“ и „$\mathfrak{o}$ регулярно“ эквивалентны.

Когерентный пучок $\mathcal{O}/\mathcal{O}'$ сосредоточен на S'. Отсюда следует, что для всех $Q \in X'$ имеем $\dim_k \mathcal{O}_Q/\mathcal{O}'_Q < +\infty$.

---

[1]) Здесь $\mathcal{O}$ обозначает пучок на X', образованный кольцами $\mathcal{O}_Q$. — *Прим. перев.*

[2]) Пусть $p\colon X \to Y$ — регулярное отображение, $\mathcal{F}$ — пучок на X. Тогда прямой образ $p_*(\mathcal{F})$ есть пучок, полученный из предпучка $\{F_U\}$, где $F_U = \Gamma(p^{-1}(U), \mathcal{F})$. На самом деле можно показать, что этот предпучок является пучком, а потому $\Gamma(U, p_*(\mathcal{F})) = \Gamma(p^{-1}(U), \mathcal{F})$. — *Прим. перев.*

Положим

$$\delta_Q = \dim_k \mathfrak{O}_Q / \mathfrak{O}'_Q, \quad Q \in X'. \tag{2}$$

Из предыдущего следует

Предложение 1. *Целое число δ_Q положительно тогда и только тогда, когда Q — особая точка X'.*

Заметим, что δ_Q — *инвариант относительно пополнения*:

$$\delta_Q = \dim_k \widehat{\mathfrak{O}}_Q / \widehat{\mathfrak{O}}'_Q. \tag{3}$$

Это немедленно следует из того, что $\mathfrak{O}_Q/\mathfrak{O}'_Q$ имеет конечную размерность.

Из (3) следует, что две особые точки, „аналитически изоморфные" (т. е. имеющие одинаковые пополнения локальных колец), имеют одно и то же δ_Q. Иначе говоря, δ_Q — *аналитический инвариант*. Из того, что $\mathfrak{O}_Q/\mathfrak{O}'_Q$ — векторное конечномерное пространство над полем k, следует, что то же самое верно и для $\mathfrak{O}'_Q/\mathfrak{c}_Q$, а следовательно, и для $\mathfrak{O}_Q/\mathfrak{c}_Q$. Идеал $\mathfrak{c}_Q$ содержит в этом случае степень $\mathfrak{r}_Q^n$ радикала $\mathfrak{r}_Q$ кольца $\mathfrak{O}_Q$, и включения (1) дают включения

$$k + \mathfrak{r}_Q \supset \mathfrak{O}'_Q \supset k + \mathfrak{r}_Q^n. \tag{4}$$

Замечание. Все предыдущее изложение проходит для алгебраического многообразия произвольной размерности при единственном условии, что множество точек, локальные кольца которых нецелозамкнуты, *конечно*.

3. Построение кривой с особенностями по ее нормальной модели

В предыдущем пункте мы исходили из X' при построении X; теперь мы будем, наоборот, строить X' по X.

Пусть X — неприводимая и неособая алгебраическая кривая; $\mathfrak{O}$ — пучок ее локальных колец и $K = k(X)$. Фиксируем конечное подмножество S кривой X и некоторое соотношение эквивалентности R на S. Положим $S' = S/R$ и определим X' как сумму множеств $X - S$ и S'. Имеем, таким образом, каноническую проекцию $p\colon X \to X'$. Если $Q \in X'$, то полагаем $\mathcal{O}_Q = \bigcap_{P \to Q} \mathcal{O}_P$ и обозначаем через $\mathfrak{r}_Q$ радикал $\mathcal{O}_Q$. Задавая также для каждого $Q \in S'$ подкольцо $\mathcal{O}'_Q$ кольца $\mathcal{O}_Q$, отличное от $\mathcal{O}_Q$, проверяем включения (4) для некоторого целого n. Если $Q \in X' - S'$, то мы полагаем $\mathcal{O}'_Q = \mathcal{O}_Q$. Подкольца $\mathcal{O}'_Q$ образуют подпучок $\mathcal{O}'$ пучка функций на X' (X' снабжается такой топологией, в которой замкнутые подмножества являются конечными подмножествами).

Предложение 2. *Пучок $\mathcal{O}'$ снабжает X' структурой алгебраической кривой, имеющей X в качестве своей нормальной модели и S' в качестве множества особых точек.*

Докажем, что если X — аффинная кривая, то таковой же будет и X'. Общий случай следует отсюда (надо покрыть X открытыми аффинными множествами).

Пусть A — координатное кольцо для X. Для всех $P \in X$ пусть $\mathfrak{a}_P$ — максимальный идеал A, образованный функциями f, которые обращаются в нуль в P. Пусть $A' \subset K$ есть пересечение $\mathcal{O}'_Q$ по Q, пробегающим X'. Очевидно, $A' \subset A$. С другой стороны, если обозначить через $\mathfrak{r}$ пересечение $\mathfrak{a}_P$ для $P \in S$, то условия (4) показывают, что A' содержит $k + \mathfrak{r}^n$ для достаточно большого n. Так как $\mathfrak{r}^n$ имеет конечную коразмерность в A, то же справедливо и для A'. Таким образом, A — A'-модуль конечного типа и A *цело* над A'. Отсюда следует (гл. III, п. 12, лемма 10), что A' — *k-алгебра конечного типа*, соответствующая аффинному алгебраическому многообразию Y. Так как A — целое замыкание A' в K, то каноническая проекция q: $X \to Y$ показывает, что X — *нормальная* модель для Y.

Остается проверить, что Y изоморфно X'. Прежде всего пусть P_1 и P_2 — две точки X, имеющие одну и ту же проекцию Q в X'. Этим точкам соответствуют гомоморфизмы φ_i: $A \to k$ ($i = 1, 2$). Если положить $\mathfrak{r}_Q = \bigcap_{P \to Q} \mathfrak{r}_P$, то гомоморфизмы φ_1 и φ_2 будут обращаться в нуль на $\mathfrak{r}_Q$, а следовательно, они совпадают на $k + \mathfrak{r}_Q$ и тем более на A' в силу

(4). Так как имеется биективное соответствие между точками Y и гомоморфизмами $A' \to k$, то отсюда следует, что P_1 и P_2 имеют одинаковые образы в Y. Обратно, предположим, что P_1 и P_2 имеют различные образы Q_1 и Q_2 в X'. В силу того, что идеалы $\mathfrak{a}_P$ максимальны в A, можно без труда найти такую $f \in A$, что

$$\begin{aligned} &f \equiv 0 \mod \mathfrak{a}_P^n \text{ при } P \to Q_1, \\ &f \equiv 1 \mod \mathfrak{a}_P^n \text{ при } P \to Q_2 \text{ или при} \\ &\qquad\qquad P \in S \text{ и } P \not\to Q_1. \end{aligned} \tag{5}$$

Формулы (4) показывают, что $f \in A'$. Так как $f(P_1) = 0$ и $f(P_2) = 1$, точки P_1 и P_2 имеют в Y различные образы.

Таким образом, каноническое отображение $X \to X'$ определяет при переходе к фактору биекцию $X' \to Y$. Нужно показать теперь, что после отождествления X' и Y с помощью этой биекции пучки $\mathfrak{O}'$ и $\mathfrak{O}_Y$ совпадут. Включение $\mathfrak{O}_Y \subset \mathfrak{O}'$ очевидно.

Итак, пусть $f \in \mathfrak{O}'_Q$, $Q \in X'$. Покажем, что f записывается в виде

$$f = a/b, \text{ где } a \in A', \ b \in A', \ b(P) \neq 0 \text{ при } P \to Q. \tag{6}$$

Поскольку $f \in \mathfrak{O}_Q = \bigcap\limits_{P \to Q} \mathfrak{O}_P$, в любом случае $f = c/d$, где

$$c \in A, \ d \in A, \ d(P) \neq 0 \text{ при } P \to Q. \tag{7}$$

Известно, что существует $t \in A$, для которого

$$\begin{aligned} &t \equiv d^{-1} \mod \mathfrak{a}_P^{-1} \text{ при } P \to Q; \\ &t \equiv 0 \mod \mathfrak{a}_P^n \text{ при } P \in S \text{ и } P \not\to Q. \end{aligned} \tag{8}$$

Произведение td входит в $\mathfrak{O}'_R$ для всех $R \in S'$, откуда $td \in A'$ и $td(P) = 1$ при $P \to Q$. Так же tc входит в $\mathfrak{O}'_R$ для всех $R \in S'$, отличных от Q. С другой стороны, $f = ct/dt$ и $f \in \mathfrak{O}'_Q$ по предположению. Отсюда получаем, что $ct \in \mathfrak{O}'_Q$ и $ct \in A'$. Если положить $a = ct$ и $b = dt$, то условия (6) выполняются, что и завершает доказательство.

Замечание. Ситуация, изученная выше, аналогична встречающейся в арифметике, когда A — *кольцо целых чисел* в числовом поле K и A' — порядок K, т. е. подкольцо A, допускающее K в качестве поля частных. Здесь мы также имеем кондуктор $\mathfrak{c}$ кольца A в A', являющийся аннулятором A-модуля A/A'. Простые идеалы A, входящие в $\mathfrak{c}$, играют роль особых точек.

4. Особые кривые, определяемые модулем

Пусть X — неособая, полная и неприводимая кривая и $\mathfrak{m} = \sum n_P P$ — „модуль" над X (см. гл. III). Мы не рассматриваем тривиальный случай, когда $\mathfrak{m} = 0$, а также случай, когда $\mathfrak{m} = P$. Таким образом, предполагается, что $\deg(\mathfrak{m}) \geqslant 2$.

Пусть S — *носитель* $\mathfrak{m}$, другими словами, множество таких $P \in X$, для которых $n_P > 0$. Мы берем за S' множество, сводящееся к единственной точке Q, и полагаем $X' = (X - S) \cup \{Q\}$ (X' получается, таким образом, из X сжатием точек S в одну). Если $\mathfrak{c}_Q$ обозначает идеал $\mathcal{O}_Q$, образованный функциями f, удовлетворяющими условию $f \equiv 0 \bmod \mathfrak{m}$, то мы полагаем

$$\mathcal{O}'_Q = k + \mathfrak{c}_Q. \tag{9}$$

Тогда выполняются все условия п. 3 [$\mathcal{O}'_Q \neq \mathcal{O}_Q$ в силу предположения $\deg(\mathfrak{m}) \geqslant 2$]. Кривая с особенностями, полученная таким образом, будет обозначаться через $X_\mathfrak{m}$. Она имеет Q в качестве единственной особой точки и

$$\delta_Q = \dim \mathcal{O}_Q/k + \mathfrak{c}_Q = \dim \mathcal{O}_Q/\mathfrak{c}_Q - 1 = \deg(\mathfrak{m}) - 1. \tag{10}$$

Идеал $\mathfrak{c}_Q$ является кондуктором $\mathcal{O}_Q$ в $\mathcal{O}_Q$.

Примеры. а) $\mathfrak{m} = 2P$. Отображение p: $X \to X_\mathfrak{m}$ биективно, а потому можно отождествить X и $X_\mathfrak{m}$. Для $Q \neq P$ имеем $\mathcal{O}'_Q = \mathcal{O}_Q$ и $\mathcal{O}'_P$ — подкольцо $\mathcal{O}_P$, образованное функциями, чьи дифференциалы аннулируются в P. Пополнение $\mathcal{O}'_P$ является поэтому подкольцом $k[[t]]$, порождаемым t^2 и t^3. Кривая $X_\mathfrak{m}$ аналитически изоморфна в P кривой $y^2 - x^3 = 0$, В этом случае говорят, что P — *точка обыкновенного возврата*.

б) $\mathfrak{m} = P_1 + P_2$, где $P_1 \neq P_2$. Здесь $X_\mathfrak{m}$ получается из X *отождествлением* P_1 и P_2. Локальное кольцо $\mathcal{O}'_Q$ точки Q, получаемое таким образом, образовано рациональными функциями на X, регулярными в P_1 и P_2 и принимающими там одинаковые значения. Кривая $X_\mathfrak{m}$ аналитически изоморфна в Q (приводимой) кривой $xy = 0$. В этом случае говорят, что Q — *двойная точка с различными касательными*.

§ 2. Теорема Римана — Роха

5. Обозначения

К предположениям п. 2 мы присоединяем условие, что кривая X (а следовательно, также и X') *полная*. Известно, что тогда X — *проективное* многообразие (см. гл. II, п. 1). То же самое рассуждение показывает, что X' — также проективное многообразие, но этим фактом мы не будем пользоваться.

Обозначим через g *род* кривой X и положим

$$\delta = \sum_{Q \in S'} \delta_Q, \tag{11}$$

$$\pi = g + \delta. \tag{12}$$

Пусть D — дивизор на X, равный нулю на S. Этот дивизор определяет на X пучок $\mathcal{L}(D)$ (см. гл. II, п. 6). Поскольку $X - S$ бирегулярно изоморфно $X' - S'$, можно перенести этот пучок на $X' - S'$ и дополнить его кольцами $\mathcal{O}'_Q$ для $Q \in S'$. Таким образом, получается подпучок $\mathcal{L}'(D)$ постоянного пучка K на X'. По определению имеем

$$\mathcal{L}'(D)_Q = \begin{cases} \mathcal{O}'_Q & \text{при } Q \in S'; \\ \mathcal{L}(D)_Q & \text{при } Q \notin S'. \end{cases} \tag{13}$$

По аналогии со случаем неособой кривой положим

$$\begin{gathered} L'(D) = H^0(X', \mathcal{L}'(D)), \quad I'(D) = H^1(X', \mathcal{L}'(D)), \\ l'(D) = \dim L'(D), \quad i'(D) = \dim I'(D). \end{gathered} \tag{14}$$

Поскольку пучок $\mathcal{L}'(D)$ локально изоморфен пучку $\mathcal{O}'$, пучок $\mathcal{L}'(D)$ когерентен и предыдущие группы когомологий *конечномерны* (что следует, впрочем, также из доказательства теоремы 1 ниже).

В частном случае, когда X' является кривой $X_\mathfrak{m}$, ассоциированной с модулем $\mathfrak{m}$ (см. п. 4), мы пишем $L_\mathfrak{m}(D)$, $I_\mathfrak{m}(D)$, $l_\mathfrak{m}(D)$, $i_\mathfrak{m}(D)$ вместо $L'(D)$, $I'(D)$, $l'(D)$, $i'(D)$.

6. Теорема Римана — Роха (основная форма)

Теорема 1. *Для всех дивизоров D, носитель которых не пересекается с S, имеем*

$$l'(D) - i'(D) = \deg(D) + 1 - \pi. \tag{16}$$

Положим $\chi'(D) = l'(D) - i'(D)$. Рассуждения гл. II, п. 4 (основанные на точной последовательности когомологий) показывают, что

$$\chi'(D+P) = \chi'(D) + 1$$

для всех $P \in X' - S'$. Так как та же формула верна для выражения $\deg(D) + 1 - \pi$, мы видим, что можно свести доказательство теоремы 1 к частному случаю $D = 0$.

В этом случае $\mathcal{L}'(D) = \mathcal{O}'$, и все сводится к доказательству того, что характеристика Эйлера — Пуанкаре $\chi(X', \mathcal{O}')$ пучка $\mathcal{O}'$ равна $1 - \pi$. Но пучок $\mathcal{O}'$ является подпучком пучка $\mathcal{O}$, образа пучка локальных колец X (см. п. 1). Получаем точную последовательность

$$0 \to \mathcal{O}' \to \mathcal{O} \to \mathcal{O}/\mathcal{O}' \to 0,$$

откуда

$$\chi(X', \mathcal{O}') = \chi(X', \mathcal{O}) - \chi(X', \mathcal{O}/\mathcal{O}').$$

Пучок $\mathcal{O}/\mathcal{O}'$ сосредоточен на конечном множестве S. Отсюда следует, что

$$\chi(X', \mathcal{O}/\mathcal{O}') = \dim H^0(X', \mathcal{O}/\mathcal{O}') = \sum_{Q \in S'} \dim \mathcal{O}_Q/\mathcal{O}'_Q = \delta.$$

Учитывая определение π, видим, что достаточно доказать равенство

$$\chi(X', \mathcal{O}) = 1 - g.$$

Но, поскольку g — род X, имеем $\chi(X, \mathfrak{O}) = 1 - g$[1]) (см. гл. II). Теорема 1 будет, таким образом, доказана после установления следующего результата.

Лемма 1. *Если алгебраическое многообразие X — нормальная модель алгебраического многообразия X', то*

$$H^q(X, \mathfrak{O}) = H^q(X', \mathfrak{O}) \text{ для всех } q \geqslant 0.$$

Когда $q = 0$, $H^q(X', \mathfrak{O})$ является множеством рациональных функций $f \in k(X)$, входящих во все $\mathfrak{O}_Q$, $Q \in X'$. Так как $\mathfrak{O}_Q = \bigcap_{P \to Q} \mathfrak{O}_P$, то $H^0(X', \mathfrak{O})$ есть также множество $f \in k(X)$, входящих во все $\mathfrak{O}_P$, $P \in X$. Отсюда следует требуемое равенство

$$H^0(X', \mathfrak{O}) = H^0(X, \mathfrak{O}). \tag{17}$$

Пусть теперь $\mathfrak{U}' = \{U'_i\}$ — покрытие X' открытыми аффинными множествами и $\mathfrak{U}$ — покрытие X множествами $U_i = p^{-1}(U'_i)$. В силу построения X U_i — тоже открытые аффинные множества и

$$H^q(X', \mathfrak{O}) = H^q(\mathfrak{U}', \mathfrak{O}), \quad H^q(X, \mathfrak{O}) = H^q(\mathfrak{U}, \mathfrak{O}).$$

Но, применяя (17) к многообразиям $U'_{i_0} \cap U'_{i_1} \cap \ldots \cap U'_{i_q}$ и их нормальным моделям $U_{i_0} \cap U_{i_0} \cap \ldots \cap U_{i_q}$, видим, что канонический гомоморфизм $C(\mathfrak{U}', \mathfrak{O}) \to C(\mathfrak{U}, \mathfrak{O})$ биективен [через $C(\mathfrak{U}, \mathfrak{O})$ обозначается комплекс, соответствующий покрытию $\mathfrak{U}$ и пучку $\mathfrak{O}$; см. АКП, п. 18], а следовательно, биективен и гомоморфизм $H^q(\mathfrak{U}', \mathfrak{O}) \to H^q(\mathfrak{U}, \mathfrak{O})$.

Следствие. $\pi = i'(0) = \dim H^1(X', \mathfrak{O}')$.

Применяя формулу (16) к дивизору $D = 0$ в силу того, что $l'(0) = 1$, получаем данное следствие.

Пример. Пусть k' — подполе поля k и F' — „поле функций от одного переменного" над k'. Мы подразумеваем под этим, что F' — регулярное расширение k' (в смысле Вейля [3],

[1]) Здесь и далее пучок локальных колец X и его прямой образ обозначаются одной и той же буквой $\mathfrak{O}$. — *Прим. перев.*

гл. I) степени трансцендентности 1 над k'. Этому полю соответствует алгебраическая проективная кривая X', определенная над k', неприводимая и k'-нормальная. После расширения поля констант до k можно рассматривать X' также и над k, причем тогда X' уже не обязательно нормальна (т. е. неособа). Предыдущее следствие и соображения о распределениях, аналогичные приведенным в гл. II, п. 5, показывают, что целое число π, поставленное в соответствие с X', совпадает с родом расширения F'/k' (в смысле Шевалле [1]). Соотношение $\pi = g + \delta$, где $\delta \geqslant 0$, очевидно, означает *убывание рода* (там же, гл. V, § 6.)

7. Приложение к вычислению рода алгебраической кривой

Предположим, что кривая X' вложена в проективное пространство $\mathbf{P}_r$. Как и для всякого проективного многообразия, для нее определен арифметический род $p_a(X')$. Напомним (см., например, Зарисский [2]), что если $\chi(X')$ - постоянный член характеристического полинома Гильберта X' в $\mathbf{P}_r$, то по определению

$$1 - p_a(X') = \chi(X').$$

Предложение 3. $p_a(X') = \pi = g + \delta$.

Действительно, известно (АПК, п. 80), что для любого проективного многообразия X' целое число $\chi(X')$ равно альтернированной сумме размерностей $H^q(X', \mathcal{O}')$. Здесь мы имеем

$$\dim H^0(X', \mathcal{O}') = 1,$$

поскольку X' связна и мы видели, что $\dim H^1(X', \mathcal{O}') = \pi$. Группы $H^q(X', \mathcal{O}')$ $(q \geqslant 2)$ равны нулю. Следовательно, $\chi(X') = 1 - \pi$, откуда предложение 3 следует по формуле для $p_a(X')$.

Предыдущее предложение представляет интерес в силу того, что позволяет свести вычисление рода g к более простому (как станет видно далее) вычислению арифметического рода π и (чисто локальному) вычислению целого числа δ. Если

X' имеет только „простые“ особенности (двойные точки с различными касательными или точки обыкновенного возврата; см. п. 4), то δ есть просто *число* особых точек.

Рассмотрим, например, случай, когда X' — *полное пересечение* в $\mathbf{P}_r$ $r-1$ гиперповерхностей степеней $a_1, \ldots, a_{r-1}$ (это означает, что идеал, определяемый X' в $k[X_0, \ldots, X_r]$, порожден $r-1$ однородными полиномами степени $a_1, \ldots, a_{r-1}$). Вычисление группы когомологий $H^1(X', \mathcal{O}')$ не представляет труда (см. АКП, п. 78, где рассматривается случай полного пересечения произвольной размерности), и мы получаем

$$\pi = \frac{1}{2} a_1 a_2 \ldots a_{r-1} a + 1, \quad \text{где} \quad a = \sum a_i - r - 1. \tag{18}$$

При $r=2$ это *формула Плюккера*, дающая род плоской кривой степени d:

$$g = \frac{1}{2} d(d-3) + 1 - \delta. \tag{19}$$

8. Род кривой на поверхности

Пусть V — проективная поверхность без особенностей и X' — кривая, лежащая на V. В случае когда V — плоскость $\mathbf{P}_2$, формула Плюккера показывает, что $p_a(X')$ зависит только от „численного“ инварианта X' — ее степени. Мы увидим, что это справедливо и в общем случае.

Уточним сначала некоторые обозначения (все эти обозначения принадлежат Зарисскому [2], [3]).

Пусть D — дивизор на V. Мы пишем $D \sim 0$ и говорим, что D *линейно эквивалентен* 0, если D — дивизор (φ) рациональной функции φ на V.

Через K обозначается дивизор рациональной дифференциальной формы степени 2, не равной тождественно нулю. Это *канонический дивизор* V, определяемый с точностью до линейной эквивалентности.

Если D_1 и D_2 — два дивизора, то им можно сопоставить целое число, обозначаемое через $(D_1 \cdot D_2)$[1]), которое харак-

---

[1]) У автора оно обозначено через $D_1 \cdot D_2$; мы воспользовались принятым в нашей литературе обозначением $(D_1 \cdot D_2)$. — *Прим. перев.*

теризуется следующими свойствами: $(D_1 \cdot D_2)$ билинейно, равно нулю, если $D_1 \sim 0$ или $D_2 \sim 0$, и совпадает со степенью цикла пересечения $D_1 \cdot {}_V D_2$, когда последняя определена (т. е. когда D_1 и D_2 не имеют общей неприводимой компоненты). Имеет место равенство

$$(D_1 \cdot D_2) = (D_2 \cdot D_1).$$

Лемма 2. *Если X — неособая кривая рода g, лежащая на V, то*

$$2g - 2 = X \cdot (X + K). \tag{20}$$

Можно найти дифференциальную форму ω степени 2, дивизор которой K содержит X с кратностью -1. Положим $K = -X + D$, где X не входит в D. Поскольку ω имеет X в качестве многообразия полюсов кратности 1, *вычет* $\operatorname{Res}_X(\omega)$ на X вполне определен: если t — рациональная функция, обращающаяся на X в нуль с кратностью 1, то можно записать ω в виде $\omega = dt/t \wedge \alpha$ и $\operatorname{Res}_X(\omega)$ есть ограничение на X дифференциальной формы α степени 1. Легко проверяется, что $\operatorname{Res}_X(\omega)$ не зависит от выбора t. Это определение показывает, что дивизор K_X на X формы ω равен циклу пересечения $X_V \cdot D$, и так как $\deg(K_X) = 2g-2$ (гл. II, п. 9), получаем $2g - 2 = (X \cdot D) = (X \cdot (X + K))$, что и доказывает лемму.

Для произвольного дивизора D на V обозначим через $\mathscr{L}(D)$ пучок ростков функций, дивизоры которых локально $\geqslant -D$. Если $D \sim D'$, то пучок $\mathscr{L}(D)$ изоморфен пучку $\mathscr{L}(D')$.

С другой стороны, для всех алгебраических когерентных пучков $\mathscr{F}$ на V полагаем $\chi(V, \mathscr{F}) = \sum (-1)^i \dim H^i(V, \mathscr{F})$ (см. АКП, п. 79). Вместо $\chi(V, \mathscr{O}_V)$ мы пишем $\chi(V)$. В соответствии с классическими определениями (см. Зарисский [2], [3]) имеем $\chi(V) = 1 + p_a(V)$.

Предложение 4. *Для всех дивизоров D на V имеем*

$$\chi(V, \mathscr{L}(D)) = \chi(V) + \frac{1}{2}(D \cdot (D - K)). \tag{21}$$

Предположим сначала, что $D = -X$, где X без особенностей. Пучок $\mathscr{L}(D)$ есть пучок идеалов, определенный с помощью X. Отсюда следует, что имеет место точная последовательность

$$0 \to \mathscr{L}(D) \to \mathcal{O}_V \to \mathcal{O}_X \to 0.$$

После перехода к характеристикам Эйлера — Пуанкаре получаем

$$\chi(V, \mathscr{L}(D)) = \chi(V) - \chi(X).$$

Так как $\chi(X) = 1 - g = -\frac{1}{2}(X \cdot (X + K))$, формула (21) доказана в этом случае.

Теперь мы сведем общий случай к случаю только что разобранному. Пусть E — гиперплоское сечение V. Применяя к пучку $\mathscr{L}(-D)$ результаты из АКП, п. 66 (или рассуждая непосредственно), мы видим, что полная линейная система $|-D + nE|$ определяет бирегулярное погружение V в проективное пространство при условии, что n достаточно велико. Беря „общее" гиперплоское сечение в этом погружении, получаем неприводимую неособую кривую X_n, такую, что $-D + nE \sim X_n$, т. е. $D - nE \sim -X_n$. Формула (21) верна для $-X_n$, а следовательно, она справедлива и для $D - nE$. Однако оба члена этой формулы — полиномы от n. Это очевидно для правого члена, а для левого следует из элементарной теоремы о когерентных пучках (АКП, п. 80, предложение 3). Эти полиномы совпадают для достаточно больших n, а следовательно, и для всех n, в частности, для $n = 0$.

Предложение 5. *Пусть X' — особая неприводимая кривая, лежащая на V, и $p_a(X') = \pi$ — ее арифметический род. Тогда*

$$p_a(X') = 1 + \frac{1}{2}(X' \cdot (X' + K)). \qquad (22)$$

Здесь снова имеем точную последовательность пучков

$$0 \to \mathscr{L}(-X') \to \mathcal{O}_V \to \mathcal{O}_{X'} \to 0,$$

откуда следует равенство $\chi(V, \mathscr{L}(-X')) = \chi(V) - \chi(X')$. Применяя (21) и принимая во внимание, что $\chi(X') = 1 - p_a(X')$, получаем формулу (22).

Примеры. 1. В случае когда $V = \mathbf{P}_2$, канонический класс K равен $-3E$, где E обозначает прямую. Если d — степень кривой X', то $X' \sim dE$, откуда $(X' \cdot X') = d^2$ и

$(X \cdot K') = -3d$. Формула (22) в этом случае снова дает формулу Плюккера.

2. В случае когда V — *квадрика* (другими словами, произведение двух проективных прямых), группа классов дивизоров имеет две образующие E_1 и E_2 различных систем и $K \sim -2E_1 - 2E_2$. Если положить $(X' \cdot E_1) = d_1$ и $(X' \cdot E_2) = d_2$, то формула (22) даст *формулу С. Сегре*

$$\pi = d_1 d_2 - d_1 - d_2 - 1. \tag{23}$$

Каждый раз, когда определена база группы классов дивизоров на V (относительно численной эквивалентности), имеем аналогичную формулу.

Замечания. 1. Для всех дивизоров D на V положим $p_a(D) = 1 + \frac{1}{2}(D \cdot (D + K))$. Целое число $p_a(D)$ называется *виртуальным арифметическим родом* дивизора D (см. Зарисский [2]).

2. Положим $l(D) = \dim H^0(V, \mathcal{L}(D))$. По теореме двойственности (см. гл. II, п. 10, а также Серр [2] и доклад Зарисского [3]) $\dim H^2(V, \mathcal{L}(D)) = l(K - D)$. Так как $\sup(D) = \dim H^1(V, \mathcal{L}(D))$ всегда $\geqslant 0$, то формула (21) дает *неравенство Римана — Роха для поверхностей*

$$l(D) + l(K - D) \geqslant 1 + p_a(V) + \frac{1}{2}(D \cdot (D - K)). \tag{24}$$

Теорема Римана—Роха, собственно говоря (в форме Хирцебруха [1] в классическом случае и Гротендика [3] в общем случае), более точна, чем формула (21): она утверждает, кроме того, что $\chi(V)$ равна $\frac{1}{12}((K \cdot K) + K_0)$, где K_0 обозначает степень „канонического класса" размерности 0 на V.

§ 3. Дифференциалы на особой кривой

9. Регулярные дифференциалы на X'

Мы сохраняем предположения и обозначения пп. 2 и 5. Пусть ω — дифференциальная форма на кривой X, нормальной модели для X', и $Q \in S'$. Говорят, что ω *регулярна* в Q, если

$$\sum_{P \to Q} \operatorname{Res}_P(f\omega) = 0 \quad \text{для всех} \quad f \in \mathcal{O}'_Q. \tag{25}$$

Множество регулярных дифференциалов в точке Q будет обозначаться через $\underline{\Omega}'_Q$. Это $\mathscr{O}'_Q$-подмодуль векторного пространства $D_k(K)$ всех дифференциалов. Если положить

$$\underline{\Omega}_Q = \bigcap_{P \to Q} \underline{\Omega}_P, \tag{26}$$

то, очевидно, $\underline{\Omega}_Q \subset \underline{\Omega}'_Q$ и немедленно проверяется, что векторные пространства $\mathscr{O}_Q/\mathscr{O}'_Q$ и $\underline{\Omega}'_Q/\underline{\Omega}_Q$ сопряжены друг другу относительно билинейной формы $\sum \mathrm{Res}_P(f\omega)$, фигурирующей в (25).

Когда $X' = X'_{\mathfrak{m}}$, где $\mathfrak{m} = \sum n_P P$ — модуль на X, условие (25) эквивалентно следующим условиям:

$$\sum \mathrm{Res}_P(\omega) = 0 \quad \text{и} \quad v_P(\omega) \geqslant n_P \quad \textit{для всех} \quad P \in S. \tag{27}$$

Вернемся к общему случаю. Если $Q \notin S'$, то полагаем $\underline{\Omega}'_Q = \underline{\Omega}_Q$, что имеет смысл, поскольку Q можно отождествить с точкой X. Множества $\underline{\Omega}'_Q$ образуют подпучок $\underline{\Omega}'$ постоянного пучка $D_k(K)$. Этот пучок когерентен (так как $\underline{\Omega}_Q$ и $\underline{\Omega}'_Q/\underline{\Omega}_Q$ когерентны). Его сечения по определению есть дифференциальные формы, всюду регулярные на X'. Дадим их характеризацию.

Предложение 6. *Для того чтобы ω была всюду регулярной на X', необходимо и достаточно, чтобы $\mathrm{Tr}_g(\omega) = 0$ для всех рациональных функций g на X, не являющихся p-й степенью и входящих во все локальные кольца $\mathscr{O}'_Q$, $Q \in S'$.*

[Относительно определения следа $\mathrm{Tr}_g(\omega)$ см. гл. II, п. 12.]

Предположим, что ω всюду регулярна на X', и пусть $g\colon X \to \Lambda$ — рациональное отображение X в проективную прямую Λ. Если бы дифференциальная форма $\mathrm{Tr}_g(\omega)$ на Λ не была нулевой, то она обладала бы полюсом λ и существовала бы функция h, регулярная на Λ в окрестности точки λ и такая, что

$$\mathrm{Res}_\lambda(h\,\mathrm{Tr}_g(\omega)) \neq 0.$$

По формуле следа (гл. II, п. 12) имеем

$$\mathrm{Res}_\lambda (h \cdot \mathrm{Tr}_g(\omega)) = \sum_{g(P)=\lambda} \mathrm{Res}_P (h \circ g \cdot \omega). \tag{28}$$

В правой части члены, соответствующие точкам $P \notin S$, равны нулю, поскольку ω и $h \circ g$ регулярны в этих точках. Если g входит в пересечение $\mathcal{O}'_Q$, то равна нулю и сумма остальных членов согласно определению регулярного дифференциала. Левая же часть отлична от нуля. Это противоречие доказывает, что $\mathrm{Tr}_g(\omega) = 0$.

Обратно, предположим, что ω нерегулярна всюду на X'. Мы построим тогда такие функцию $g\colon X \to \Lambda$ и точку $\lambda \in \Lambda$, что $\mathrm{Res}_\lambda(\mathrm{Tr}_g(\omega)) \neq 0$. Обозначим через $\mathfrak{m}$ модуль с носителем S, больший чем кондуктор $\mathfrak{c}$. Если $g \equiv 0 \mod \mathfrak{m}$ во всех P, проектирующихся в $Q \in S'$, то $g \in \mathcal{O}'_Q$.

Предположим сначала, что ω имеет полюс порядка $n \geqslant 1$ в точке $P_0 \notin S$. Теорема о независимости нормирований показывает существование функции g, такой, что $v_{P_0}(g) = n-1$, $g \equiv \mu \mod \mathfrak{m}$ [где $\mu \neq \lambda = g(P_0)$] и $g(P) \neq \lambda$ во всех полюсах ω, отличных от P_0. Кроме того, можно предположить, что g имеет в данной точке простой нуль, откуда следует, что g не p-я степень. Тогда

$$\mathrm{Res}_\lambda(\mathrm{Tr}_g(\omega)) = \sum_{g(P)=\lambda} \mathrm{Res}_P (g\omega).$$

По построению все члены суммы справа равны нулю, исключая член $\mathrm{Res}_{P_0}(g\omega)$, заведомо отличный от нуля. Отсюда и следует наш результат для этого случая.

Предположим теперь, что ω нерегулярна в точке $Q \in S'$, т. е. что существует $f \in \mathcal{O}'_Q$ с $\sum\limits_{P \to Q} \mathrm{Res}_P(f\omega) \neq 0$. Положим $f(Q) = \lambda$. Для любой точки P, проектирующейся в Q, пусть n_P — целое число, по меньшей мере равное коэффициенту при P в модуле $\mathfrak{m}$, т. е. $-v_P(\omega)$. Выберем тогда функцию g, такую, что $v_P(f-g) \geqslant n_P$ при $P \to Q$, $g \equiv \mu \mod \mathfrak{m}$ при $P \not\to Q$ (где $\lambda \neq \mu$), и $g(P) \neq \lambda$ в любом полюсе P формы ω вне S. В силу выбора $\mathfrak{m}$ и n_P имеем включение $g \in \mathcal{O}'_R$ для всех $R \in S'$. Кроме того, так же как выше, получаем, что g

не является p-й степенью. Поэтому

$$\mathrm{Res}_\lambda(\mathrm{Tr}_g(\omega)) = \sum_{g(P)=\lambda} \mathrm{Res}_P(g\omega) = \sum_{P\to Q} \mathrm{Res}_P(g\omega) =$$
$$= \sum_{P\to Q} \mathrm{Res}_P(f\omega) \neq 0.$$

Предложение 6 доказано.

10. Теорема двойственности

Пусть D — дивизор, равный нулю на S. Сопоставим ему пучок $\underline{\Omega}'(D)$, положив

$$\underline{\Omega}'(D)_Q = \begin{cases} \underline{\Omega}'_Q & \text{при } Q \in S'; \\ \underline{\Omega}(D)_Q & \text{при } Q \notin S'. \end{cases}$$

Положим также $\Omega'(D) = H^0(X', \underline{\Omega}(D))$. Дифференциал ω входит в $\Omega'(D)$, если он регулярен во всех точках $Q \in S'$ и удовлетворяет условиям $v_P(\omega) \geqslant v_P(D)$ для всех $P \notin S$. Когда $D = 0$, мы получаем дифференциалы, *всюду регулярные* на X'.

Теорема 2. *Для всех дивизоров, равных нулю на S', векторное пространство $\Omega'(D)$ канонически изоморфно пространству, двойственному к $I'(D) = H^1(X', \mathscr{L}(D))$.*

Следствие 1. $i'(D) = \dim \Omega'(D)$.

Следствие 2. *Размерность векторного пространства дифференциальных форм, всюду регулярных на X', равна π.*

Для доказательства теоремы 2 нам понадобится интерпретация $\Omega'(D)$ и $I'(D)$ на языке *распределений*. Пусть R — алгебра распределений на X (см. гл. II, п. 5). Обозначим через R' подалгебру R, образованную распределениями $\{r_P\}$, такими, что $r_{P_1} = r_{P_2}$, если P_1 и P_2 имеют одинаковый образ в X'. Через $R'(D)$ обозначим подмножество R', образованное распределениями $\{r_P\}$, такими, что $v_P(r_P) \geqslant -v_P(D)$, если $P \notin S$, и $r_P \in \mathfrak{O}'_Q$, если P — точка S, имеющая в качестве образа в S' точку Q.

Известно, что пространство $D_k(K)$ всех дифференциалов отождествляется с топологически двойственным к пространству R/K, т. е. с множеством линейных форм ω на R, аннулирующихся на K и на подходящем подмножестве $R(\Delta)$ (обозначения см. в гл. II, п. 5). Говорят, что такая линейная форма ω входит в $\Omega'(D)$, если ω аннулируется на $R'(D)$. Таким образом, $\Omega'(D)$ — *топологически двойственное пространство* к векторному пространству $R/R'(D)+K$, снабженное топологией, определяемой образами $R(\Delta)$.

Перейдем теперь к рассмотрению $I'(D)$. На пространстве X' имеем точную последовательность пучков

$$0 \to \mathscr{L}'(D) \to K \to K/\mathscr{L}'(D) \to 0. \tag{29}$$

Поскольку K — постоянный пучок, а X' неприводимо, то $H^0(X', K) = K$ и $H^q(X', K) = 0$ для $q \geqslant 1$. Точная последовательность (29) дает тогда

$$K \to H^0(X', K/\mathscr{L}'(D)) \to H^1(X', \mathscr{L}'(D)) \to 0. \tag{30}$$

Рассуждения, проведенные в гл. II для пучка $K/\mathscr{L}(D)$, применимы также к пучку $A' = K/\mathscr{L}'(D)$. Они показывают, что $H^0(X', A')$ отождествляется с прямой суммой A'_Q для $Q \in X'$. Так как эта сумма очевидным образом изоморфна $R'/R'(D)$, то $I'(D) = H^1(X', \mathscr{L}'(D))$ *канонически отождествляется с фактором* $R'/(R'(D)+K)$.

Положим $V = R'/(R'/(D)+K)$ и $W = R/(R'(D)+K)$. Имеем $V \subset W$. Нам нужно доказать, что *пространство, двойственное* (алгебраически) пространству V, *можно отождествить с пространством, двойственным* (топологически) *пространству* W, другими словами, что любую линейную форму на V можно однозначно продолжить до линейной непрерывной формы на W. Это будет показано после проверки двух следующих свойств:

1) *V плотно в W;*

2) *V дискретно относительно топологии, индуцируемой W.*

Проверка свойства 1). Надо показать, что для всех дивизоров Δ

$$R' + R(\Delta) = R.$$

Пусть $r = \{r_P\}$ — произвольный элемент R. Существует элемент $f \in K$, такой, что $v_P(f - r_P) \geqslant v_P(\Delta)$ для всех $P \in S$. Пусть g — распределение $f - r$. Представим его в виде

$g = g' + g''$, где $g'_P = 0$ для $P \in S$ и $g''_P = 0$ для $P \notin S$.

Тогда $g'' \in R(\Delta)$, $g' \in R'$ и $f \in R'$. Это показывает, что $r = f - g' - g''$ входит в $R' + R(\Delta)$.

Проверка свойства 2). Надо доказать существование дивизора Δ, такого, что

$$R' \cap [K + R'(D) + R(\Delta)] = K + R(D). \tag{31}$$

Пусть n — такое целое число, что из соотношения $v_P(f) \geqslant n$ для $P \to Q$ следует $f \in \mathcal{O}'_Q$. Такое число существует согласно п. 2. Выбираем в качестве Δ дивизор $\Delta = D - \sum_{P \in S} nP$. Пусть $r = f + r' + s$ — элемент из левой части (31), где $r \in R'$, $f \in K$ и $s \in R(\Delta)$. В силу того, что $s = r - f - r'$, имеем $s \in R'$. Другими словами, s_P не зависит от образа Q точки P в X'. В силу выбора Δ элемент s_P входит в $\mathcal{O}'_Q$, а поскольку Δ совпадает с D вне S, то $s \in R'(D)$, что доказывает (31) и завершает доказательство теоремы 2.

Замечание. Можно дополнить теорему 2, показав, что $H^1(X', \underline{\Omega}')$ изоморфно k и что двойственность между $H^0(X', \underline{\Omega}(D))$ и $H^1(X', \mathcal{L}'(D))$ устанавливается, как в гл. II с помощью $\cup$-произведения.

11. Равенство $n_Q = 2\delta_Q$

Пусть $Q \in S'$ и $\mathfrak{c}_Q$ — проводник $\mathcal{O}_Q$ в $\mathcal{O}'_Q$. Поскольку $\mathfrak{c}_Q$ — идеал $\mathcal{O}'_Q$, существует дивизор $\sum_{P \to Q} n_P P$, такой, что $\mathfrak{c}_Q$ отождествляется с множеством функций $f \equiv 0 \bmod \sum n_P P$.

Идеал $\mathfrak{c}_Q$ всегда можно отождествлять с дивизором $\sum n_P P$.

С помощью дифференциалов можно дать простую интерпретацию $\mathfrak{c}_Q$. Действительно, как мы видели, $\underline{\Omega}'_Q/\underline{\Omega}_Q$ двойственно $\mathcal{O}_Q/\mathcal{O}'_Q$. Оба эти $\mathcal{O}'_Q$-модуля имеют один и тот же аннулятор $\mathfrak{c}_Q$. Таким образом, $f \in \mathfrak{c}_Q$ тогда и только тогда, когда $v_P(f\omega) \geqslant 0$ для всех $P \to Q$ и всех $\omega \in \underline{\Omega}'_Q$. Это позволяет сказать, что *n_P равно $\operatorname{Sup}(-v_P(\omega))$, где ω пробегает $\underline{\Omega}'_Q$.*

Обозначим теперь через $n_Q = \sum\limits_{P \to Q} n_P$ степень дивизора $\mathfrak{c}_Q$. Мы сравним *n_Q и δ_Q.*

Предложение 7. *$\delta_Q + 1 \leqslant n_Q \leqslant 2\delta_Q$ для всех $Q \in S'$. Равенство $n_Q = 2\delta_Q$ выполняется тогда и только тогда, когда $\underline{\Omega}'_Q$ является свободным $\mathcal{O}'_Q$-модулем ранга* 1.

Имеем $n_Q = \dim \mathcal{O}'_Q/\mathfrak{c}_Q$, и включение $k + \mathfrak{c}_Q \subset \mathcal{O}'_Q$ показывает, что $n_Q \geqslant \delta_Q + 1$.

С другой стороны, как мы только что видели, для всех $P \to Q$ существует дифференциал $\omega_P \in \underline{\Omega}'_Q$, такой, что $v_P(\omega_P) = -n_P$. Взяв линейную комбинацию ω_P и принимая во внимание тот факт, что поле k бесконечно, получаем дифференциал $\omega \in \mathcal{O}'_Q$, такой, что $v_P(\omega) = -n_P$ для всех $P \to Q$. Очевидно, что $f\omega \in \underline{\Omega}_Q \Longleftrightarrow f \in \mathfrak{c}_Q$. Это показывает, что отображение $f \to f\omega$ определяет инъекцию $\mathcal{O}'_Q/\mathfrak{c}_Q$ в $\underline{\Omega}'_Q/\underline{\Omega}_Q$, откуда вытекает неравенство $n_Q - \delta_Q \leqslant \delta_Q$. Если, кроме того, $\underline{\Omega}'_Q$ является $\mathcal{O}'_Q$-модулем ранга 1, то дифференциал ω обязательно образует базу и предыдущее отображение сюръективно. Это показывает, что $n_Q - \delta_Q = \delta_Q$. Обратно, если это равенство выполняется, то отображение сюръективно и любой дифференциал $\alpha \in \underline{\Omega}'_Q$ является суммой дифференциала $f\omega\,(f \in \mathcal{O}'_Q)$ и дифференциала $\beta \in \underline{\Omega}_Q$. Так как β может быть также записан в виде $g\omega$ где $g \in \mathfrak{c}_Q$, то ω образует базу $\underline{\Omega}'_Q$, что и завершает доказательство.

Если $n_Q = 2\delta_Q$ для всех $Q \in S'$, то пучок $\underline{\Omega}'$ *локально свободен* и соответствует, таким образом, классу дивизоров K' на X'. Из предыдущего следует, что $K \sim K' - \mathfrak{c}$, значит, в частности, $2g - 2 = \deg(K') - 2\delta$, т. е.

$$\deg\ (K') = 2\pi - 2. \tag{32}$$

Пучок $\underline{\Omega}'(D)$ изоморфен в этом случае пучку $\mathscr{L}'(K' - D)$, откуда получаем теорему Римана — Роха во *второй форме*

$$l'(D) - l'(K' - D) = \deg(D) + 1 - \pi. \tag{33}$$

12. Дополнения

Ввиду важности формул (32) и (33) было бы интересно дать условия, при которых $n_Q = 2\delta_Q$. Оказывается, так будет тогда, когда X' — *полное пересечение* в проективном пространстве (Розенлихт [1], § 5). Так будет также тогда, когда X' *погружено в неособую поверхность* V. Действительно, можно доказать, что для всех $Q \in X'$ $\mathscr{O}'_Q$-модуль $\underline{\Omega}'_Q$ образован вычетами на X' дифференциалов ω на V, таких, что $(\omega) \geqslant -X'$ в Q (см. Самюэль [1] и Горенштейн [1]), а в этом случае $\underline{\Omega}'_Q$ — свободный модуль ранга 1. Эта характеризация регулярных дифференциалов показывает, кроме того, что канонический дивизор K' кривой X' равен $X' \times \times_V (X' + K_V)$. Используя (32), мы возвращаемся к формуле (22), дающей арифметический род X'.

Эти результаты, прямое доказательство которых довольно утомительно, переоткрываются естественным образом в рамках теории Гротендика [2]. Последний доказал (не опубликовано), что если X' погружена в неособое многообразие Y произвольной размерности n, то имеет место канонический изоморфизм

$$\underline{\Omega}'_Q = \operatorname{Ext}^{n-1}_{\mathscr{O}_Q(Y)}(\mathscr{O}'_Q,\ \underline{\Omega}^n_Q(Y)), \tag{34}$$

где $\mathscr{O}_Q(Y)$ и $\underline{\Omega}^n_Q(Y)$ обозначают соответственно локальное кольцо многообразия Y в точке Q и модуль дифференциальных форм степени n на Y, регулярных в Q. В случае когда X' — *пол-*

ное пересечение в Q, можно явно записать свободную резольвенту $\mathcal{O}_Q(Y)$-модуля $\mathcal{O}'_Q$ и усмотреть, что $\underline{\Omega}'_Q$ — свободный модуль ранга 1 над $\mathcal{O}'_Q$. При доказательстве используется тот факт, что если $f_1, \ldots, f_{n-1}$ — образующие идеала X' в $\mathcal{O}_Q(Y)$ и $x_1, \ldots, x_n$ образуют регулярную систему параметров $\mathcal{O}_Q(Y)$, то модуль $\underline{\Omega}'_Q$ допускает в качестве базиса дифференциал ω, получаемый при „делении“ $dx_1 \wedge \ldots \wedge dx_n$ на $df_1 \wedge \ldots \wedge df_{n-1}$. Для $n=2$ имеется единственное уравнение $f(x, y)=0$ и ω записывается в классическом виде $\omega = dx/f'_y = -dy/f'_x$.

Библиографические замечания

В изучении особых кривых главной проблемой долгое время была проблема разрешения особенностей. Эта проблема была решена при помощи „квадратичных“ преобразований; читатель найдет ее изложение у Севери [1] или Норткотта [1—3]. Метод нормализации, введенный Зарисским, быстрее ведет к цели, но дает менее полный результат; например, если применить, следуя Юнгу, квадратичные преобразования к кривой разветвления проекции поверхности V на плоскость, то легко получить разрешение особенностей V (в случае характеристики 0).

Построение особой кривой по плоской кривой и полулокальному кольцу ее поля функций было осуществлено Розенлихтом [1], который рассмотрел также случай приводимой кривой над произвольным полем. Результаты Розенлихта содержат как теорему Римана — Роха, так и теорию регулярных дифференциалов. Эти результаты были известны для случая, когда кривая имеет лишь „обыкновенные“ особенности (см. Севери [3], гл. I).

Отметим недавнюю работу Хиронаки [1], в которой доказывается, что целое число $\pi = g + \delta$ совпадает с арифметическим родом кривой. Этот факт в случае обыкновенных особенностей был известен также итальянским геометрам.

Равенство $n_Q = 2\delta_Q$ для кривых, лежащих на поверхности, доказано Горенштейном [1] и Самюэлем [1]; аналогичное изложение в аналитической геометрии имеется у Колаиры [1], [2]. Точку зрения, приведенную в конце п. 12, мне устно сообщил Гротендик; я надеюсь, что он в скором времени опубликует детальное изложение [1]).

---

[1]) Как сообщается в письме автора от 16 июля 1967 г., он уже утратил эту надежду. — *Прим. ред.*

ГЛАВА

V

ОБОБЩЕННЫЕ ЯКОБИЕВЫ МНОГООБРАЗИЯ

Эта глава посвящена построению и элементарному изучению обобщенного якобиевого многообразия алгебраической кривой. При изложении мы придерживаемся мемуара Розенлихта [2], в свою очередь находящегося под влиянием „Абелевых многообразий“ Вейля [5], в которых рассматривается случай обыкновенного якобиевого многообразия. Как и названные авторы, мы используем метод „общих точек“; это заставляет нас отказаться от точки зрения предыдущих глав (где все точки имели координаты в фиксированном основном поле) и принять точку зрения „Оснований“ [3]. Конечно, можно заменить общие точки дивизорами на произведениях многообразий, если сначала детально изложить свойства этих дивизоров (т. е. по существу ввести в рассмотрение когомологии алгебраических когерентных пучков на произведении многообразий). Однако это завело бы нас слишком далеко.

§ 1. Построение обобщенных якобиевых многообразий

1. Рациональные дивизоры

Во всей главе X обозначает проективную неприводимую и неособую алгебраическую кривую над полем k. В § 1—3 поле k будет предполагаться *алгебраически замкнутым*. В соответствии с „Основаниями“ (Вейль А. [3]) выбираем *универсальную область* Ω. Напомним, что Ω — алгебраически замкнутое расширение поля k бесконечной степени трансцендентности. Все рассматриваемые поля (исключая поля функций) будут подполями поля Ω конечного типа над k. *Точкой* кривой X называется точка P, все координаты которой принадлежат Ω. Поле $k(P)$, порожденное над k этими координатами, будет расширением конечного типа поля k. Говорят, что P *рациональна* над полем K, если $k(P)\subset K$. Из предположения, что k алгебраически замкнуто, следует, что X содержит *бесконечное число рациональных точек над* k.

Напомним теперь определение и основные свойства рациональных дивизоров; доказательства можно найти в „Основаниях" (Вейль А. [3]) или в работе Самюэля [3].

Пусть $D=\sum n_i P_i$ — дивизор на X. Выберем аффинную модель U многообразия X, содержащую все P_i и определенную над полем k. С аффинной кривой U связано кольцо координат $A=k[U]$. Оно является дедекиндовым кольцом (нормальным и размерности 1). Если рассматривать U как кривую над Ω, то ее кольцом координат будет $A_\Omega = A \otimes_k \Omega$. Дивизор D определяется идеалом (в общем случае дробным) $\mathfrak{d}$ кольца A_Ω. Рассуждения из элементарной линейной алгебры показывают тогда, что существует наименьшее поле K, такое, что $\mathfrak{d}$ имеет вид $\mathfrak{d}=\mathfrak{v}\otimes_k \Omega$, где $\mathfrak{v}$ — векторное подпространство над полем K пространства $A_K = A\otimes_k K$. Другими словами, K — наименьшее поле (содержащее k), такое, что $\mathfrak{d}$ порождается многочленами с коэффициентами в K. Поле K называется *полем рациональности для* D [обозначение $K=k(D)$]. Если L — произвольное поле, то через $L(D)$ обозначается композит $L(k(D))$. Говорят, что дивизор D *рационален над* L, если $L(D)=L$, т. е. если $\mathfrak{d}$ может быть порожден уравнениями с коэффициентами в L. Это определение показывает, что если D_1 и D_2 рациональны над L, то рациональны также дивизоры D_1-D_2 и $\sup(D_1, D_2)$. Если φ — рациональная функция на L [т. е. принадлежит полю частных $L(X)$ алгебры A_L], то ее дивизор (φ) рационален над L В случае когда дивизор D сводится к одной точке P, определение $L(D)$ совпадает с определением $k(P)$, данным выше.

Вообще, для того чтобы дивизор $D=\sum n_\alpha P_\alpha$ ($n_\alpha \neq 0$) был рационален над полем L, необходимо и достаточно, чтобы выполнялись следующие три условия (см. Вейль А. [3] и Самюэль [3]).

1) $k(P_\alpha)\subset \bar{L}$, где $\bar{L}$ — алгебраическое замыкание L [другими словами, дивизор D должен быть алгебраичен над L];

2) $D^\sigma = D$ для всех L-автоморфизмов σ поля $\bar{L}$ [или поля Ω, что сводится к тому же согласно 1)];

3) целые числа n_α делятся на $[L(P_\alpha):L]_i$, степень несепарабельности расширения $L(P_\alpha)/L$.

Пусть D — положительный дивизор степени n; его можно отождествить (см. гл. III, п. 14) с точкой $\bar{D}$ симметрического произведения $X^{(n)}$. Последнее, очевидно определено над k и поэтому можно говорить о поле $k(\bar{D})$. Это поле совпадает с $k(D)$, согласно результатам Чжоу (см. Самюэль [3], стр. 104; доказательства Чжоу и Самюэля используют свойства „координат Чжоу", но нетрудно дать и прямое доказательство). Фактически мы используем этот результат только в следующем частном случае, который имеется у Вейля [5] (стр. 10) и у Ленга [5] (стр.30).

Лемма 1. *Пусть K — поле и $M_1, \ldots, M_n$ — n независимых общих точек X над K. Если M обозначает дивизор $M_1 + \ldots + M_n$, то $K(M) = K(M_1, \ldots, M_n)_s$, где $K(M_1, \ldots, M_n)_s$ — множество элементов $K(M_1, \ldots, M_n)$, инвариантных относительно всех перестановок* $[1, n]$.

[Заметим, что выражение „$M_1, \ldots, M_n$ — независимые общие точки над K" означает, что расширение $K(M_1, \ldots, M_n)/K$ имеет степень трансцендентности n.]

2. Отношение эквивалентности, определяемое модулем

Начиная с этого момента, фиксируем *модуль* $\mathfrak{m}$ с носителем S. Предположим, что точки S рациональны над k (если k не алгебраически замкнуто, то необходимо предположить, что модуль $\mathfrak{m}$ рационален над k как дивизор; в этом случае результаты двух первых параграфов останутся без изменений, а результаты § 3 должны быть слегка изменены; мы возвратимся к этому в § 4).

Пусть D и D' — два дивизора, равных нулю на S. Мы говорим, что D и D' *$\mathfrak{m}$-эквивалентны*, и записываем это в виде $D \underset{\mathfrak{m}}{\sim} D'$, если существует отличная от нуля рациональная функция g, удовлетворяющая двум условиям:

а) $g \equiv 1 \pmod{\mathfrak{m}}$, см. гл. III, п. 1,

б) $(g) = D' - D$.

Условие а) должно быть опущено, если $\mathfrak{m} = 0$. В общем случае можно заменить условие а) условием сравнимости g по $\operatorname{mod} \mathfrak{m}$ с постоянной, отличной от нуля.

Придерживаясь обозначений гл. I, мы обозначим через $C_{\mathfrak{m}}$ группу классов дивизоров, равных нулю на S по модулю $\mathfrak{m}$-эквивалентности, и через $C_{\mathfrak{m}}^0$ подгруппу $C_{\mathfrak{m}}$, образованную классами степени 0. Можно также интерпретировать $C_{\mathfrak{m}}$ как группу *классов расслоенных пространств со слоями из векторных пространств размерности* 1, *имеющих в качестве базы особую кривую* $X_{\mathfrak{m}}$, ассоциированную с модулем $\mathfrak{m}$ (гл. IV, п. 4). Соответствие между расслоенными пространствами и дивизорами устанавливается следующим образом; пусть Q — единственная особая точка кривой $X_{\mathfrak{m}}$ и E — расслоенное пространство; можно найти рациональное сечение S пространства E, регулярное и не обращающееся в нуль в точке Q; так как $X_{\mathfrak{m}} - Q = X - Q$, можно говорить о дивизоре (s) сечения S, который равен нулю на S и определен с точностью до $\mathfrak{m}$-эквивалентности; легко проверяется тогда, что $E \to (s)$ определяет изоморфизм группы классов расслоенных пространств на группу $C_{\mathfrak{m}}$.

Пусть D — дивизор. Найдем *положительный* дивизор D', такой, что $D \underset{\mathfrak{m}}{\sim} D'$. Как и в гл. II в случае $\mathfrak{m}=0$, это сводится к отысканию функций g, удовлетворяющих условию $(g) \geqslant -D$ вне S и удовлетворяющих а). Такая функция g входит в локальное кольцо $\mathfrak{O}_Q$ особой точки Q особой кривой $X_{\mathfrak{m}}$. Таким образом, $g \in L_{\mathfrak{m}}(D)$ в обозначениях гл. IV, п. 5. Наоборот, *если* $g \in L_{\mathfrak{m}}(D)$ *и не обращается в нуль на* S, дивизор $D' = (g) + D$ $\mathfrak{m}$-эквивалентен D. Так как функции $g \in L_{\mathfrak{m}}(D)$, аннулирующиеся на S, суть функции $g \in L(D-\mathfrak{m})$, мы видим в результате, что *множество положительных дивизоров* D', *таких, что* $D' \underset{\mathfrak{m}}{\sim} D$, *находится в биективном соответствии с проективным пространством, ассоциированным с векторным пространством* $L_{\mathfrak{m}}(D)$, *исключая проективное подпространство, ассоциированное с* $L(D-\mathfrak{m})$.

Лемма 2. *Пусть D — дивизор, равный нулю на S и рациональный над полем K. Существует базис $L_{\mathfrak{m}}(D)$ [соответственно $I_{\mathfrak{m}}^*(D)$], образованный функциями (соот-*

ветственно дифференциальными формами), рациональными над K.

[Для того чтобы избежать смешения с универсальной областью, через $I^*_{\mathfrak{m}}(D)$ обозначается пространство сечений пучка $\Omega_{\mathfrak{m}}(D)$; см. гл. IV, § 3.]

Нам предстоит доказать, что принадлежность к $L_{\mathfrak{m}}(D)$ налагает на функцию $f \in \Omega(X)$ K-линейные условия. Эти условия двух видов: во-первых, что f сравнима по $\operatorname{mod} \mathfrak{m}$ с константой; во-вторых, что $(f) \geqslant -D$. Первое условие, очевидно, K-линейно (оно даже k-линейно); второе условие также K-линейно в соответствии с определением поля рациональности дивизора. Отсюда следует искомый результат для $L_{\mathfrak{m}}(D)$. Для $I^*_{\mathfrak{m}}(D)$ сначала сводим все к частному случаю $\mathfrak{m} = 0$, а затем замечаем, что $I(D)$ изоморфно $L(\Delta - D)$, где Δ — канонический дивизор. Так как Δ всегда можно выбрать рациональным над k, мы получаем сведение к случаю, рассмотренному вначале.

Следствие. *Если существует только один положительный дивизор D', такой, что $D' \underset{\mathfrak{m}}{\sim} D$, то этот дивизор рационален над K.*

Единственность D' означает, что $\dim L_{\mathfrak{m}}(D) = 1$ и $L(D - \mathfrak{m}) = 0$. По предыдущей лемме существует функция $g \in L_{\mathfrak{m}}(D)$, не сводящаяся к 0 и рациональная над K. Так как $D' = (g) + D$, отсюда следует, что D рационален над K.

3. Предварительные леммы

Пусть D — дивизор, равный нулю на S. Положим (см. гл. IV, п. 5)

$$l_{\mathfrak{m}}(D) = \dim L_{\mathfrak{m}}(D) \text{ и } i_{\mathfrak{m}}(D) = \dim I_{\mathfrak{m}}(D).$$

По теореме Римана — Роха имеем

$$l_{\mathfrak{m}}(D) - i_{\mathfrak{m}}(D) = \deg(D) + 1 - \pi,$$

где π обозначает арифметический род кривой с особенностями $X_{\mathfrak{m}}$, т. е.

$$\pi = g \qquad \text{при} \quad \mathfrak{m} = 0;$$

$$\pi = g + \deg(\mathfrak{m}) - 1 \quad \text{при} \quad \mathfrak{m} \neq 0.$$

Лемма 3. *Пусть K — поле, D — рациональный дивизор над K и P — общая точка X над K. Если $i_{\mathfrak{m}}(D) > 0$, то*

$$i_{\mathfrak{m}}(D + P) = i_{\mathfrak{m}}(D) - 1.$$

Векторное пространство $I_{\mathfrak{m}}(D+P)^*$ отождествляется с подпространством $I_{\mathfrak{m}}(D)^*$, образованным дифференциалами ω этого пространства, которые обращаются в нуль в точке P. Следовательно, всегда $i_{\mathfrak{m}}(D+P) \geqslant i_{\mathfrak{m}}(D) - 1$, и остается доказать, что существует по крайней мере один дифференциал $\omega \in I_{\mathfrak{m}}^*(D)$, не обращающийся в нуль в P. Однако, поскольку $i_{\mathfrak{m}}(D) > 0$, из леммы 2 вытекает, что существует ненулевая дифференциальная форма $\omega \in I_{\mathfrak{m}}(D)$, рациональная над K. Множество точек, где ω обращается в нуль, необходимо алгебраично над K, а следовательно, не содержит точки P.

Следующий результат является фундаментальным для дальнейшего.

Лемма 4. *Пусть D — дивизор степени 0, рациональный над полем K, и $M_1, \ldots, M_\pi$ — π общих точек, независимых над K. Тогда*

а) $l_{\mathfrak{m}}\left(D + \sum_{i=1}^{\pi} M_i\right) = 1$;

б) *существует положительный дивизор Δ (и притом единственный), такой, что $\Delta \sim D + \sum_{i=1}^{\pi} M_i$;*

в) $K(\Delta) = K(M_1, \ldots, M_\pi)_s$.

Поскольку $\deg(D) = 0$, то $l_{\mathfrak{m}}(D) \leqslant 1$ и теорема Римана — Роха показывает, что $i_{\mathfrak{m}}(D) \leqslant \pi$. Применяя несколько раз лемму 3, видим, что $i_{\mathfrak{m}}\left(D + \sum_{i=1}^{\pi} M_i\right) = 0$. Применяя снова теорему Римана — Роха, получаем а).

Таким образом, существует функция g (единственная с точностью до умножения на константу), принадлежащая

$L_{\mathfrak{m}}\left(D+\sum_{1}^{\pi} M_i\right)$. Если $\mathfrak{m}=0$, это доказывает б). Если $\mathfrak{m}\neq 0$, необходимо, кроме того, убедиться в том, что $L\left(D+\sum_{1}^{\pi} M_i-\mathfrak{m}\right)=0$ (см. п. 2). Положим в этом случае $A=D+\sum_{1}^{\pi} M_i-\mathfrak{m}$ и предположим, что $l(A)\geqslant 1$. Степень дивизора A равна $g-1$, и обычная формула Римана — Роха показывает, что $i(A)=l(A)\geqslant 1$. С другой стороны, применяя несколько раз лемму 3 (где на этот раз $\mathfrak{m}=0$), получаем, что $l(A)=i(D-\mathfrak{m})-\pi$, откуда $i(D-\mathfrak{m})>\pi$. Но дивизор $D-\mathfrak{m}$ имеет степень <0, откуда $l(D-\mathfrak{m})=0$. Применяя теорему Римана — Роха, получаем $i(D-\mathfrak{m})=\pi$, что приводит к противоречию.

Остается доказать в). По лемме 2) можно выбрать рациональную функцию g над полем $K\left(D+\sum_{1}^{\pi} M_i\right)$, которое совпадает с $K(M_1, \ldots, M_n)_s$ по лемме 1. Так как Δ равно $(g)+D+\sum_{1}^{\pi} M_i$, то оно рационально над $K(M_1, \ldots, M_n)_s$. С другой стороны, если применить а) к $D=0$, получим $l_{\mathfrak{m}}\left(\sum_{1}^{\pi} M_i\right)=1$. Это доказывает, что $\sum_{1}^{\pi} M_i$ — единственный дивизор, $\mathfrak{m}$-эквивалентный $\Delta-D$. Рассуждения, проделанные выше[1]), показывают тогда, что $K\left(\sum_{1}^{\pi} M_i\right)$ содержится в поле $K(\Delta-D)=K(\Delta)$. Отсюда, наконец, следует равенство в).

4. Закон композиции на симметрическом произведении $X^{(\pi)}$

Пусть $Y=X^{(\pi)}$ — симметрическое произведение π экземпляров X. Мы снабдим сейчас Y рациональным законом композиции, который превратит Y в „бирациональную группу".

[1]) Следствие к лемме 2. — *Прим. перев.*

Как мы уже указывали, всякий положительной дивизор степени π: $M = M_1 + \ldots + M_\pi$ можно отождествить с точкой Y. В случае когда M_i — независимые общие точки над полем K, мы получаем точку $M \in Y$, являющуюся общей точкой Y над K, а мы видели, что поле $K(M)$ совпадает с полем *точки* M на Y.

Выберем теперь точку $P_0 \in X$, рациональную над k и вне S. Эта точка будет единицей для закона группы, который мы строим.

Лемма 5. *Пусть M и N — две независимые общие точки Y над полем K. Существует дивизор R (и притом единственный), такой, что $R \underset{\mathfrak{m}}{\sim} M + N - \pi P_0$ и*

$$K(M, N) = K(R, M) = K(R, N).$$

Положим $M = \sum_{i=1}^{\pi} M_i$. Точки M_i — независимые общие точки над полем $K(N)$, а также над $K(N - \pi P_0)$, поскольку P_0 рациональна над k. Лемма 4 доказывает тогда существование и единственность дивизора R, такого, что

$$R \underset{\mathfrak{m}}{\sim} M + N - \pi P_0.$$

Видно также, что $K(R, N) = K(M, N)$, откуда, меняя ролями M и N, получаем $K(R, M) = K(M, N)$.

Предложение 1. *На многообразии $Y = X^{(\pi)}$ существует рациональный закон композиции (и притом единственный) F: $Y \times Y \to Y$, определенный над полем k и такой, что если M и N — две независимые общие точки Y над полем k, то $F(M, N)$—точка R, определенная в лемме 5. Кроме того, этот закон композиции превращает Y в „бирациональную группу“ (другими словами, этот закон композиции нормален в смысле Вейля* [5], § V).

Пусть M и N — две общие независимые точки многообразия Y над полем k и R — точка Y, определенная в лемме 5. В силу того, что $k(R) \subset k(M, N)$, существует рациональное отображение F: $Y \times Y \to Y$ (и притом единственное), которое определено над k и отображает (M, N) в R. Пусть теперь M' и N' — две независимые общие точки Y над полем K; тем более M' и N' независимы над k. Следовательно, существует k-автоморфизм σ универсальной области Ω, такой, что $M' = M^\sigma$ и $N' = N^\sigma$. Поскольку F определено над k, имеем

$$F(M^\sigma, N^\sigma) = F(M, N)^\sigma, \quad \text{откуда} \quad F(M', N') = R^\sigma.$$

Но по предположению существует функция g, такая, что $g \equiv 1 \bmod \mathfrak{m}$ и

$$(g) = M + N - \pi P_0 - R.$$

Применяя σ, находим

$$(g^\sigma) = M' + N' - \pi P_0 - R^\sigma,$$

где $g^\sigma \equiv 1 \bmod \mathfrak{m}$ (поскольку $\mathfrak{m}$ рационально над k). Это показывает, что $F(M', N') = R^\sigma$ есть дивизор, соответствующий (M', N') по лемме 5. Первая часть предложения доказана.

Остается показать, что F — нормальный закон композиции. Сначала надо проверить, что F *ассоциативен относительно общих точек*, другими словами, что

$$F(M, F(M', M'')) = F(F(M, M'), M''),$$

когда M, M', M'' — три независимые общие точки. Так как левая и правая части — однозначные положительные дивизоры, $\mathfrak{m}$-эквивалентные $M + M' + M'' - 2\pi P_0$, это очевидно. Необходимо еще проверить, что если положить $R = F(M, N)$, то

$$k(M, N) = k(R, M) = k(R, N).$$

Это есть второе утверждение леммы 5. Предложение доказано.

Заметим, что закон композиции F *коммутативен.*

5. Переход от бирациональной группы к алгебраической

Мы только что построили „бирациональную группу", закон композиции которой определен над k. Согласно результатам Вейля ([5], § V, расширено и дополнено в [9]), такая группа бирационально изоморфна настоящей алгебраической группе (где закон композиции и взятие обратного элемента – регулярные отображения, а не только рациональные). Кроме того, эта группа, как и изоморфизм, может быть определена над k. Мы ограничимся кратким указанием этапов доказательства, вновь отсылая за деталями к Вейлю [5], [9].

Заметим, что искомая алгебраическая группа, если она существует, определяется *однозначно*. Это равносильно тому, что всякий бирациональный изоморфизм между двумя алгебраическими группами G_1 и G_2 необходимо бирегулярен, что является частным случаем следующего результата.

Лемма 6. *Любое рациональное отображение $f\colon G_1 \to G_2$, являющееся гомоморфизмом относительно общих точек, всюду регулярно.*

Условие леммы означает, что существует открытое непустое подмножество U группы G_1, такое, что f регулярно на U и $f(xy) = f(x)f(y)$ для x, y, $xy \in U$. Оставляя фиксированным x и меняя y, получаем, что f регулярно на открытом множестве xU. Так как множества xU покрывают G_1, отображение f всюду регулярно.

Существование искомой алгебраической группы установить труднее. Сначала доказывается

Лемма 7. *Для любой бирациональной группы Y, определенной над полем k, существует алгебраическая группа G, определенная над расширением K/k и бирационально изоморфная Y над K* (см. Вейль [5], § 5, теорема 15, а также [9], п. 6).

Затем строится открытое множество Y' многообразия Y, на котором закон композиции имеет достаточно регулярные свойства. Группа G определяется склеиванием нескольких экземпляров Y' с помощью общих трансляций. Это те трансляции, которые приводят к необходимости расширить основное поле.

Как только G построена над расширением K/k, можно „спустить“ ее основное поле до поля k.

Лемма 8. *Для любой бирациональной группы Y, определенной над K, существует алгебраическая группа G_0, определенная над k и бирационально изоморфная над K группе Y.*

Используя теоремы „спуска основного поля“, получаем, что расширение K/k можно выбрать сепарабельным (а также регулярным); относительно теорем спуска см. Вейль [11].

В частном случае, когда k алгебраически замкнуто, можно дать непосредственную конструкцию G_0 (см. Розенлихт [2], теорема 4). Этот случай будет, впрочем, единственным, который нам понадобится.

6. Построение якобиева многообразия $J_{\mathfrak{m}}$

Объединяя предложение 1 и лемму 8, получаем

Предложение 2. *Существует алгебраическая группа $J_{\mathfrak{m}}$ и бирациональное отображение φ: $X^{(\pi)} \to J_{\mathfrak{m}}$, определенное над k и такое, что если M и N — две независимые общие точки $X^{(\pi)}$, то*

$$\varphi(M) + \varphi(N) = \varphi(M * N),$$

где $M * N$ обозначает дивизор R из леммы 5. *Кроме того, предыдущие свойства определяют $J_{\mathfrak{m}}$ и φ однозначно с точностью до изоморфизма.*

Группа $J_{\mathfrak{m}}$ называется *обобщенным якобиевым многообразием* кривой X (относительно модуля $\mathfrak{m}$).

Более подробно отображение φ изучается в § 2. Отметим пока, что, поскольку φ определено над k, $\varphi(M)$ определено для любой общей точки $X^{(\pi)}$. С другой стороны, композиция $M * N$ определена, если M и N — *независимые общие точки* на $X^{(\pi)}$. В общем случае пусть $M_1, \ldots, M_r$ — r независимых общих точек $X^{(\pi)}$. Лемма 5 показывает, что можно определить рекуррентно композицию $M_1 * M_2 * \ldots * M_r$, которая будет общей точкой $X^{(\pi)}$. Эту ситуацию описывает

Лемма 9. *Пусть $M_1, \ldots, M_r$ [соответственно $(N_1, \ldots, N_r)$] суть r независимых общих точек $X^{(\pi)}$. Следующие три условия эквивалентны:*

а) $M_1 * \ldots * M_r = N_1 * \ldots * N_r$;

б) $M_1 + \ldots + M_r \underset{\mathfrak{m}}{\sim} N_1 + \ldots + N_r$;

в) $\varphi(M_1) + \ldots + \varphi(M_r) = \varphi(N_1) + \ldots + \varphi(N_r)$.

В силу леммы 5 композиция $M_1 * \ldots * M_r$ есть однозначно определенный положительный дивизор, $\mathfrak{m}$-эквивалентный

$M_1 + \ldots + M_r - (r-1)\pi P_0$, откуда а)$\Leftrightarrow$б). Эквивалентность же а)$\Leftrightarrow$в) следует из того, что φ — биективный гомоморфизм на общих точках.

§ 2. *Универсальный характер обобщенных якобиевых многообразий*

В этом параграфе мы покажем, что якобиево многообразие $J_{\mathfrak{m}}$, определенное в § 1, удовлетворяет свойству универсальности, которое было сформулировано в теореме 2 гл. I.

7. Гомоморфизм группы дивизоров X в $J_{\mathfrak{m}}$

Пусть D — дивизор на X, равный нулю на S. Поставим ему в соответствие элемент $\theta(D)$ многообразия $J_{\mathfrak{m}}$.

Пусть K - поле, содержащее $k(D)$, и $M = \sum_{i=1}^{\pi} M_i$ — общая точка $X^{(\pi)}$ в K. По лемме 4 существует единственный дивизор $N \in X^{(\pi)}$, такой, что

$$N \underset{\mathfrak{m}}{\sim} D - (\deg D) P_0 + M$$

и $K(N) = K(M)$. Это показывает, что N — общая точка в K. Образы $\varphi(M)$ и $\varphi(N)$ точек M и N при отображении φ: $X^{(\pi)} \to J_{\mathfrak{m}}$ являются вполне определенными элементами $J_{\mathfrak{m}}$. Положим

$$\theta_M(D) = \varphi(N) - \varphi(M).$$

Это определение имеет смысл, так как очевидно, что N не изменится, если сузить поле K, и разность $\varphi(N) - \varphi(M)$ не зависит от K.

Лемма 10. *Пусть K — поле, и D, D' — два рациональных дивизора над K. Положим $D'' = D + D'$. Если M, M', M'' — три независимые общие точки над K, то*

$$\theta_{M''}(D'') = \theta_M(D) + \theta_{M'}(D').$$

Обозначим через N, N', N'' точки, определяемые D, D', D'' соответственно при построенном выше соответствии между дивизорами и точками. Надо доказать соотношение

$$\varphi(N'') - \varphi(M'') = \varphi(N) - \varphi(M) + \varphi(N') - \varphi(M'),$$

которое записывается также в виде

$$\varphi(N) + \varphi(N') + \varphi(M'') = \varphi(N'') + \varphi(M) + \varphi(M').$$

Так как $K(N) = K(M)$ и $K(N') = K(M')$, то N, N', M'' — независимые общие точки. То же самое относится и к трем другим точкам N'', M и M'. По лемме 9 доказываемая формула эквивалентна следующей, которая очевидна:

$$N + N' + M'' \underset{\mathfrak{m}}{\sim} N'' + M + M'.$$

Лемма 11. $\theta_M(D)$ *не зависит от* M.

Заметим сначала, что $\theta_M(0) = 0$, так как в этом случае $N = M$. Применяя лемму 10 с $D' = 0$, получаем

$$\theta_M(D) = \theta_{M''}(D)$$

в случае, когда M и M'' — независимые общие точки.

Если теперь M' — другая общая точка для K, то всегда можно найти третью общую точку M'', которая будет независима как от M, так и от M'. В силу предыдущего

$$\theta_M(D) = \theta_{M''}(D) = \theta_{M'}(D).$$

Лемма доказана.

Далее будем писать $\theta(D)$ вместо $\theta_M(D)$.

Лемма 12. $\theta(P) = \varphi(P)$, *если* $P = \sum_{i=1}^{\pi} P_i$ — *общая точка* $X^{(\pi)}$.

Пусть M — общая точка $X^{(\pi)}$, независимая от P. Если взять дивизор $N \in X^{(\pi)}$, такой, что

$$N \sim P + M - \pi P_0,$$

то это будет дивизор, обозначенный через $P*M$ в предложении 2. По определению, а также в силу предложения 2 имеем

$$\theta(P) = \theta_M(P) = \varphi(N) - \varphi(M) = \varphi(P*M) - \varphi(M) = \varphi(P).$$

Лемма 13. *Если дивизор D рационален над полем K, то точка $\theta(D) \in J_{\mathfrak{m}}$ рациональна над K.*

Построение $\theta(D)$ в виде $\varphi(N) - \varphi(M)$ показывает, что $\theta(D)$ рациональна над полем $K(N) = K(M)$. Так как это верно для любой общей точки M поля K, отсюда следует, что $k(\theta(D))$ содержится в пересечении полей $K(M)$, которое совпадает с K.

Предложение 3. *Отображение θ есть гомоморфизм группы дивизоров, равных нулю на S, на группу $J_{\mathfrak{m}}$. Ядро этого отображения образовано дивизорами, $\mathfrak{m}$-эквивалентными nP_0, где n - целое число.*

Лемма 10 показывает, что θ — гомоморфизм. Образ этого гомоморфизма есть подгруппа в $J_{\mathfrak{m}}$, которая, согласно лемме 12, содержит все общие точки $J_{\mathfrak{m}}$. Таким образом, эта подгруппа совпадает с $J_{\mathfrak{m}}$ (действительно, любая точка алгебраической группы является произведением двух общих точек). Поэтому отображение θ сюръективно.

Для того чтобы $\theta(D) = 0$, необходимо и достаточно, чтобы

$$\varphi(M) = \varphi(N)$$

(обозначения M и N те же, что и в начале этого пункта). В силу леммы 9 (или определения φ) это означает, что $M \underset{\mathfrak{m}}{\sim} N$, т. е. что $D \sim (\deg D) P_0$.

8. Каноническое отображение X в $J_{\mathfrak{m}}$

Докажем сначала один вспомогательный результат о накрытиях.

Лемма 14. *Пусть X и X' — две кривые (как всегда полные и неособые) и $g: X \to X'$ - сепарабельное накрытие степени $n+1$. Для всех $P \in X$ дивизор*

$$g^{-1}(g(P))$$

имеет вид $P + H_P$, где H_P - положительный дивизор степени n. Если отождествить H_P с точкой симметрического произведения $X^{(n)}$, то $P \to X_P$ — регулярное отображение X в $X^{(n)}$.

Воспользуемся тем же методом, что и в п. 13 гл. III. Пусть Y — накрытие Галуа X', содержащее X; $\mathfrak{g}$ — группа Галуа накрытия $Y \to X'$ и $\mathfrak{h} \subset \mathfrak{g}$ — группа Галуа накрытия $Y \to X$. Выберем представителей σ_i $(i = 1, \ldots, n+1)$ классов $\mathfrak{g}$ по модулю $\mathfrak{h}$, и пусть σ_{n+1} — представитель класса $\mathfrak{h}$. Если обозначить через π проекцию $Y \to X$, то, как известно (см. гл. III, п. 13), $g^{-1}(g(P)) = \sum \pi \circ \sigma_i(Q)$, где Q обозначает точку Y, которая проектируется в P. Отсюда

$$H_P = \sum_{i=1}^{n} \pi \circ \sigma_i(Q).$$

Определим теперь регулярное отображение h: $Y \to X^n$

$$h(Q) = (\pi \circ \sigma_1(Q), \ \ldots, \ \pi \circ \sigma_n(Q)).$$

Умножая h на каноническое отображение $X^n \to X^{(n)}$, получаем регулярное отображение

$$h'\colon \ Y \to X^{(n)}.$$

Предыдущая формула показывает, что h' при переходе к фактору определяет отображение h'': $X \to X^{(n)}$, которое, очевидно, регулярно и совпадает с отображением $P \to H_P$. Лемма доказана.

Замечание. Лемму 14 можно рассматривать как частный случай теоремы о „вычитании“, которая формулируется следующим образом.

Пусть T и X — два алгебраических многообразия. Предположим, что каждому $t \in T$ поставлены в соответствие три положительных цикла размерности нуль многообразия X, а именно H_t, H'_t H''_t, со свойством

$$H_t = H'_t + H''_t.$$

Пусть n, n', n'' — степени этих циклов, которые по предположению не зависят от t. Говорят, что семейство H_t *регулярно*, если соответствующее ему отображение H: $T \to X^{(n)}$ регулярно. Тогда *если два из трех семейств H_t, H'_t и H''_t регулярны, то третье также будет регулярным*. Доказательство является упражнением на симметрические функции.

Возвратимся теперь к якобиеву многообразию $J_{\mathfrak{m}}$ и отображению θ. Отображение θ определено для всех дивизоров X, равных нулю на S, в частности, для точек $P \subset X - S$. Докажем

Предложение 4. *Отображение* θ: $X - S \to J_{\mathfrak{m}}$ *рационально, всюду регулярно и определено над* k.

Мы воспользуемся леммой.

Лемма 15. *Пусть* M — *общая точка* $X^{(\pi)}$ *в поле* K. *Существует рациональное отображение* θ': $X \to J_{\mathfrak{m}}$, *определенное над полем* $K(M)$, *регулярное во всех точках* $X - S$, *рациональных над* K, *и совпадающее в этих точках с* θ.

Применим эту лемму. Когда M и K варьируются, отображение θ' не меняется, поскольку оно совпадает с θ во всех точках $X - S$, рациональных в k. Таким образом, можно говорить об *отображении* θ'. Так как любая точка X рациональна в подходящем поле K, мы видим, что θ' регулярно на $X - S$ и совпадает там с θ. Наконец, θ' определено над пересечением полей $K(M)$, которое совпадает с полем k.

Остается доказать лемму. Предположим, что $\pi \neq 0$; в противном случае нечего доказывать, так как группа $J_{\mathfrak{m}}$ сводится тогда к нейтральному элементу.

Пусть P — точка $X - S$, отличная от точки P_0, выбранной в п. 4, и рациональная над k. По лемме 4 существует дивизор $N \in X^{(\pi)}$, такой, что

$$N \underset{\mathfrak{m}}{\sim} -P_1 + P_0 + M$$

и $K(N) = K(M)$.

Пусть g — рациональная функция, такая, что

$$(g) = N + P_1 - P_0 - M, \quad g \equiv 1 \pmod{\mathfrak{m}}.$$

Поскольку $l_{\mathfrak{m}}(-P_1 + P_0 + M) = 1$, эта функция единственна и определена над полем $K(M)$ (см. доказательство леммы 4). Дивизор $(g)_\infty$ *полюсов* функции g не больше дивизора $P_0 + M$. Мы докажем, что он *равен* $P_0 + M$.

Прежде всего точка P_0 — полюс g, поскольку она отлична от P_1 и не входит в N (N — общий дивизор над K).

Таким образом, надо доказать, что если $M=\sum_{i=1}^{\pi} M_i$, то все M_i — полюсы g. Докажем это для одной из них, например M_π. Если бы это было не так, то мы имели бы

$$g \in L_{\mathfrak{m}}\left(P_0 - P_1 + \sum_{i<\pi} M_i\right) \text{ и } l_{\mathfrak{m}}\left(P_0 - P_1 + \sum_{i<\pi} M_i\right) \geqslant 1,$$

откуда по теореме Римана — Роха

$$i_{\mathfrak{m}}\left(P_0 - P_1 + \sum_{i<\pi} M_i\right) \geqslant 1$$

и в силу леммы 3 $i_{\mathfrak{m}}(P_0 - P_1) \geqslant \pi$. Снова применяя теорему Римана — Роха, получим $l_{\mathfrak{m}}(P_0 - P_1) \geqslant 1$, откуда следует существование функции h, такой, что

$$h \equiv 1 \pmod{\mathfrak{m}} \quad \text{и} \quad (h) = P_0 - P_1.$$

Это означает, что h — регулярный изоморфизм X на проективную прямую Λ и соотношение $(h) \equiv 1 \pmod{\mathfrak{m}}$ возможно в единственном случае $\mathfrak{m}=0$. Но в этом случае мы имели бы $\pi = g + \delta = 0$, что было исключено.

Таким образом, дивизор полюсов функции g есть $P_0 + M$, а дивизор нулей — $P_1 + N$. Отображение $g\colon X \to \Lambda$ можно рассматривать как накрытие степени $\pi + 1$. Поскольку P_0 — простой полюс, g не является p-й степенью, и это накрытие сепарабельно. Следовательно, к нему можно применить лемму 14: если положить $g^{-1}(g(P)) = P + H_P$, то отображение $P \to H_P$ есть регулярное отображение $s\colon X \to X^{(\pi)}$. Кроме того, как легко показать, это отображение определено над $K(M)$. Положим теперь

$$\theta'(P) = \varphi(M) - \varphi(H_P).$$

Отображение $\theta'\colon X \to J_{\mathfrak{m}}$ рационально и определено над $K(M)$. Покажем, что оно обладает всеми требуемыми свойствами.

Предположим, что точка P рациональна над K и не содержится в S, и пусть $a = g(P)$. Предположим, что $P \neq P_0$, т. е. $a \neq \infty$. Имеем тогда $(g - a) \geqslant P - P_0 + M$. Это показывает, что $g - a$ — однозначно (с точностью до множителя) определяемая функция, входящая в $L_{\mathfrak{m}}(P_0 + M - P)$

(см. лемму 4). Согласно доказательству этой леммы, $g-a$ не обращается в нуль на S. Если положить $g'=(g-a)/(1-a)$, то $g'\equiv 1 \pmod{\mathfrak{m}}$. Имеем

$$(g')=g^{-1}(a)-(g)_\infty=P+H_P-P_0-M,$$

откуда

$$H_P \underset{\mathfrak{m}}{\sim} -P+P_0+M.$$

Таким образом, дивизор, соответствующий $-P+P_0+M$ по лемме 4, совпадает с H_P. Это показывает, что H_P — общая точка над K и что $\varphi(H_P)$ определено. Кроме того, имеем по определению θ

$$\theta(-P)=\varphi(H_P)-\varphi(M),$$

откуда

$$\theta(P)=\theta'(P).$$

В случае $P=P_0$ (который мы исключили) эта формула тривиальна.

Наконец, θ' регулярно в P, так как с точностью до переноса на $J_\mathfrak{m}$ отображение θ' является композицией отображения s: $X\to X^{(\pi)}$, которое регулярно (лемма 14), и отображения φ: $X^{(\pi)}\to J_\mathfrak{m}$, регулярного в $s(P)=H(P)$, поскольку это общая точка $X^{(\pi)}$. Этим завершается доказательство леммы 15, а также предложения 4.

9. Универсальное свойство якобиевых многообразий $J_\mathfrak{m}$

Лемма 16. *Каноническое продолжение отображения* θ: $X-S\to J_\mathfrak{m}$ *на симметрическое произведение* $X^{(\pi)}$ *совпадает с рациональным отображением* φ *из предложения* 2.

Пусть $S\theta$ — каноническое продолжение θ на симметрическое произведение $(X-S)^{(\pi)}$. Это есть регулярное отображение $(X-S)^{(\pi)}$ в $J_\mathfrak{m}$, и его, следовательно, можно рассматривать как *рациональное* отображение $X^{(\pi)}$ в $J_\mathfrak{m}$. Чтобы доказать, что оно совпадает с φ, достаточно доказать, что

$S\theta(M) = \varphi(M)$ в случае, когда $M = \sum_{i=1}^{\pi} M_i$ — *общая* точка $X^{(\pi)}$. Но по определению

$$S\theta = \sum_{i=1}^{\pi} \theta(M_i) = \theta(M),$$

и лемма 12 показывает, что $\theta(M) = \varphi(M)$.

Итак, нет необходимости различать отображения φ и θ. Для унификации мы выбираем обозначение φ (или $\varphi_{\mathfrak{m}}$, желая подчеркнуть зависимость от $\mathfrak{m}$) как для канонического отображения $X \to J_{\mathfrak{m}}$, так и для расширения этого отображения на группу дивизоров, равных нулю на S. Заметим, что все построение зависит от выбора „начальной" точки P_0; впрочем, $\varphi(P_0) = 0$. Другой выбор P_0 изменяет φ только на перенос, как вскоре будет видно. Следующая теорема суммирует свойства отображения φ: $X \to J_{\mathfrak{m}}$.

Теорема 1. а) *Отображение* $\varphi_{\mathfrak{m}}: X \to J_{\mathfrak{m}}$ *рационально, определено над* k *и регулярно во всех точках* $X - S$.

б) *Продолжение* $\varphi_{\mathfrak{m}}$ *на дивизоры, равные нулю на* S, *определяет при переходе к фактору изоморфизм группы* $C_{\mathfrak{m}}^{0}$ *классов дивизоров степени* 0 (*по отношению к* $\mathfrak{m}$-*эквивалентности*) *на группу* $J_{\mathfrak{m}}$.

в) *Продолжение* $\varphi_{\mathfrak{m}}$ *на симметрическое произведение* $X^{(\pi)}$ *является бирациональным отображением* $X^{(\pi)}$ *на* $J_{\mathfrak{m}}$.

Очевидно, что, наоборот, свойства а), б), в) и условие нормировки $\varphi_{\mathfrak{m}}(P_0) = 0$ однозначно характеризуют $J_{\mathfrak{m}}$ и отображение $\varphi_{\mathfrak{m}}$.

Докажем теперь, что $J_{\mathfrak{m}}$ обладает свойством универсальности, сформулированным в гл. I.

Теорема 2. *Пусть* $f: X \to G$ — *рациональное отображение* X *в коммутативную группу* G, *допускающее* $\mathfrak{m}$ *в качестве модуля. Положим* $g_0 = f(P_0)$. *Тогда существует единственный алгебраический гомоморфизм* $F: J_{\mathfrak{m}} \to G$, *такой, что* $f = F \circ \varphi_{\mathfrak{m}} + g_0$.

Так как к отображению f можно прибавить перенос, то считаем $g_0 = 0$. Если D — дивизор степени 0 на X, равный нулю на S, то элемент $f(D) \in G$ не зависит от класса

$\mathfrak{m}$-эквивалентности D. При переходе к фактору получим, следовательно, гомоморфизм $C^0_{\mathfrak{m}} \to G$ группы этих классов в G. По теореме 1, б) существует, следовательно, единственный гомоморфизм $F\colon J_{\mathfrak{m}} \to G$, такой, что $f = F \circ \varphi_{\mathfrak{m}}$ для любой точки $P \in X$ (или для любого дивизора, что сводится к тому же самому). Остается показать, что F — *алгебраический* гомоморфизм. Итак, пусть Sf — продолжение f на $X^{(\pi)}$. Это есть рациональное отображение $X^{(\pi)}$ в G, регулярное на $(X - S)^{(\pi)}$ в силу определения симметрического произведения. По определению F имеем $Sf = F \circ \varphi$, если обозначить через φ каноническое отображение $X^{(\pi)} \to J_{\mathfrak{m}}$. Но φ бирегулярно на открытом непустом множестве U многообразия $J_{\mathfrak{m}}$. Отсюда следует, что F совпадает на U с регулярным отображением $Sf \circ \varphi^{-1}$. С помощью переноса получаем, что гомоморфизм F регулярен всюду.

Замечание. Доказательство теоремы 2 показывает также, что если f определено над полем K, то над тем же полем определено и Sf, а следовательно, и F.

Следствие 1. *При построении пары $(\varphi_{\mathfrak{m}}, J_{\mathfrak{m}})$ другой выбор P_0 не меняет $J_{\mathfrak{m}}$, а $\varphi_{\mathfrak{m}}$ меняет на перенос.*

Применяя теорему 2 к новому отображению $\varphi'_{\mathfrak{m}}\colon X \to J'_{\mathfrak{m}}$, получаем гомоморфизм $F\colon J_{\mathfrak{m}} \to J'_{\mathfrak{m}}$. Так же получаем гомоморфизм $F'\colon J'_{\mathfrak{m}} \to J_{\mathfrak{m}}$. Свойство единственности теоремы 2 показывает тогда, что $F \circ F' = 1$ и $F' \circ F = 1$. Следовательно, можно отождествить $J_{\mathfrak{m}}$ и $J'_{\mathfrak{m}}$, и тогда $\varphi'_{\mathfrak{m}} = \varphi_{\mathfrak{m}} + \varphi'_{\mathfrak{m}}(P_0)$.

Следствие 2. *Всякое рациональное отображение X в коммутативную группу можно разложить с помощью подходящего отображения $\varphi_{\mathfrak{m}}$.*

Действительно, по теореме 1 гл. III такое отображение всегда обладает по крайней мере одним модулем.

10. Инвариантные дифференциальные формы на $J_{\mathfrak{m}}$

Поскольку $J_{\mathfrak{m}}$ — коммутативная алгебраическая группа размерности π, инвариантные дифференциальные формы на $J_{\mathfrak{m}}$ образуют векторное пространство размерности π. Если

ω — такая форма, то $\alpha = \varphi^*(\omega)$ — дифференциальная форма на X, очевидно, регулярная вне S. Более точно, имеем

Предложение 5. *Отображение* $\omega \to \varphi^*(\omega)$ *есть биекция множества инвариантных дифференциальных форм на* $J_\mathfrak{m}$ *на множество дифференциальных форм* α *на* X, *удовлетворяющих условию* $(\alpha) \geqslant -\mathfrak{m}$.

Предположим сначала, что $\varphi^*(\omega) = 0$. Пусть $g\colon X^\pi \to J_\mathfrak{m}$ — отображение $(x_1, \ldots, x_\pi) \to \sum \varphi(x_i)$ и $h_i\colon X^\pi\colon J_\mathfrak{m}$ — отображение $(x_1, \ldots, x_\pi) \to \varphi(x_i)$. В силу того, что $g = \sum h_i$, имеем $g^*(\omega) = \sum h_i^*(\omega)$ (см. гл. III, предложение 16), откуда $g^*(\omega) = 0$. Но отображение g разлагается на $X^\pi \to \to X^\pi \to J_\mathfrak{m}$, причем отображения $X^\pi \to X^{(\pi)}$ и $X^{(\pi)} \to J_\mathfrak{m}$ являются сюръективными и сепарабельными в общей точке. [Напомним, что рациональное отображение $f\colon X \to Y$, где X и Y — неприводимые многообразия, *сюръективно* в общей точке, если $f(X)$ плотно в Y; в этом случае поле $k(Y)$ отождествляется с подполем $k(X)$, и если расширение $k(X)/k(Y)$ сепарабельно (соответственно радикально, примарно), то говорят, что f сепарабельно (соответственно радикально, примарно).] Отображение g, таким образом, само сюръективно и сепарабельно в общей точке, откуда получаем, что из $g^*(\omega) = 0$ следует $\omega = 0$ в силу характеризации сепарабельных расширений с помощью дифференциалов (см., например, [11], сообщение 13). Отображение $\omega \to \varphi^*(\omega)$, таким образом, *инъективно*.

Обозначим теперь через $\Omega(-\mathfrak{m})$ векторное пространство дифференциальных форм α на X, таких, что $(\alpha) \geqslant -\mathfrak{m}$. Теорема Римана — Роха показывает, что $\dim \Omega(-\mathfrak{m}) = \pi$, т. е. эта размерность равна размерности пространства инвариантных дифференциальных форм на $J_\mathfrak{m}$. Следовательно, достаточно показать, что $\varphi^*(\omega) \in \Omega(-\mathfrak{m})$ для любой инвариантной дифференциальной формы ω на $J_\mathfrak{m}$.

Дифференциалы $\alpha \in \Omega(-\mathfrak{m})$ не имеют полюсов вне множества S. Формула вычетов показывает, таким образом, что $\sum_{P \in S} \mathrm{Res}_P(\omega) = 0$, и, сравнивая это с гл. IV, п. 9, мы видим, что $\Omega(-\mathfrak{m})$ *есть множество дифференциалов, всюду регулярных на* $X_\mathfrak{m}$. *Для проверки того, что* $\alpha = \varphi^*(\omega)$ *вхо-*

дит в $\Omega(\mathfrak{m})$, достаточно, следовательно, показать (см. гл. IV, предложение 6), что $\mathrm{Tr}_g(\alpha)=0$ для любой рациональной функции g на X, удовлетворяющей сравнению $g\equiv 0 \pmod{\mathfrak{m}}$ и не являющейся p-й степенью.

Итак, пусть $h=\mathrm{Tr}_g$ — отображение проективной прямой Λ в группу $J_\mathfrak{m}$, определяемое, как в гл. III, п. 2. По лемме 4 гл. III, п. 6 имеем $\mathrm{Tr}_g(\alpha)=h^*(\omega)$. С другой стороны, поскольку $\mathfrak{m}$ — модуль для $\varphi\colon X\to J_\mathfrak{m}$, отображение h постоянно (гл. III, п. 5, предложение 9). Отсюда следует, что $h^*(\omega)=0$. Предложение доказано.

Следствие 1. *Пусть J — обыкновенное якобиево многообразие X. Отображение $\omega\to\varphi^*(\omega)$ является изоморфизмом множества инвариантных дифференциалов на J на множество дифференциалов первого рода на X.*

Это есть частный случай $\mathfrak{m}=0$.

Следствие 2. *Если* $\deg(\mathfrak{m})\geqslant 2$, *отображение* $\varphi_\mathfrak{m}$ *нерегулярно ни в одной точке* $P\in S$.

Пусть $P\in S$ и n_P — коэффициент при P в $\mathfrak{m}$. Из неравенства $\deg(\mathfrak{m})\geqslant 2$ получаем $\mathfrak{m}-P>0$. Теорема Римана — Роха показывает тогда, что

$$\dim\Omega(-\mathfrak{m}+P)=\pi-1,$$

и существует дифференциал $\alpha\in\Omega(-\mathfrak{m})$, не входящий в $\Omega(-\mathfrak{m}+P)$, т. е. имеющий полюс, порядок которого в точности равен n_P в точке P. По предложению 5 такой дифференциал имеет вид $\varphi_\mathfrak{m}^*(\omega)$, где ω регулярен на $J_\mathfrak{m}$. Отсюда следует, что $\varphi_\mathfrak{m}$ не может быть регулярно в P.

Замечание. Случай $\deg(\mathfrak{m})=1$ тривиален: кривая $X_\mathfrak{m}$ в этом случае сводится к X и $\mathfrak{m}$-эквивалентность есть обычная линейная эквивалентность; соответствующее якобиево многообразие есть обыкновенное якобиево многообразие.

§ 3. Строение якобиевых многообразий $J_\mathfrak{m}$

11. Обыкновенные якобиевы многообразия

В случае $\mathfrak{m}=0$ обобщенные якобиевы многообразия сводятся к обыкновенным якобиевым многообразиям J.

По теореме 1 каноническое отображение φ: $X \to J$ (определенное с точностью до переноса) всюду регулярно; то же самое относится и к продолжению его на симметрическое произведение $X^{(g)}$. Так как φ: $X^{(g)} \to J$ бирационально, образ $X^{(g)}$ плотен в J, а поскольку $X^{(g)}$ — полное многообразие, его образ замкнут и равен J. Таким образом, мы видим, что J является образом полного многообразия, и, следовательно, полно, т. е. J есть *абелево многообразие*.

Далее, отображение φ: $X \to J$ *универсально* относительно рациональных отображений X в абелевы многообразия. В самом деле, если f: $X \to A$ — такое отображение, то известно (поскольку A — полное многообразие), что оно всюду регулярно, и теорема 1 гл. III показывает, что f обладает модулем $\mathfrak{m} = 0$. Теорема 2 дает в этом случае разложение $f = F \circ \varphi$, где F: $J \to A$ — „аффинный" гомоморфизм (т. е. гомоморфизм в обычном смысле, связанный с переносом). Это свойство выражают так: «J — *многообразие Альбанезе* кривой X». Известно (см. Ленг [5]), что такое многообразие существует для любого алгебраического многообразия X; мы еще вернемся к этому вопросу.

12. Соотношения между якобиевыми многообразиями $J_\mathfrak{m}$

Пусть $\mathfrak{m}$ и $\mathfrak{m}'$ — два модуля, причем $\mathfrak{m} \geqslant \mathfrak{m}'$. Этим двум модулям и выбору начальной точки P_0 соответствуют якобиевы многообразия $J_\mathfrak{m}$ и $J_{\mathfrak{m}'}$ и отображения $\varphi_\mathfrak{m}$ и $\varphi_{\mathfrak{m}'}$, которые мы и будем сравнивать.

Предложение 6. *Существует единственный гомоморфизм F: $J_\mathfrak{m} \to J_{\mathfrak{m}'}$, такой, что $\varphi_{\mathfrak{m}'} = F \circ \varphi_\mathfrak{m}$. Этот гомоморфизм сюръективен, сепарабелен и его ядром является связная подгруппа $H_{\mathfrak{m}/\mathfrak{m}'}$ группы $J_\mathfrak{m}$.*

Отображение $\varphi_{\mathfrak{m}'}$: $X \to J_{\mathfrak{m}'}$ обладает модулем $\mathfrak{m}'$, а следовательно, тем более, модулем $\mathfrak{m}$. Так как $\varphi_{\mathfrak{m}'}(P_0) = 0$, из теоремы 2 следуют существование и единственность F.

Пусть теперь S: $X^{(\pi')} \to X^{(\pi)}$ — отображение, получаемое при переходе к фактору по отображению

$$(M_1, \ldots, M_{\pi'}) \to (M_1, \ldots, M_{\pi'}, P_0, \ldots, P_0).$$

Поскольку $J_\mathfrak{m}$ бирационально изоморфно $X^{(\pi)}$, а $J_{\mathfrak{m}'}$ изоморфно $X^{(\pi')}$, отображение s канонически определяет рациональное отображение

$$s'\colon J_{\mathfrak{m}'} \to J_\mathfrak{m}.$$

Кроме того, очевидно, что $F \circ s' = 1$, т. е. что s' — „рациональное сечение“ для проекции $F\colon J_\mathfrak{m} \to J_{\mathfrak{m}'}$. Все свойства, высказанные в предложении, следуют теперь из существования этого сечения, если дополнительно учесть, что $J_\mathfrak{m}$ *бирационально изоморфно* произведению $J_{\mathfrak{m}'} H_{\mathfrak{m}/\mathfrak{m}'}$.

Предыдущее предложение показывает по существу, что якобиевы многообразия $J_\mathfrak{m}$ образуют *проективную систему* групп; на самом деле, это сказано не совсем точно, поскольку нельзя выбрать *одну и ту же* начальную точку P_0 для *всех* модулей $\mathfrak{m}$ сразу. Говоря точнее, $J_\mathfrak{m}$ образуют проективную систему *главных однородных пространств* (см. п. 21, а также гл. VI).

Заметим, что $J_{\mathfrak{m}'}$ отождествляется с фактором $J_\mathfrak{m}/H_{\mathfrak{m}/\mathfrak{m}'}$; знание якобиевых многообразий для достаточно больших модулей $\mathfrak{m}$ дает возможность определить все якобиевы многообразия (включая наиболее общие якобиевы многообразия $J_\mathfrak{d}$, построенные Розенлихтом для любой особой кривой, имеющей X в качестве своей нормальной модели).

13. Соотношения между $J_\mathfrak{m}$ и J

Положив $\mathfrak{m}' = 0$ в предложении 6, получим, что $J_\mathfrak{m}$ есть *расширение* якобиева многообразия J с помощью связной группы. Обозначим последнюю группу через $L_\mathfrak{m}$ и изучим ее строение.

С теоретико-множественной точки зрения определение L не представляет труда: по теореме 1 точка $d \in J_\mathfrak{m}$ соответствует классу $\mathfrak{m}$-эквивалентности дивизора D, который равен нулю на S и степень которого можно считать нулевой. Образ d в J равен нулю тогда и только тогда, когда D линейно эквивалентен нулю, т. е. когда существует рациональная функция g, такая, что $D = (g)$. Поскольку D равен нулю на S, эта функция *обратима* в каждой точке $P \in S$; другими словами, $v_P(g) = 0$.

Обратно, всякая функция g, удовлетворяющая этому условию, определяет дивизор $D = (g)$, класс которого d входит в рассматриваемое ядро $L_{\mathfrak{m}}$. Имеем $d = 0$ в $J_{\mathfrak{m}}$, если $D = h$, где $h \equiv 1 \pmod{\mathfrak{m}}$, что приводит к равенству $g = \lambda h$, где λ — константа $\neq 0$.

Обозначим теперь через U_P мультипликативную группу функций f, таких, что $v_P(f) = 0$, и через $U_P^{(n)}$ — подгруппу в U_P функций f, таких, что $v_P(1 - f) \geqslant n$. Функция g определяет для каждой точки P элемент $g_P \in U_P / U_P^{(n_P)}$, где n_P обозначает коэффициент при P в $\mathfrak{m}$. Наоборот, известно, что каждой системе элементов g_P соответствует некоторая функция g. Таким образом, все сводится к рассмотрению группового произведения

$$R_{\mathfrak{m}} = \prod_{P \in S} U_P / U_P^{(n_P)}.$$

Каждый из множителей содержит в качестве подгруппы группу G_m констант. Обозначим через Δ „диагональную“ группу, образованную элементами $(\lambda, \lambda, \ldots, \lambda)$, где $\lambda \in G_m$, и положим

$$H_{\mathfrak{m}} = R_{\mathfrak{m}} / \Delta.$$

Из всего предыдущего тогда следует

Предложение 7. *Отображение $g \to (g)$ при переходе к фактору определяет биективный гомоморфизм группы $H_{\mathfrak{m}}$ на группу $L_{\mathfrak{m}}$, являющуюся ядром канонического гомоморфизма $J_{\mathfrak{m}} \to J$.*

Остается описать строение *алгебраической группы* многообразия $L_{\mathfrak{m}}$, к чему мы и переходим.

14. Алгебраическая структура на локальных группах $U/U^{(n)}$

Пусть U — мультипликативная группа формальных рядов $f(t)$, удовлетворяющих условию $v(t) = 0$, и пусть $U^{(n)}$ — подгруппа в U, образованная такими рядами, что $v(1 - f) \geqslant n$. Элемент $f \in U^{(n)}$ записывается тогда в виде

$$f = 1 + a_n t^n + \ldots.$$

Ясно, что факторгруппа $U/U^{(n)}$ допускает в качестве системы представителей полиномы

$$f = a_0 + a_1 t + \ldots + a_{n-1} t^{n-1}, \quad a_0 \neq 0.$$

Следовательно, $U/U^{(n)}$ можно рассматривать как открытое подмножество аффинного пространства размерности n, снабженного соответствующей алгебраической структурой.

Лемма 17. *Описанная выше алгебраическая структура согласована со структурой группы $U/U^{(n)}$. Кроме того, она не зависит от выбора униформизующей t.*

Если $f = a_0 + a_1 t + \ldots + a_{n-1} t^{n-1}$ и $g = b_0 + b_1 t + \ldots$ $\ldots + b_{n-1} t^{n-1}$ — два элемента $U/U^{(n)}$, то их произведение h имеет в качестве представителя элемент $c_0 + c_1 t + \ldots$ $\ldots + c_{n-1} t^{n-1}$, где

$$c_i = \sum_{r+s=i} a_r b_s,$$

Закон композиции задается, следовательно, полиномиальной формулой. Это показывает, что он всюду регулярен. Так же проверяются регулярность операции взятия обратного элемента и регулярность операции, определенной „изменением переменной“:

$$t' = \alpha_1 t + \ldots, \quad \alpha_1 \neq 0.$$

Пусть $V_{(n)}$ есть группа $U^{(1)}/U^{(n)}$, т. е. подгруппа в $U/U^{(n)}$, образованная полиномами вида

$$f = 1 + a_1 t + \ldots + a_{n-1} t^{n-1}.$$

Лемма 18. *Группа $U/U^{(n)}$ изоморфна произведению группы G_m на группу $V_{(n)}$.*

Действительно, любая функция f записывается однозначным образом в виде произведения константы $a_0 \neq 0$ на функцию $g \in V_{(n)}$. Более того, это разложение согласовано с алгебраической структурой $U/U^{(n)}$, поскольку a_0 — регулярная функция на $U/U^{(n)}$.

Группа $V_{(n)}$ является многообразием, бирегулярно изоморфным аффинному пространству размерности $n-1$. Более точно, имеет место

Лемма 19. *Для любого целого i $(1 \leqslant i \leqslant n-1)$ пусть g_i — формальный ряд порядка i. Тогда всякий элемент из $V_{(n)}$ записывается однозначным образом в виде*

$$g = (1 + a_1 g_1) \ldots (1 + a_{n-1} g_{n-1}),$$

где a_i — константы. Отображение, ставящее в соответствие g набор $(a_1, \ldots, a_{n-1})$, является бирегулярным отображением $V_{(n)}$ на аффинное пространство размерности $n-1$.

Пусть $g = 1 + b_1 t + \ldots + b_{n-1} t^{n-1}$ и $g_1 = c_1 t + \ldots$. Если положить $a_1 = b_1/c_1$, то частное $g/(1 + a_1 g_1) = h_1$ удовлетворяет условию $v(1 - h_1) \geqslant 2$. Определим, далее, a_2 так, чтобы частное $h_1/(1 + a_2 g_2) = h_2$ удовлетворяло условию $v(1 - h_2) \geqslant 3$ и т. д. Каждый раз коэффициент a_i и функция h_i определяются полиномиальной формулой, а следовательно, всюду регулярны. Как *алгебраическая группа* $V_{(n)}$ допускает разложение на множители, изоморфные G_a. Более того, имеет место

Лемма 20. *Группа $V_{(n)}$ — унипотентная группа, изоморфная группе матриц вида*

$$\begin{pmatrix} 1 & a_1 & a_2 & \ldots & a_{n-1} \\ 0 & 1 & a_1 & \ldots & a_{n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

Нужный изоморфизм получается сопоставлением t нильпотентной матрицы Жордана порядка n.

15. Структура группы $V_{(n)}$ в случае нулевой характеристики

Когда характеристика основного поля равна 0, можно определить *экспоненту* $\exp(g) = 1 + g + \ldots + g^n/n! + \ldots$ для любого формального ряда порядка > 0, причем имеет место обычная формула

$$\exp(g_1 + g_2) = \exp(g_1) \cdot \exp(g_2).$$

Предложение 8. *Для любого целого $i\,(1 \leqslant i \leqslant n-1)$ пусть g_i — формальный ряд порядка i. Всякий элемент $g \in V_{(n)}$ однозначно представляется в виде произведения*

$$g = \exp(a_1 g_1) \ldots \exp(a_{n-1} g_{n-1}),$$

где a_i — константы. Отображение, ставящее в соответствие g набор $(a_1, \ldots, a_{n-1})$, является бирегулярным изоморфизмом алгебраической группы V_n на группу $(G_a)^{n-1}$.

Существование и единственность разложения и тот факт, что оно приводит к бирегулярному отображению $V_{(n)} \to G_a^{(n-1)}$, доказываются точно так же, как в лемме 19. Единственным новым моментом является то, что сохраняется структура группы; это следует из формулы $\exp(g_1 + g_2) = \exp(g_1) \times \times \exp(g_2)$.

Следствие. *В случае характеристики нуль локальная группа $U/U^{(n)}$ изоморфна произведению $G_m \times (G_a)^{n-1}$.*

16. Структура группы $V_{(n)}$ в случае положительной характеристики

Использовать экспоненциальный ряд больше уже нельзя. Вместо него используется ряд

$$F(t) = \exp\left(-\left(t + \frac{t^p}{p} + \ldots + \frac{t^{p^n}}{p^n} + \ldots\right)\right).$$

Простое вычисление показывает, что этот ряд (с рациональными коэффициентами) можно представить в виде бесконечного произведения

$$F(t) = \prod_{(n,\,p)=1} (1 - t^n)^{\mu(n)/n},$$

где μ обозначает функцию Мёбиуса.

Последнее выражение для F показывает, очевидно, что коэффициенты *F — целые p-адические числа*, а следовательно, F сохраняет смысл в характеристике p.

Пусть теперь $\vec{x}=(x_0, x_1, \ldots)$ — вектор Витта (конечной или бесконечной длины); рассмотрим произведение рядов

$$E(\vec{x})=F(x_0)\cdot F(x_1)\ \ldots .$$

Переходя к вспомогательным компонентам $x^{(0)}, x_1^{(1)}, \ldots$ вектора $\vec{x}$, получаем

$$E(\vec{x})=\exp\left(-x^{(0)}-\frac{x^{(1)}}{p}-\frac{x^{(2)}}{p^2}-\ \ldots\right).$$

В силу аддитивности векторов Витта это означает, что

$$E(\vec{x}+\vec{y})=E(\vec{x})E(\vec{y}),$$

если $\vec{x}$ и $\vec{y}$ бесконечной длины.

В соответствии с принципом продолжения тождеств эта формула остается верной при характеристике p. *Для векторов Витта функция E заменяет экспоненту, это есть экспонента Артина — Хассе* (см. Артин и Хассе [1]; Дьёдонне [3]).

Пусть $\vec{x}$ — вектор Витта, t — скаляр. Обозначим через $\vec{x}\cdot t$ произведение $\vec{x}$ на вектор Витта $(t, 0, \ldots)$. Компонентами $\vec{x}\cdot t$ являются $(x_0 t, x_1 t^p, \ldots, x_n t^{p^n}, \ldots)$. Ряд $E(\vec{x}\cdot t)$ определен, и мы имеем

$$E(\vec{x}\cdot t)=F(x_0 t)F(x_1 t^p)\ \ldots =$$
$$=(1-x_0 t+\ \ldots)(1-x_1 t^p+\ \ldots)\ \ldots .$$

Сформулируем теперь результат, заменяющий в случае характеристики p предложение 8.

Предложение 9. *Для любого i, взаимно простого с p и $\leqslant n-1$, обозначим через r_i наименьшее целое r, такое, что $p^r \geqslant n/i$, и выберем формальный ряд g_i по-*

рядка i. Всякий элемент $g \in V_{(n)}$ однозначно представим в виде произведения

$$g = \prod_{\substack{(i,\, p)=1 \\ 1 \leqslant i \leqslant n-1}} E(\vec{a}_i \cdot g_i),$$

где $\vec{a}_i$ — векторы Витта длины r_i. Отображение, ставящее в соответствие g векторы $\vec{a}_i$, является бирегулярным изоморфизмом алгебраической группы $V_{(n)}$ на произведение групп Витта W_{r_i}.

Доказательство по существу такое же, как и доказательство леммы 19 и предложения 8.

Следствие. *В случае характеристики $p > 0$ локальная группа $U/U^{(n)}$ изоморфна произведению G_m на группы Витта.*

17. Соотношения между $J_\mathfrak{m}$ и J; определение алгебраической структуры группы $L_\mathfrak{m}$

Вернемся к обозначениям и предположениям п. 13. Группа $R_\mathfrak{m}$ есть произведение локальных групп $U_P/U_P^{(n_P)}$, причем, согласно предыдущим пунктам, каждая из этих групп каноническим образом снабжена структурой алгебраической группы. Группа $R_\mathfrak{m}$ тоже является, таким образом, алгебраической. Более того, используя лемму 18, получаем разложение

$$R_\mathfrak{m} = \prod_{P \in S} G_{m,\, P} \times \prod_{P \in S} V_{(n_P)},$$

где $G_{m,\, P}$ обозначает группу, изоморфную мультипликативной группе G_m и соответствующую точке P. (Это является частным случаем разложения линейной коммутативной группы в произведение мультипликативных групп и унипотентной группы.)

Диагональная группа Δ из п. 13 содержится в множителе $\Pi G_{m,\, P}$. Она является даже прямым сомножителем, так как если P_1 — точка S, то можно записать

$$\prod_{P \in S} G_{m,\, P} = \Delta \times \prod_{P \in S - P_1} G_{m,\, P}.$$

Факторгруппа $H_{\mathfrak{m}} = R_{\mathfrak{m}}/\Delta$ изоморфна, следовательно, произведению $G_{m,\,P} (P \in S - P)$ и $V_{(n_P)} (P \in S)$. Обозначим через θ каноническую биекцию $\theta: H_{\mathfrak{m}} \to L_{\mathfrak{m}}$. Имеет место

Теорема 3. *Отображение* $\theta: H_{\mathfrak{m}} \to L_{\mathfrak{m}}$ *является бирегулярным изоморфизмом.*

(Другими словами, структура *алгебраической группы* многообразия $L_{\mathfrak{m}}$ получается перенесением структуры $H_{\mathfrak{m}}$, которую мы и будем определять.)

Доказательство проводится в несколько этапов.

Лемма 21. *Пусть g и h — две рациональные функции на X. Для любой точки λ проективной прямой Λ пусть $D_\lambda = (g + \lambda h)$ и T — подмножество Λ, образованное $\lambda \in \Lambda$, такими, что D_λ имеет общую точку с S. Тогда $\lambda \to \varphi(D)$ является регулярным отображением $\Lambda - T$ в $L_{\mathfrak{m}}$.*

Поменяв в случае надобности местами g и h, можно предположить, что $D_\lambda = (g - \lambda)$. Пусть тогда $\psi = \mathrm{Tr}_g(\varphi)$. Это есть регулярное отображение $\Lambda - T$ в $J_{\mathfrak{m}}$ (см. гл. III) и

$$\varphi(D_\lambda) = \psi(\lambda) - \psi(\infty).$$

Это показывает, что $\lambda \to \varphi(D_\lambda)$ — регулярное отображение $\Lambda - T$ в $J_{\mathfrak{m}}$. Так как $\varphi(D_\lambda) \in L_{\mathfrak{m}}$ и $L_{\mathfrak{m}}$ снабжена структурой, индуцированной с $J_{\mathfrak{m}}$, лемма доказана.

Лемма 22. *Отображение* $\theta: H_{\mathfrak{m}} \to L_{\mathfrak{m}}$ *регулярно.*

Достаточно показать, что регулярно каждое в отдельности из отображений $\theta: G_{m,\,P} \to L_{\mathfrak{m}}$ и $\theta: V_{(n_P)} \to L_{\mathfrak{m}}$. Пусть $\lambda \in G_{m,\,P}$. По определению имеем $\theta(\lambda) = \varphi((U_\lambda))$, где u_λ — рациональная функция на X, сравнимая с $\lambda \pmod{\mathfrak{m}}$ в P и сравнимая с $1 \pmod{\mathfrak{m}}$ в точках $S - P$. Пусть v — такая функция, что $v \equiv 1 \pmod{\mathfrak{m}}$ в P, $v \equiv 0 \pmod{\mathfrak{m}}$ на $S - P$. Можно считать, что $u_\lambda = (\lambda - 1)v + 1$. Лемма 21 показывает тогда, что $\lambda \to \varphi((u_\lambda))$ — регулярное отображение $G_{m,\,P} = \Lambda - \{0\} - \{\infty\}$ в $L_{\mathfrak{m}}$. Таким же образом рассуждаем применительно к $V_{(n)}$. Для каждого i $(1 \leqslant i \leqslant n_P - 1)$ выбираем функцию g_i порядка i в P и порядка $\geqslant n_Q$ в $Q \in S - P$. Лемма 21 показывает, что $\lambda_i \to \varphi((1+\lambda_i g_i))$ есть регулярное отображение $\Lambda - \{\infty\}$ в $L_\mathfrak{m}$. Отсюда, применяя лемму 19, получаем нужный результат.

Таким образом, отображение $\theta\colon H_\mathfrak{m} \to L_\mathfrak{m}$ есть биективный и регулярный гомоморфизм. В случае характеристики 0 из этих свойств вытекает, что θ бирегулярен: но это не так в случае характеристики P (можно только утверждать, что он радикален). Надо еще доказать, что касательное отображение к θ биективно, другими словами, что из $\theta^*(\beta)=0$ следует $\beta=0$, если β — инвариантная дифференциальная форма степени 1 на $L_\mathfrak{m}$ (см. гл. III, п. 11, следствие 2 предложения 16). Но группа $L_\mathfrak{m}$ определяется как подгруппа якобиева многообразия $J_\mathfrak{m}$. Ее инвариантные дифференциалы индуцируются дифференциалами $J_\mathfrak{m}$, и дифференциал ω на $J_\mathfrak{m}$ индуцирует 0 на $L_\mathfrak{m}$ тогда и только тогда, когда он порожден дифференциалом обыкновенного якобиева многообразия J. Таким образом, все сводится к доказательству следующей леммы.

Лемма 23. *Если ω — инвариантная дифференциальная форма на $J_\mathfrak{m}$, не порожденная инвариантной дифференциальной формой на J, то $\theta^*(\omega)\neq 0$.*

Пусть $\alpha=\varphi^*(\omega)$ — дифференциал, индуцированный на X дифференциалом ω. В силу предложения 5 и его следствия 1 имеем $(\alpha) \geqslant -\mathfrak{m}$, и α не является дифференциалом первого рода. Пусть $P \in S$ — полюс α и n — его порядок. Имеем $1 \leqslant n \leqslant n_P$. Предположим сначала, что $n \geqslant 2$, и пусть g — рациональная функция порядка $n-1$ в P и порядка $\geqslant n_Q$ в $Q \in S - P$, не являющаяся p-й степенью. Пусть $\psi = \mathrm{Tr}_g(\varphi)$ — регулярное отображение $\Lambda - \{0\}$ в $J_\mathfrak{m}$. С другой стороны, отображение $\lambda \to 1+\lambda g$ определяет регулярное отображение $\Lambda - \{\infty\}$ в $U_P/U_P^{(n_P)}$ (см. леммы 19 и 22) и после композиции регулярное отображение $h\colon \Lambda - \{\infty\} \to J_\mathfrak{m}$. Поскольку h факторизуется θ, достаточно показать, что $h^*(\omega)\neq 0$. Но отображения h и ψ связаны формулой

$$h(\lambda)=\psi\left(-\frac{1}{\lambda}\right)-\varphi(\infty).$$

Достаточно, следовательно, доказать, что $\psi^*(\omega) \neq 0$. По лемме 4 гл. III, п. 6 имеем $\psi^*(\omega) = \mathrm{Tr}_g(\alpha)$. Если обозначить через λ тождественное отображение Λ на Λ, то формула следов показывает, что

$$\mathrm{Res}_0(\lambda \, \mathrm{Tr}_g(\alpha)) = \sum_{g(Q)=0} \mathrm{Res}_Q(g_\alpha) = \mathrm{Res}_P(g_\alpha).$$

Последнее выражение отлично от нуля по предположению о g и α. Таким образом, $\mathrm{Tr}_g(\alpha) \neq 0$, что и завершает доказательство в случае $n \geqslant 2$. При $n = 1$ за g можно принять функцию $\equiv 1 \pmod{\mathfrak{m}}$ в P и $\equiv 0 \,(\mathrm{mod} \cdot \mathfrak{m})$ в $S - P$. Имеем $\mathrm{Res}_1(\lambda \, \mathrm{Tr}_g(\alpha)) \neq 0$, и доказательство завершается точно так же.

Замечание. Таким образом $J_\mathfrak{m}$ — „расширение“ линейной группы $L_\mathfrak{m}$, которую мы определили с помощью обыкновенного якобиева многообразия. Например, если $\mathfrak{m} = 2P$, то $L_\mathfrak{m} = G_a$; если $\mathfrak{m} = P + Q$, $P \neq Q$, то $L_\mathfrak{m} = G_m$. Но знания J и $L_\mathfrak{m}$, очевидно, недостаточно для определения $J_\mathfrak{m}$ — необходимо еще определить тип расширения. Мы еще вернемся к этому в гл. VII.

18. Локальные символы

Пусть $g \in U_P$, где $P \in S$. Элемент g определяет при переходе к фактору элемент из $U_P / U_P^{(n_P)}$, а следовательно, элемент группы $H_\mathfrak{m}$, который мы обозначим через $\bar{g}$.

Предложение 10. $\theta(\bar{g}) = -(\varphi_\mathfrak{m}, g)_P$.

Пусть g' — рациональная функция, удовлетворяющая условиям

$$g' \equiv g \pmod{\mathfrak{m}} \text{ в } P; \quad g' \equiv 1 \pmod{\mathfrak{m}} \text{ на } S - P.$$

По определению $\theta(\bar{g}) = \varphi_m((g'))$. С другой стороны, свойства 1) и 2) локальных символов показывают, что

$$(\varphi_\mathfrak{m}, g')_P = (\varphi_\mathfrak{m}, g)_P; \quad (\varphi_\mathfrak{m}, g')_Q = 0 \quad \text{при} \quad Q \in S - P.$$

Применяя свойства 3) и 4) локальных символов, получаем

$$(\varphi_{\mathfrak{m}}, g)_P = -\sum_{Q \in S} (\varphi_{\mathfrak{m}}, g')_Q = -\sum_{Q \in S} v_Q(g')\varphi_{\mathfrak{m}}(Q) = -\varphi_{\mathfrak{m}}((g')),$$

откуда и следует нужный результат.

Таким образом, отображение $f: X \to G$ есть комбинация локальных символов относительно точек $P \in S$ (с точностью до перемены знака).

Отметим также, что если отображение $f: X \to G$ разлагается на $X \to J_{\mathfrak{m}} \xrightarrow{F} G$ (см. теорему 2), то $(f, g)_P = F((\varphi_{\mathfrak{m}}, g)_P)$, откуда $(f, g)_P = -F \circ \theta(\bar{g})$. Таким образом, *знание локальных символов* $(f, g)_P$ *эквивалентно знанию ограничения* F *на* $L_{\mathfrak{m}}$. Имеем также, что локальные символы — регулярные функции от g в смысле структуры алгебраической группы для групп $U_P/U_P^{(n)}$.

19. Случай поля комплексных чисел

Предположим, что основное поле k—это поле комплексных чисел **C**. Алгебраическая структура $J_{\mathfrak{m}}$ определяет в этом случае *аналитическую* структуру на $J_{\mathfrak{m}}$, которая превращает $J_{\mathfrak{m}}$ в комплексную группу Ли. Мы собираемся определить эту группу.

Нам потребуется две леммы.

Лемма 24. *Пусть G — связная алгебраическая коммутативная группа, и p: $G' \to G$ — связное конечное накрытие (в топологическом смысле) группы G. Тогда на G существует и притом единственная структура алгебраической группы, совместимая с ее аналитической структурой и такая, что p—регулярное рациональное отображение.*

Пусть N — ядро p. Это есть конечная группа и, следовательно, существует целое число n, такое, что $N \subset G'_n$, где G'_n обозначает подгруппу элементов порядка n группы G'. Умножение на n является эндоморфизмом G', касательное отображение к которому сюръективно. Таким образом, этот эндоморфизм превращает G' в собственное накрытие с конечной группой G'_n в качестве ядра. Так как $N \subset G'_n$, этот гомоморфизм определяет при переходе к фактору гомоморфизм h: $G \to G'$, а композиция $p \circ h$ определяет умножение на n в G. Ядро H гомоморфизма h конечно, и G' отождествляется с G/H. Таким образом, G' как факторгруппу G можно снабдить структурой алгебраической группы. Отсюда немедленно следует, что эта структура отвечает всем поставленным требованиям и что она единственна

Лемма 25. *При предположениях предыдущей леммы пусть f: $X \to G'$ — непрерывное отображение неприводимого алгебраического многообразия в группу G'. Для того чтобы f было рациональным всюду регулярным отображением, необходимо и достаточно, чтобы $p \circ f$ было рациональным регулярным отображением X в G.*

Необходимость очевидна. Предположим, что $p \circ f = g$ — всюду регулярное рациональное отображение. Из того, что $G' \to G$ — накрытие, заключаем, что f *голоморфно*. Пусть $X' \to X$ — прообраз накрытия (в алгебраическом смысле) $G' \to G$ при отображении g. По определению X' отождествляется с подмногообразием $X \times G'$, образованным парами (x, y'), такими, что $g(x) = p(y')$. Как известно (см., например, Вейль [12], приложение), связные компоненты X' одни и те же как в топологии Зарисского, так и в обыкновенной топологии, т. е. отображение f определяет голоморфное сечение s накрытия $X' \to X$ по формуле $s(x) = (x, f(x))$. Отсюда вытекает, что $s(X)$ *неприводимая компонента* X'. График s в $X \times X'$ является, следовательно, алгебраическим подмногообразием и проекция $s(X) \to X$ есть регулярное рациональное отображение, являющееся аналитическим изоморфизмом. Таким образом, это бирегулярный изоморфизм (Серр [3], предложение 9). Значит, s регулярно, а следовательно, регулярно и f.

Замечания. 1. Можно избежать ссылки на последнюю работу, используя тот факт, что пополнения локальных колец X и $s(X)$ совпадают. Если X нормально, то можно также сослаться на „основную теорему“ Зарисского.

2. Мы использовали тот факт, что неприводимое алгебраическое многообразие связно в обычной топологии. В частном случае кривых можно дать очень простое доказательство этого факта (Шевалле [1], стр. 250). Прежде всего можно

считать, что кривая X неособая (поскольку образ связного пространства связен) и полная (поскольку связная поверхность остается связной, если к ней добавить конечное число точек). Предположим теперь, что X имеет по крайней мере две связные компоненты X_1 и X_2, и пусть $P \in X_1$. Применяя теорему Римана — Роха к дивизору nP, где n достаточно велико, видим, что существует непостоянная функция f на X, имеющая P своим единственным полюсом. Функция f индуцирует, следовательно, на X_2 всюду голоморфную функцию, совпадающую с константой в силу принципа максимума, что невозможно, так как непостоянная рациональная функция принимает каждое значение лишь конечное число раз.

Вернемся теперь к якобиеву многообразию $J_{\mathfrak{m}}$. Если обозначить через T касательное пространство к $J_{\mathfrak{m}}$ в начальной точке, то T будет двойственно пространству инвариантных дифференциальных форм на $J_{\mathfrak{m}}$, которое канонически изоморфно $\Omega(-\mathfrak{m})$ (см. предложение 5). Таким образом, определение T зависит только от X и $\mathfrak{m}$. Далее, экспоненциальное отображение exp: $T \to J_{\mathfrak{m}}$ превращает T в накрытие $J_{\mathfrak{m}}$, ядро которого мы обозначим через $\Gamma_{\mathfrak{m}}$. Это дискретная подгруппа в T.

Можно определить отображение $\varphi_{\mathfrak{m}}$: $X - S \to J_{\mathfrak{m}}$ следующим образом. Пусть P_0 — фиксированная начальная точка и $P \in X - S$. Выберем путь γ в $X - S$ с началом в P_0 и концом в P. Для любой дифференциальной формы $\omega \in \Omega(-\mathfrak{m})$ интеграл $\int_{P_0}^{P} \omega$ (вдоль γ) линейно зависит от ω. Его можно, следовательно, отождествить с элементом $\theta(\gamma) \in T$. По определению

$$\langle \theta(\gamma), \omega \rangle = \int_{\gamma} \omega.$$

Элемент $\theta(\gamma)$ зависит только от *класса гомотопии* γ на $X - S$, а потому определяет отображение

$$\theta: \tilde{X} - \tilde{S} \to T$$

универсального накрытия $\tilde{X} - \tilde{S}$ для $X - S$ в T. Согласно построению, отображение $\exp \circ \theta$: $\tilde{X} - \tilde{S} \to J_{\mathfrak{m}}$ имеет тот же дифференциал, что и композиция отображений $\tilde{X} - \tilde{S} \to$

$\to X - S \to J_{\mathfrak{m}}$. Так как каждое из них отображает P_0 в 0, то они совпадают.

Это показывает, в частности, что если γ — *цикл* степени $\theta(\gamma)$, то элемент $\theta(\gamma)$ входит в ядро $\Gamma_{\mathfrak{m}}$ отображения exp: $T \to J_{\mathfrak{m}}$. Так получается канонический гомоморфизм

$$\theta\colon H_1(X - S) \to \Gamma_{\mathfrak{m}},$$

где $H_1(X - S)$ обозначает группу гомологий размерности 1 с целыми коэффициентами.

Предложение 11. *Гомоморфизм θ является биекцией $H_1(X - S)$ на $\Gamma_{\mathfrak{m}}$.*

Пусть s — число точек S. Согласно предыдущим пунктам, группа $J_{\mathfrak{m}}$ является расширением J с помощью произведения $s - 1$ раз взятых групп G_m и групп G_a. Фундаментальная группа $\pi_1(J_{\mathfrak{m}})$ является, следовательно, расширением группы $\pi_1(J)$ с помощью группы $\mathbf{Z}^{s-1}$; она является свободной абелевой группой ранга $2g + s - 1$. С другой стороны, известно, что $H_1(X)$ — свободная группа ранга $2g$, и точная последовательность групп гомологий показывает тогда, что $H_1(X-S)$ — свободная группа ранга $2g + s - 1$. Поскольку две группы $\Gamma_{\mathfrak{m}} = \pi_1(J_{\mathfrak{m}})$ и $H_1(X - S)$ — свободные группы одинакового ранга, достаточно показать, что θ *сюръективно*.

Предположим, что это не так. Тогда существует подгруппа Γ' группы $\Gamma_{\mathfrak{m}}$ конечного индекса > 1 в $\Gamma_{\mathfrak{m}}$, содержащая образ $H_1(X - S)$ при отображении θ. Пусть $J' = T/\Gamma'$; это конечное накрытие $J_{\mathfrak{m}}$. Далее, предположение, что Γ' содержит $\theta(H_1(X - S))$, показывает, что отображение $\varphi_{\mathfrak{m}}$ поднимается до непрерывного (и даже голоморфного) отображения $\psi\colon X - S \to J'$. Леммы 24 и 25 показывают, что J' каноническим образом снабжается структурой алгебраической группы, для которой отображение ψ рационально и регулярно. Применяя к ψ предложение 14 гл. III, видим, что $\mathfrak{m}$ — модуль для ψ и, согласно теореме 2, существует гомоморфизм $F\colon J_{\mathfrak{m}} \to J'$, такой, что $\psi = F \circ \varphi_{\mathfrak{m}}$. Композиция F и проекции $J' \to J_{\mathfrak{m}}$ является тогда тождественным отображением, что невозможно. Этим доказательство завершается.

Отождествляя $\Gamma_{\mathfrak{m}}$ с $H_1(X - S)$ с помощью θ, имеем

Следствие. *Группа $J_{\mathfrak{m}}$ аналитически изоморфна фактору двойственного пространства к* $\Omega(-\mathfrak{m})$ *по дискретной подгруппе* $H_1(X-S)$.

Для обыкновенных якобиевых многообразий это хорошо известный результат.

Замечание. В общем случае аналитическая структура $J_{\mathfrak{m}}$ не определяется однозначно своей алгебраической структурой. В самом деле, легко привести примеры алгебраических групп, *имеющих аналитические автоморфизмы, не являющиеся алгебраическими* (группа $G_a \times G_m$), а также примеры алгебраических групп, *аналитически изоморфных, но не изоморфных алгебраически* ($G_m \times G_m$ аналитически изоморфна расширению группы G_a с помощью эллиптической кривой J).

§ 4. Построение обобщенных якобиевых многообразий; случай произвольного основного поля

20. Спуск основного поля

Пусть k_1 — расширение поля k и V — алгебраическое многообразие над k_1 (или k_1-*многообразие*). „Спустить основное поле V до k" означает найти k-многообразие W, бирегулярно изоморфное V над k_1. Другими словами, для этого нужно иметь бирегулярный изоморфизм $f\colon W \to V$, определенный над k_1.

Предположим, начиная с этого места, что k_1 — конечное *нормальное расширение* поля k. Пусть $\mathfrak{g}$ — его группа Галуа. Обозначим через V^σ многообразие, получаемое из V применением σ. С точки зрения „Оснований" (Вейль А. [3]), где V определено с помощью карт и отображений перехода u_{ij}, многообразие V^σ определяется теми же картами, но другими отображениями перехода, а именно u_{ij}^σ. С точки зрения *схем* Шевалле (Картан и Шевалле [1]), V^σ определяется тем же полем и теми же локальными кольцами, что и V, σ изменяет лишь структуру k_1-алгебры. Все это применимо равным образом и к W, но, поскольку W — k-многообразие, W и W^σ можно отождествить. Преобразование f^σ отображения f

является, таким образом, бирегулярным изоморфизмом W на V^σ, что позволяет положить

$$h_\sigma = f^\sigma \circ f^{-1}. \qquad (*)$$

Отображения h_σ $(\sigma \in \mathfrak{g})$ являются k_1-изоморфизмами V на V^σ и удовлетворяют тождеству

$$h_{\sigma\tau} = (h_\sigma)^\tau \circ h_\tau. \qquad (**)$$

Таким образом, можно уточнить понятие спуска основного поля следующим образом. Дан k_1-изоморфизм h_σ: $V \to V^\sigma$, удовлетворяющий (**); ищется k-многообразие W и изоморфизм f: $W \to V$, удовлетворяющий (*). В этой постановке задача и будет рассматриваться в дальнейшем.

Предложение 12. а) *Если спуск основного поля возможен, то он однозначен с точностью до k-изоморфизма.*

б) *Спуск основного поля возможен, когда V есть объединение открытых аффинных множеств U_i, определенных над k_1 и таких, что*

$$h_\sigma(U_i) \subset U_i^\sigma. \qquad (***)$$

Пусть f: $W \to V$ и f: $W' \to V$ — два решения задачи о спуске основного поля и $\varphi = f^{-1} \circ f'$. По предположению φ — бирегулярный изоморфизм, определенный над k_1. С другой стороны, формулы $f^\sigma \circ f' = h_\sigma = f'^\sigma \circ f'^{-1}$ показывают, что $\varphi^\sigma = \varphi$ для всех $\sigma \in \mathfrak{g}$, откуда следует, что φ определено над k, что и доказывает а).

При доказательстве б) можно ограничиться случаем, когда многообразие V аффинно. Пусть A — его координатное кольцо, рассматриваемое как k_1-алгебра. Координатное кольцо V^σ есть A, рассматриваемое как k_1-алгебра с применением σ, а задание изоморфизма h_σ: $V \to V^\sigma$ эквивалентно заданию автоморфизма $\bar{\sigma}$ для A, продолжающего изоморфизм σ поля k_1. Условие (**) означает, что $\overline{\sigma\tau} = \bar{\sigma} \cdot \bar{\tau}$, другими словами, что группа $\mathfrak{g}$ действует на A. Пусть $B = A^\mathfrak{g}$ — множество элементов A, инвариантных относительно операций $\bar{\sigma}$, $\sigma \in \mathfrak{g}$. Поскольку $[k_1 : k] < \infty$, кольцо A есть k-алгебра конечного типа и любой элемент A цел над B. Согласно лемме 10 гл. III, отсюда следует, что B — k-алгебра конечного типа. Пусть W — аффинное k-многообразие, имеющее B в качестве координатного кольца. Чтобы доказать, что W удовлетворяет поставленному в задаче требованию, достаточно доказать, что алгебра $B \otimes_k k_1$ отождествляется с A. Это вытекает из следующей хорошо известной леммы.

Лемма 26. *Пусть E — векторное пространство над полем k_1; предположим, что для каждого $\sigma \in \mathfrak{g}$ дана σ-линейная биекция $\bar{\sigma}$ пространства E на себя, такая, что $\overline{\sigma\tau} = \bar{\sigma} \cdot \bar{\tau}$. Если F обозначает множество элементов E, инвариантных относительно операций $\bar{\sigma}$, то $E = F \otimes_k k_1$.* (Другими словами, E обладает базой, образованной элементами, инвариантными относительно $\bar{\sigma}$.)

Напомним кратко доказательство этой леммы. Положим $r = [k_1 : k]$, и пусть C — алгебра эндоморфизмов векторного пространства k_1 над полем k. Гомотетии образуют подалгебру в C, которую можно отождествить с k_1. Далее, k-линейные комбинации элементов $\mathfrak{g}$ образуют другую подалгебру (обозначим ее через D) алгебры C. Пусть θ: $k_1 \otimes_k D \to C$ — линейное отображение, определенное произведением. Теорема о независимости автоморфизмов показывает, что θ инъективно, а так как $k_1 \otimes_k D$ и C имеют одну и ту же размерность r^2, то θ биективно. Это показывает, что $k_1 \otimes_k D$, снабженное надлежащей структурой алгебры (структурой „скрещенного произведения“), является простой алгеброй. Но задание операций $\bar{\sigma}$ превращает E в модуль над $k_1 \otimes_k D$. Как известно, отсюда следует, что E — прямая сумма простых модулей, каждый из которых изоморфен k_1. Это показывает, что E имеет вид $F \otimes_k k_1$ и завершает доказательство. (Оносительно подробностей доказательства см. Бурбаки, Алгебра, гл. VIII.)

Следствие 1. *Спуск основного поля возможен, когда многообразие V удовлетворяет следующему условию:*

(****) *Всякое конечное подмножество V, состоящее из алгебраических точек над k_1, содержится в открытом аффинном алгебраическом над k_1 множестве.*

Отметим сначала, что в условии (****) можно требовать, чтобы искомое открытое аффинное множество было определено над k_1; в противном случае достаточно заменить его на пересечение множеств, сопряженных ему над k_1. Проверим, что (****) $\Rightarrow$ (***). Пусть x — точка V, алгебраическая над k_1. Для каждого $\sigma \in \mathfrak{g}$ выберем продолжение σ на $k_1(x)$, обозначая его опять через σ. Определена точка x^σ, входящая в V^σ. Если положить $y_\sigma = h_\sigma^{-1}(x^\sigma)$, то условие (****) показывает существование открытого аффинного множества U в V, содержащего все y_σ. Кроме того, согласно сказанному выше, можно считать, что U определено над k_1. Положим

$$U' = \bigcap h_\tau (U)^{\tau^{-1}}.$$

Открытое множество U' является открытым аффинным подмножеством V, определенным над k_1, и содержит точку x, так как $x^\tau \in h_\tau(U)$. Непосредственное вычисление показывает, что $h_\sigma(U') = U'^\sigma$. Открытые множества U' обладают, следовательно, всеми требуемыми свойствами, а поскольку они покрывают множество точек V, алгебраических над k_1, то они покрывают все V.

Следствие 2. *Спуск основного поля возможен в случае, когда V является*

1) *либо локально замкнутым подмногообразием проективного пространства*;

2) *либо однородным пространством алгебраической группы G, определенным над k.*

Покажем, что в каждом случае выполняется условие (****). В случае 1) пусть $\overline{V}$ — замыкание V и $F = \overline{V} - V$. Множество F определено над алгебраическим расширением K поля k_1. Элементарные рассуждения показывают тогда, что для достаточно большого n существует однородный полином Φ степени n с коэффициентами из K, обращающийся в нуль на F и не обращающийся в нуль ни в одной точке данного конечного множества S. Множество U точек V, в которых Φ не обращается в нуль, будет открытым аффинным множеством, удовлетворяющим нашим требованиям (см. АКП, п. 52).

В случае 2) выберем открытое аффинное множество U_1 многообразия V, определенное над k_1, и для всех $s \in S$ обозначим через A_s множество $g \in G$, таких, что $g \cdot s \in U_1$. Множества A_s являются открытыми непустыми подмножествами G и имеют, следовательно, общую точку g, которую можно считать алгебраической над k_1. Множество $U = g^{-1}U_1$ отвечает нашим требованиям.

Замечание. Предыдущие результаты аналогичны результатам гл. III, п. 12 относительно факторов многообразия по конечной группе автоморфизмов. Метод, которому мы следовали, сводится к рассмотрению V как многообразия над k (обязательно приводимого: его компоненты соответствуют V^σ) и переходу к фактору по группе автоморфизмов, определяемой операциями h_σ.

21. Главные однородные пространства

Пусть G — алгебраическая группа, определенная над полем k. *Однородное пространство* H над группой G есть непустое алгебраическое многообразие, на котором транзитивно действует группа G; другими словами, дано отображение $(g, h) \to g \cdot h$ многообразия $G \times H$ в H, всюду регулярное и удовлетворяющее обычным тождествам

$$1 \cdot h = h, \quad g \cdot (g' \cdot h) = (g \cdot g') \cdot h,$$

причем для всех $h \in H$ отображение $g \to g \cdot h$ является сюръекцией G на H. Если H и отображение $G \times H \to H$ определены над k, то говорят, что однородное пространство H определено над k или что H — k-однородное пространство. [Заметим, что однородное пространство *не обязательно* имеет вид G/G', где G' — алгебраическая подгруппа G. Действительно, для отождествления H с G/G' необходимо сначала выбрать точку $h \in H$, рациональную над k, а такая точка может и не существовать; далее, если она существует, отображение $G/G' \to H$ в общем случае не изоморфизм, а лишь радикальное отображение.]

Однородное пространство H называется *главным*, если из $g \cdot h = h$ следует $g = 1$ и если отображение, ставящее в соответствие каждой паре (h, h') точек H однозначный элемент $g \in G$, для которого $h' = g \cdot h$, является регулярным отображением $H \times H$ в G. Если последнее отображение определено над k, то говорят, что H главное однородное пространство, определенное над k.

Если H имеет рациональную точку над k, скажем h_0, отображение $g \to g \cdot h_0$ есть бирегулярный изоморфизм G на H; можно сказать, что H — „аффинное пространство", соответствующее группе G. При алгебраически замкнутом поле нет, следовательно, никакой разницы между „главным однородным пространством" и „группой", что не так при произвольном поле, так как классы главных однородных пространств над G образуют множество, аналогичное „группе Брауэра", и зависят от арифметических свойств k. Более точно это множество изоморфно $H^1(\mathfrak{g}_s, G_s)$, где $\mathfrak{g}_s$ - группа Галуа k_s/k (k_s - сепарабельное замыкание k) и G_s обозначает группу точек G, рациональных над k_s. Разумеется, когомологии должны быть определены с помощью *непрерывных* цепей, причем $\mathfrak{g}_s$ имеет естественную топологию групп Галуа, а G_s имеет дискретную топологию (см Ленг и Тейт [1]). Если k — конечное поле, то $H^1(\mathfrak{g}_s, G_s)$ тривиальна, что будет проверено в гл VI. Но $H^1(\mathfrak{g}_s, G_s)$ уже нетривиальна в случае числовых или p-адических полей (см., например, Тейт [2]).

22. Построение якобиевых многообразий $J_\mathfrak{m}$ над совершенным полем

Пусть k — совершенное поле и $\bar{k}$ его алгебраическое замыкание. Пусть X кривая, определенная над k, и $\mathfrak{m}$ — модуль над X. Мы предположим, что $\mathfrak{m}$ *рационален* над k (см. § 1); поскольку k совершенно, это означает лишь то, что точки носителя S алгебраичны над k и что $\mathfrak{m}^\sigma = \mathfrak{m}$ для всех элементов σ из группы Галуа расширения $\bar{k}/k$. Мы покажем, что при этих условиях якобиево многообразие $J_\mathfrak{m}$ можно определить над полем k.

Мы знаем, во всяком случае, что $J_\mathfrak{m}$ может быть определено над полем $\bar{k}$, как и каноническое отображение

$\varphi_{\mathfrak{m}}\colon X \to J_{\mathfrak{m}}$. Так как для построения алгебраического многообразия необходимо иметь лишь конечное число констант, то из этого тотчас же вытекает существование конечного расширения k_1/k, такого, что многообразие $J_{\mathfrak{m}}$, его закон композиции и отображение $\varphi_{\mathfrak{m}}$ будут определены над k_1. Расширив в случае необходимости k_1, можем считать k_1 расширением Галуа поля k. Пусть $\mathfrak{g}$ — его группа Галуа.

Применим теперь к многообразию $J_{\mathfrak{m}}$ процесс спуска основного поля, описанный в п. 20. Пусть $\sigma \in \mathfrak{g}$ и $\theta_{\mathfrak{m}}^{\sigma}\colon X \to J_{\mathfrak{m}}^{\sigma}$. Отображение $\varphi_{\mathfrak{m}}^{\sigma}$ обладает модулем $\mathfrak{m}^{\sigma} = \mathfrak{m}$, а следовательно, представляется в виде $\varphi_{\mathfrak{m}}^{\sigma} = h_{\sigma} \circ \varphi_{\mathfrak{m}}$, где $h_{\sigma}\colon J_{\mathfrak{m}} \to J_{\mathfrak{m}}^{\sigma}$ — „аффинный“ гомоморфизм. Вообще говоря, отображение h_{σ} определено над $\bar{k}$; в нашем же случае, если α — k_1-автоморфизм поля $\bar{k}$, то $\varphi_{\mathfrak{m}}^{\alpha} = \varphi_{\mathfrak{m}}$, $\varphi_{\mathfrak{m}}^{\alpha\sigma} = \varphi_{\mathfrak{m}}^{\sigma}$, откуда $\varphi_{\mathfrak{m}}^{\sigma} = h_{\alpha}^{\sigma} \circ \varphi_{\mathfrak{m}}$ и единственность $h_{\sigma\tau}$ показывает, что $h_{\sigma}^{\alpha} = h_{\sigma}$, т. е. что h_{σ} определено над k_1. Та же единственность доказывает справедливость формулы $h_{\sigma\tau} = (h_{\sigma})^{\tau} \circ h_{\tau}$. Таким образом, можно произвести спуск основного поля с помощью h_{σ} и получить k-многообразие, которое мы обозначим через $J_{\mathfrak{m}}^{(1)}$. Таким же образом, действуя с однородными частями $\overset{0}{h}_{\sigma}$ аффинных гомоморфизмов h_{σ}, получим с помощью спуска основного поля другое k-многообразие, которое обозначим через $J_{\mathfrak{m}}^{(0)}$. Поскольку $\overset{0}{h}_{\sigma}$ — гомоморфизмы относительно групповой структуры $\overset{0}{J}_{\mathfrak{m}}$, групповой закон $\overset{0}{J}_{\mathfrak{m}}$, индуцированный с $J_{\mathfrak{m}}$, *определяется над k.* Кроме того, $J_{\mathfrak{m}}^{(1)}$ — *главное однородное пространство*, определенное над k, и отображение $\varphi_{\mathfrak{m}}\colon X \to J_{\mathfrak{m}}^{(1)}$ *определено над k.*

Далее, отображение $\varphi_{\mathfrak{m}}\colon X \to J_{\mathfrak{m}}^{(1)}$ можно охарактеризовать как обладающее свойством *универсальности.* Вообще пусть H — главное однородное пространство над группой G и f — отображение кривой X в H. Если D — дивизор *степени* 0 на X, равный нулю на множестве точек, где f не определена, то можно определить $f(D)$ как элемент *группы* G. В частности, это дает возможность говорить, что f *обладает модулем* $\mathfrak{m}$: как только $D_{\mathfrak{m}} \sim 0$, должно быть $f(D) > 0$.

Предложение 13. *Пусть* $f\colon X \to H$ — *рациональное отображение кривой* X *в главное однородное пространство* H *над группой* G. *Если* f *обладает модулем* $\mathfrak{m}$, *то можно представить* f *в виде*

$$f = \theta \circ \varphi_{\mathfrak{m}},$$

где $\theta\colon J_{\mathfrak{m}}^{(1)} \to H$ — *аффинный гомоморфизм. Это разложение однозначно; если, кроме того,* A *определено над расширением* k' *поля* k, *то и* θ *определено над тем же полем.*

Существование и единственность θ не зависят от основного поля и уже доказаны (теорема 2). Предположим поэтому, что f определено над расширением k' поля k, и пусть $k'' = k' \cdot k$ — композит полей k' и $\bar{k}$. Покажем сначала, что θ определено над k''. Поскольку k'' содержит $\bar{k}$, можно отождествить $J_{\mathfrak{m}}^{(1)}$ с $J_{\mathfrak{m}}$, и построение θ, данное в доказательстве теоремы 2 $\left(\text{в виде композиции } J_{\mathfrak{m}} \to X^{(\pi)} \to H\right)$, показывает, что θ определено над k''. Так как k'' — расширение Галуа над k', достаточно убедиться теперь в том, что $\theta^{\alpha} = \theta$ для всех k'-автоморфизмов α универсальной области. Но $f = \theta^{\alpha} \circ \varphi_{\mathfrak{m}}$, поскольку $\varphi_{\mathfrak{m}}$ и f определены над k', откуда $\theta^{\alpha} = \theta$ в силу единственности θ.

Следствие. *Отображение* $\varphi_{\mathfrak{m}}\colon X \to J_{\mathfrak{m}}^{(1)}$ *характеризуется с точностью до* k*-изоморфизма свойством предложения* 13.

Замечание. Предыдущие рассуждения имеют более общее значение — они показывают, что все „канонические" построения можно проводить над основным полем исходного многообразия при условии, что это поле совершенно. В качестве примера вернемся к ситуации п. 5. Пусть Y — бирациональная группа, определенная над совершенным полем k. Из леммы 8 (непосредственно доказанной Розенлихтом для алгебраически замкнутых полей) следует, что Y бирационально изоморфно над $\bar{k}$ алгебраической группе G, определенной единственным образом. Применяя к G спуск основного поля, получаем, что G можно определить над k, что доказывает лемму 8 в случае совершенного поля.

23. Случай произвольного поля

Так как для дальнейшего нам будет достаточно случая совершенного основного поля, мы ограничимся краткими замечаниями.

Пусть k — произвольное поле и k_s — его сепарабельное замыкание (т. е. композит всех сепарабельных алгебраических расширений поля k). Пусть X — кривая, определенная над k, и $\mathfrak{m}$—рациональный модуль над k. Начнем с построения якобиевого многообразия $J_{\mathfrak{m}}$ *над полем* k_s, повторяя построение, данное в § 1 для случая алгебраически замкнутого поля. Это построение основывается лишь на возможности выбрать вне S точку P_0, рациональную над $\bar{k}$. Эта возможность реализуется и над k_s в силу следующей леммы.

Лемма 27. *Всякое алгебраическое многообразие* Y, *определенное над* k_s, *обладает рациональной точкой над* k_s.

(Применяя этот результат к открытым аффинным множествам в Y, мы видим, что эти точки *плотны* в Y.)

Наметим доказательство этого хорошо известного результата. Пусть K — поле рациональных функций на Y над k_s. Достаточно показать, что для модели Y' поля K множество рациональных над k_s точек Y' плотно в Y'. Пусть $f_1, \ldots, f_n$ — сепарирующий базис трансцендентности K над k_s и g — образующая поля $K/k_s(f_1, \ldots, f_n)$. Функция g удовлетворяет алгебраическому уравнению

$$a_0 g^m + \ldots + a_m = 0, \quad a_i \in k_s(f_1, \ldots, f_n),$$

производная которого не обращается тождественно в нуль (по определению сепарирующего базиса тренсцендентности). Если в качестве модели Y' поля K взять подмногообразие аффинного пространства размерности $n+1$, определенного предыдущим уравнением, то любая точка Y', у которой первые n координат принадлежат k_s и не обращают в нуль ни производную уравнения, ни a_0, принадлежит k_s. Так как множество этих точек, очевидно, плотно в Y', это доказывает лемму.

Если якобиевы многообразия определены над k_s, то спуск основного поля k_s до k проводится точно так же, как в предыдущем пункте. Таким образом, можно доказать предложение 13 для произвольного поля.

Библиографические замечания

Теория обыкновенных якобиевых многообразий имеет истоки в теоремах Абеля и Якоби; с этой точки зрения можно сказать, что „обобщенная проблема Якоби" (см. Клебш и Гордон [1], § 43, а также Крацер и Виртингер [1], § 13) лежит в основе теории обобщенных якобиевых многообразий. Последние явно появляются впервые у Севери ([3], гл. II) в случае обыкновенных особенностей (разумеется, основное поле есть поле комплексных чисел C). Севери изучает их аналитическую и алгебраическую структуры (иногда не отделяя одну от другой) и замечает, что эти многообразия бирационально изоморфны произведению обыкновенных якобиевых многообразий и линейных многообразий. Розенлихт в работе [2] рассматривает более общую ситуацию (более общими являются как особенности, так и основное поле); большая часть результатов этой главы принадлежит ему.

Метод, примененный Чжоу [1] для построения обыкновенных якобиевых многообразий, можно использовать также для обобщенных якобиевых многообразий, см. Игуза [2]. В работе Игузы обобщенные якобиевы многообразия появляются как „пределы" обыкновенных якобиевых многообразий, так же как у Кодаиры [1] вырожденные слои в аналитических расслоениях.

Структура группы обратимых элементов в $k[[T]]$ выяснена Артином — Хассе, Уэплсом, Дьёдонне и др. Библиографию можно найти в заметке Дьёдонне [3].

Теорема о спуске основного поля явно используется во многих работах Шателе (см., например, Барсотти [2]), но без достаточного обоснования. Она уточнена и доказана Вейлем [11].

ГЛАВА

VI

ПОЛЯ КЛАССОВ

§ 1. *Отображение* $x \to x^q - x$

1. Алгебраические многообразия над конечным полем

Пусть k — конечное поле из $q = p^n$ элементов, а V — алгебраическое многообразие, определенное над k (т. е. k-*многообразие*). Пусть многообразие V определено с помощью карт U^i (изоморфных афинным k-многообразиям) и функций перехода u_{ij} (с коэффициентами в поле k). Если $x = (x_1, \ldots, x_r)$ — точка афинного пространства, то мы обозначаем через Fx, или x^q, точку с координатами $(x_1^q, \ldots, x_r^q)$. Отображение $x \to Fx$ коммутирует с полиномиальными отображениями, в частности оно отображает каждое множество U_i в себя и коммутирует с функциями u_{ij}. После склеивания карт U_i это отображение действует и на многообразии V Мы будем обозначать его действие на точку x также через Fx или x^q.

Можно дать и другую интерпретацию отображения F. Пусть V — алгебраическое многообразие, определенное над алгебраически замкнутым полем K (например, над алгебраическим замыканием $\bar{k}$ поля k или даже над универсальной областью Ω). Автоморфизм $x \to x^p$ поля K преобразует V в многообразие, которое мы будем обозначать через V^p (если это не может привести к смешению его с произведением p многообразий V), и определяет каноническое отображение $\theta: V \to V^p$. Это отображение биективно, взаимно непрерывно и отождествляет регулярные функции на многообразии V^p с p-ми степенями регулярных функций на V (с точки зрения пучков это особенно простое описание многообразия V^p). Можно сказать, что отображение $\theta: V \to V^p$ является максимальным радикальным накрытием высоты 1 (в таком виде мы уже встречались с ним несколько раз, см. гл. III, п. 8 и 14).

Повторяя эту конструкцию n раз, мы получаем отображение $\theta^n\colon V \to V^q$, которое радикально и имеет степень $q^{\dim V}$. Если многообразие V определено над полем k, то многообразия V и V^q канонически изоморфны и, беря композицию этого изоморфизма θ^n, получаем определенное выше отображение F.

Предложение 1. *Структура k-многообразия V однозначно определяется его структурой многообразия над Ω и отображением F.*

Действительно, как легко видеть, рациональные функции, определенные над полем k, характеризуются условием

$$f \circ F = f^q.$$

[Несмотря на свою тривиальность, это предложение будет играть важную роль в дальнейшем. Это объясняется тем, что изучение многообразий над конечными полями часто можно свести к изучению их над алгебраическими замыканиями основного поля.]

Если W — подмногообразие V, определенное над расширением K/k, то его образ FW при отображении F тоже есть подмногообразие многообразия V. Для рациональности W над полем k необходимо и достаточно, чтобы $FW = W$; то же самое относится и к произвольному *циклу*. В частности, множество V_k рациональных точек над k многообразия V является множеством *неподвижных точек* отображения F.

Если V и V' — два многообразия над полем k, а φ — рациональное отображение с графиком W, то существует единственное рациональное отображение, обозначаемое через φ^F, график которого есть FW. Отображение φ^F можно также характеризовать формулой

$$\varphi^E \circ F = F \circ \varphi.$$

Имеем $(\varphi \circ F = F \circ \varphi) \Longleftrightarrow (\varphi^F = \varphi) \Longleftrightarrow (\varphi$ определено над $k)$. Все эти свойства немедленно проверяются с помощью того или иного из определений отображения F, данных выше.

2. Расширение и спуск основного поля

При тех же обозначениях, что и в предыдущем пункте, пусть k_1/k — конечное расширение поля k степени m. Поле k имеет q^m элементов и определяет отображение $F_1\colon V \to V$. Ясно, что $F_1 = F^m$.

Наоборот, пусть задано многообразие V, определенное над полем k_1, и отображение $F: V \to V$ многообразия V в себя, такое, что $F^m = F_1$. Найдем условие, при котором можно произвести *спуск* поля определения многообразия V до поля k (в смысле гл. V, п. 20) так, чтобы F совпадало с соответствующим отображением $x \to x^q$. Для простоты предположим, что выполняются условия следствия 1 предложения 12 из гл. V (все конечные подмножества многообразия V, алгебраические над полем k_1, содержатся в открытом аффинном подмножестве многообразия W, алгебраическом над k_1).

Предложение 2. *При предыдущих предположениях для возможности спуска необходимо и достаточно, чтобы $F = \varphi \circ \theta$, где $\theta: V \to V^q$ — каноническое отображение многообразия V на V^q, а φ — бирегулярный изоморфизм многообразия V^q на V.*

Необходимость очевидна. Для доказательства достаточности применим результаты из гл. V (п. 20). Группа Галуа $\mathfrak{g}$ расширения k_1/k является циклической группой порядка m и порождается автоморфизмом $\sigma: \lambda \to \lambda^q$. Спуск поля k_1 определяется изоморфизмами $h_\alpha: V \to V^\alpha$, $\alpha \in \mathfrak{g}$, удовлетворяющими условию коциклов

$$h_{\alpha\beta} = h_\alpha^\beta \circ h_\beta \text{ (см. гл. V, п. 20).} \qquad (^{**})$$

Вследствие цикличности группы $\mathfrak{g}$ система изоморфизмов h_α определяется изоморфизмом $h = (h_\sigma)^{-1}$, а условие $(^{**})$ переписывается в виде

$$h \circ h^\sigma \circ \ldots \circ h^{\sigma^{m-1}} = 1 \text{ (многообразия } V \text{ и } V^{\sigma^m} = V^{q^m} \text{ отождествляются).} \qquad (^{**\prime})$$

Возьмем теперь в качестве h отображение φ, такое, что $F = \varphi \circ \theta$. Соотношение $F^m = F_1$ показывает, что отображение F коммутирует с отображением F_1, а следовательно, оно определено над полем k_1. То же самое относится и к отображению $h = \varphi$. Остается проверить условие $(^{**\prime})$. Для этого заметим сначала, что для всех отображений ρ имеем $\rho^\sigma \circ \theta = \theta \circ \rho$. Воспользовавшись этой формулой, а также определением отображения h, получаем

$$\left(h \circ h^\sigma \circ \ldots \circ h^{\sigma^{m-1}}\right) \circ \theta^m = F^m = F_1.$$

Вместе с равенством $\theta^m = F_1$ (если учесть отождествление $V = V^{q^m}$) это доказывает (**′). Таким образом, на многообразии V получаем структуру k-многообразия. Кроме того, из построения видно, что отображение F соответствует заданному отображению.

3. Торы над конечным полем

В качестве примера покажем, как можно применить предложение 2 к классификации *торов над конечным полем* k (именно эти группы встречаются в локальной части обобщенных якобиевых многообразий кривой, определенной над полем k).

Итак, пусть V — тор размерности r, другими словами — группа $(G_m)^r$. Наша задача произвести спуск его основного поля k_1 до поля k так, чтобы получить над этим полем *алгебраическую группу*. Эта задача сводится к рассмотрению операций F, которые являются эндоморфизмами группы $(G_m)^r$. Так как каждому такому эндоморфизму соответствует квадратная матрица порядка r с коэффициентами в $\mathbf{Z}$, то после отождествления F с соответствующей матрицей условие факторизации в предложении 2 выражается соотношением $F = q \cdot \Phi$, где Φ — обратимая матрица [т. е. элемент группы $GL(r, \mathbf{Z})$]. Условие $F^m = F_1$ выражается соотношением $\Phi^m = 1$. Таким образом, k-группам, изоморфным над $\bar{k}$ группе $(G_m)^r$, соответствуют *элементы конечного порядка* группы $GL(r, \mathbf{Z})$. Две такие группы k-изоморфны тогда и только тогда, когда соответствующие матрицы сопряжены в группе $GL(r, \mathbf{Z})$ Следовательно, мы получаем биективное соответствие между классами таких групп и классами целочисленных представлений степени r конечной циклической группы. В случае, когда порядок последней группы есть простое число l, эти представления полностью определяются группой классов идеалов циклического поля $Q\left(\sqrt[l]{1}\right)$ (см. Рейнер [1]).

Приведем, следуя Тейту, одно определение, тесно связанное с представлением k-группы G описанного типа; для этого рассматривается дискретная группа рациональных *характеров* группы G, определенных над $\bar{k}$ (семинар Шевалле [3], сообщение 4), и на $X(G)$ определяется действие группы Галуа расширения $\bar{k}/k$.

Знание матрицы Φ, соответствующей группе G, позволяет рассматривать различные вопросы относительно G. Например, число рациональных точек группы G над расширением k_n степени n поля k равно

$$\nu_n(G) = \det\left(q^n - \Phi^n\right) = \sum_{h=0}^{r}(-1)^h q^{n(r-h)} \sum_{i_1<\cdots<i_h} \left(\lambda_{i_1} \ldots \lambda_{i_h}\right)^n,$$

где $\lambda_1, \ldots, \lambda_r$ — собственные значения Φ (являющиеся корнями из единицы). Исходя отсюда, можно вычислить *дзета-функцию* многообразия G:

$$\zeta_G(s, k) = \prod_{h=0}^{r} \prod_{i_1<\cdots<i_h} \left(1 - \lambda_{i_1} \ldots \lambda_{i_h} q^{r-h} t\right)^{(-1)^{h+1}},$$

где, как обычно, $t = q^{-s}$. Если обозначить через Φ_h h-ю внешнюю степень матрицы Φ, то эта формула записывается проще

$$\zeta_G(s, k) = \prod_{h=0}^{r} \det\left(1 - q^{r-h} t \Phi_h\right)^{(-1)^{h+1}}. \qquad (1)$$

Сомножители $\det\left(1 - q^{r-h} t\Phi_n\right)$ аналогичны сомножителям, встречающимся в неабелевых L-функциях Артина. Более точно:

Пусть L — конечное расширение Галуа числового поля K с группой Галуа $\mathfrak{g}$. Пусть далее M — гомоморфизм группы $\mathfrak{g}$ в $GL(r, \mathbf{Z})$. Представление M определяет спуск основного поля L тора $(G_m)^r$ до поля K, причем мы получаем алгебраическую группу G, определенную над полем K. Если $\mathfrak{p}$ — простой дивизор поля K, то редукция по модулю $\mathfrak{p}$ группы G определяет группу $G_{\mathfrak{p}}$ предыдущего типа (это справедливо для почти всех $\mathfrak{p}$). Матрица Φ, соответствующая группе $G_{\mathfrak{p}}$, совпадает с матрицей $M(\sigma_{\mathfrak{p}})$, где $\sigma_{\mathfrak{p}} \in \mathfrak{g}$ обозначает гомоморфизм Фробениуса $(\mathfrak{p}, L/K)$, соответствующий дивизору $\mathfrak{p}$ (этот гомоморфизм определен с точностью до внутреннего автоморфизма). Положим

$$\zeta_G(s) = \prod_{\mathfrak{p}} \zeta_{G_{\mathfrak{p}}}(s)$$

(где произведение определено с точностью до конечного числа сомножителей). Это выражение есть *дзета-функция группы G в смысле Хассе — Вейля.* Формула (1) дает явное выражение этой функции

$$\zeta_G(s) = \prod_{h=0}^{r} L_h(s - r + h)^{(-1)^h} \text{ (с точностью до элементарного множителя)}, \quad (2)$$

где L_h обозначает L-функцию Артина, соответствующую представлению группы $\mathfrak{g}$ с помощью h-й внешней степени представления M. Заметим, что эта функция лишь рационально зависит от представления M, другими словами, она не изменится при замене группы G на изогенную ей группу.

Формула (2) дает типичный пример поведения дзета-функции при спуске основного поля. Другие примеры (эллиптические кривые или абелевы многообразия с комплексным умножением, кубические поверхности) см. у Дейринга [1], Шимуры и Таниямы [1], Вейля [8].

4. Отображение $x \to x^{-1}Fx$

Пусть k — конечное поле из q элементов, а G — алгебраическая группа над этим полем. Чтобы избежать смешения x^q с q-й степенью элемента x в группе G, будем все время использовать обозначение Fx.

Предложение 3. *Если группа G связна, то отображение $x \to x^{-1}Fx$ сюръективно.*

Более общо для $y \in G$ рассмотрим эндоморфизм u_y группы G, определяемый равенством

$$u_y(x) = x^{-1}yFx.$$

Поскольку отображение $F: G \to G$ разлагается в композицию $G \to G^q \to G$, его дифференциал тождественно равен нулю. Поэтому $d(u_y) = d(x^{-1})\, yFx$, и, следовательно, отображение, касательное к u_y, *всюду сюръективно.* Тем более отображение u_y почти всюду сюръективно, и $u_y(G)$ содержит открытое непустое множество $\mathfrak{u}_y$. Если теперь z — какая-нибудь точка группы G, то предположение о связности G дает $\mathfrak{u}_z \cap \mathfrak{u}_e \neq \phi$.

Пусть $t \in u_z \cap u_e$. Имеем $t = x^{-1}zFx$ и $t = y^{-1}Fy$, где $x, y \in G$. Положив $u = yx^{-1}$, получаем

$$z = u^{-1}Fu,$$

что и доказывает предложение.

Следствие 1. *Всякое однородное пространство относительно группы G, определенное над полем k, имеет над этим полем рациональную точку.*

Пусть H — однородное пространство и $h \in H$. Поскольку H однородно, существует элемент $g \in G$, такой, что $h = gFh$. Согласно предложению 3, существует $x \in G$, такой, что $g = x\ Fx$, откуда $x \cdot h = Fx \cdot Fh$. Так как отображение $G \times H \to H$ определено над k, имеем $Fx \cdot Fh = F(x \cdot h)$. Равенство $x \cdot h = F(x \cdot h)$ показывает тогда, что точка $x \cdot h$ пространства H рациональна над k.

Примеры. Всякое многообразие Севери — Брауэра (Шателе [1]) над конечным полем тривиально. Всякая линейная алгебраическая группа, определенная над полем k, содержит подгруппу Бореля, также определенную над k (так как множество таких подгрупп естественным образом снабжается структурой однородного пространства).

Следствие 2. *Пусть $0 \to G \xrightarrow{u} G' \xrightarrow{v} G'' \to 0$ — точная последовательность линейных алгебраических групп, определенных (как и гомоморфизмы u и v) над конечным полем k. Тогда последовательность*

$$0 \to G_k \to G'_k \to G''_k \to 0$$

точна.

(Напомним, что если V — многообразие над полем k, то через V_k обозначается множество точек V, рациональных над полем k.)

Единственный нетривиальный факт здесь — это то, что группа G'_k отображается *на* группу G''_k. Пусть $x'' \in G''_k$ и H — его прообраз в группе G'. Множество H является смежным классом по модулю G, а следовательно, *однородным пространством* относительно группы G. Равенство $Fx'' = x''$ показывает, что $FH = H$, т. е. что H определено над k. Из следствия 1 получаем поэтому, что H содержит рациональную точку x над полем k, откуда и следует нужный нам результат.

[Разумеется, условие связности группы G существенно. Мы увидим дальше, что происходит, когда группа G конечна.]

5. Квадратичные формы над конечным полем

Покажем, каким образом предложение 3, примененное к унимодулярным ортогональным группам, заново дает классификацию квадратичных форм над конечным полем.

Пусть V — векторное пространство конечной размерности n над полем k, а Q — квадратичная форма на V. Предположим сначала, что характеристика p поля k не равна 2. В этом случае дискриминант Δ формы Q является элементом группы k^*/k^{*2}, которую можно отождествить с помощью отображения $\lambda \to \lambda^{(q-1)/2}$ с группой $\{+1, -1\}$.

Предложение 4. *Для того чтобы две квадратичные формы были эквивалентны, необходимо и достаточно, чтобы они имели одинаковый дискриминант.*

(Тем самым получается полная классификация квадратичных форм над k: каждая такая форма эквивалентна форме вида $x_1^2 + x_2^2 + \ldots + x_{n-1}^2 + gx_k^2$, где g — квадрат или нет.)

Предположим сначала, что дискриминант Δ равен 1, и покажем, что Q эквивалентна форме $x_1^2 + \ldots + x_n^2$ в векторном пространстве $E = k^n$. Эта эквивалентность, во всяком случае, имеет место над алгебраическим замыканием $\bar{k}$ поля k в силу элементарной теоремы о квадратичных формах. Пусть $u\colon E \to V$ — изоморфизм пространства E на V, определенный над $\bar{k}$. Если в пространстве V выбрать ортогональный базис e_i, то сразу же получим, что $\det(u)^2 = \Delta$. Рассмотрим линейное отображение $v = u^{-1}Fu$. Имеем

$$\det(v) = \Delta^{-1/2}\Delta^{q/2} = \Delta^{(q-1)/2} = +1.$$

Кроме того, ясно, что $v \in \mathbf{O}(E)$ — ортогональной группе пространства E. Так как унимодулярная ортогональная группа $\mathbf{O}_+(E)$ *связна*, то применимо предложение 3, которое показывает, что элемент v можно записать в виде $v = w^{-1}Fw$, где $w \in \mathbf{O}_+(E)$. Положив $u' = u \cdot w^{-1}$, получим изоморфизм пространства E на V. Этот изоморфизм инвариантен относительно отображения F, а следовательно, определен над полем k, что доказывает теорему для этого случая.

Если дискриминант Δ не является квадратом, подобное рассуждение проводится точно так же, с заменой формы $x_1^2 + \ldots + x_n^2$ на форму $x_1^2 + \ldots + gx_n^2$, где g – не квадрат.

[Вместо предложения 3 можно было бы использовать следствие 1, замечая, что квадратичные формы на пространстве V с заданным дискриминантом естественным образом образуют однородное пространство относительно группы $\mathbf{0}_+(E)$.]

В случае когда характеристика равна 2, надо различать случаи четного и нечетного n. В первом случае группа $\mathbf{0}(E)$ содержит связную подгруппу $\mathbf{0}_+(E)$ индекса 2 и имеются два типа квадратичных форм, характеризуемых *Арф-инвариантом.* Во втором случае группа $\mathbf{0}(E)$ связна и существует один-единственный тип квадратичных форм (подробности см. у Дьедонне [1], гл. 1, § 16, и гл. 2, § 10).

6. Изогения $x \to x^q - x$; коммутативный случай

Предположим теперь, что группа G коммутативна и закон композиции записывается аддитивно. В этом случае запись x^q вместо Fx не приведет к недоразумениям.

Предложение 5. *Пусть k_1 — конечное расширение поля k с группой Галуа $\mathfrak{g}$. Если G — коммутативная связная алгебраическая группа над полем k, то*

$$H^m(\mathfrak{g}, G_{k_1}) = 0 \quad \textit{для всех} \quad m \geqslant 1.$$

(Речь идет о когомологиях конечной группы $\mathfrak{g}$, действующей очевидным образом на рациональные над полем k_1 точки группы G.)

Так как $\mathfrak{g}$ циклична, группы $H^m(\mathfrak{g}, G_{k_1})$ зависят лишь от четности числа m. Пусть $m = 1$. Надо доказать, что всякий элемент, след которого равен нулю, можно представить в виде $x - x^\sigma$. Итак, пусть $g \in G_{k_1}$ и

$$g + g^q + \ldots + g^{q^{n-1}} = 0, \quad \text{где} \quad n = [k_1 : k].$$

Согласно предложению 3, элемент g можно записать в виде $g = x^q - x$, где $x \in G$. Предыдущая формула показывает тогда, что

$$\left(x^{q^n} - x^{q^{n-1}}\right) + \ldots + \left(x^q - x\right) = 0,$$

откуда $x^{q^n} = x$. Это показывает, что $x \in G_{k_1}$, и доказывает тривиальность группы $H^1(\mathfrak{g}, G_{k_1})$. Так как группа G_{k_1} конечна, то *лемма Хербранда* (Шевалле [2], § 10) показывает, что группа $H^2(\mathfrak{g}, G_{k_1})$ имеет тот же порядок, что и $H^1(\mathfrak{g}, G_{k_1})$. Предложение доказано.

Следствие. *Всякий элемент группы G_k является следом элемента группы G_{k_1}.*

Это следует из того, что $H^2(\mathfrak{g}, G_{k_1}) = 0$.

[*Непосредственное доказательство*: пусть $\varphi(x) = x + x^q + \ldots + x^{q^{n-1}}$. Дифференциал гомоморфизма φ равен дифференциалу x, откуда следует, что отображение φ сюръективно. Для $y \in G_k$ выберем элемент $x \in G$, такой, что $\varphi(x) = y$. Равенство $y^q = y$ показывает, что $x \in G_{k_1}$.]

Вернемся к отображению $\wp(x) = x^q - x$. Доказательство предложения 3 [основанное на вычислении дифференциала отображения $\wp(x)$] показывает, что отображение $\wp$ сепарабельно. Кроме того, поскольку G коммутативна, оно является гомоморфизмом группы G в себя. Ядро этого гомоморфизма состоит из элементов $x \in G$, для которых $x^q = x$. Оно совпадает, следовательно, с группой G_k. Поэтому имеет место точная последовательность

$$0 \to G_k \to G \xrightarrow{\wp} G \to 0.$$

Эта последовательность показывает, что группа G определяет свое собственное *накрытие*, которое, очевидно, абелево (над k), причем группа Галуа изоморфна группе переносов $x \to x + a$, $a \in G_k$. Мы увидим, что это накрытие является *максимальным* из всех накрытий, обладающих этими свойствами (что сближает его с „абсолютным полем классов" Гильберта; более точное сопоставление будет проведено в § 4, 5, 6).

Предложение 6. *Пусть θ: $G' \to G$ сепарабельная изогения над полем k. Тогда следующие четыре условия эквивалентны:*

1) *расширение* $k(G')/k(G)$, *определяемое изогенией* θ, *является расширением Галуа*;

2) *это расширение абелево*;

3) *ядро изогении* θ *содержится в группе* G'_k;

4) *изогения* θ *является факторизогенией изогении* $\wp\colon G \to G$.

При выполнении этих условий группа Галуа расширения $k(G')/k(G)$ *изоморфна группе переносов* $x \to x + a$, *где* a *принадлежит ядру отображения* θ.

Из 2) тривиально следует 1). Далее, 1) $\Rightarrow$ 3), так как элементы группы Галуа преобразуют каждую рациональную точку в рациональную, а поэтому элементы из $\theta^{-1}(0)$, получающиеся из нуля, рациональны. Наконец, 3) $\Rightarrow$ 1), так как переносы $x \to x + a$, $a \in \theta^{-1}(0)$, определены над полем k и являются $k(G)$-автоморфизмами поля $k(G')$, причем число их равно степени расширения. Таким образом, утверждения 1), 2), 3) эквивалентны.

Имеем 4) $\Rightarrow$ 2), так как всякое подполе абелевого расширения абелево. Обратно, пусть справедливо 3) и $\wp'\colon G' \to G'$ — изогения $x \to x^q - x$ в G'. Так как отображение θ определено над k, имеет место коммутативная диаграмма

$$\begin{tikzcd} G' \arrow[r, "\wp'"] \arrow[d, "\theta"] & G' \arrow[d, "\theta"] \\ G \arrow[r, "\wp"] & G \end{tikzcd}$$

Поскольку ядро отображения θ содержится в ядре отображения $\wp'$, а именно в группе G'_k, отображение $\wp'$ определяет при переходе к фактору гомоморфизм $\alpha\colon G \to G'$, и, таким образом, отображение $\wp\colon G \to G$ разлагается в $G \xrightarrow{\alpha} G' \xrightarrow{\theta} G$.

Замечание. В случае когда группа G не предполагается коммутативной, отображение

$$\wp(x) = x^{-1}Fx$$

не является в общем случае гомоморфизмом. Но, во всяком случае, $\wp(x) = \wp(y)$ тогда и только тогда, когда $x \equiv y \pmod{G_k}$, а поэтому отображение $\wp$ определяет изоморфизм *однородного* *пространства G/G_k на группу G.* В частности, отображение $\wp$: $G \to G$ определяет *неразветвленное накрытие Галуа*, которое обладает свойствами, очень близкими к свойствам изогении.

§ 2. Накрытия и изогении

7. Определения, относящиеся к накрытиям

Пусть k — поле, $\bar{k}$ — его алгебраическое замыкание и V — неприводимое, нормальное алгебраическое многообразие, определенное над $\bar{k}$. Обозначим через $K = \bar{k}(V)$ поле рациональных функций на V. Известно, что понятие *накрытия* многообразия V имеет *бирациональный* характер, другими словами, зависит только от поля K. Более точно, пусть L/K — конечное сепарабельное расширение поля K (мы ограничиваемся сепарабельными расширениями, намереваясь в дальнейшем более подробно изучить случай *абелевого* расширения). *Нормальная модель* W многообразия V в поле L определяется как многообразие, локальные кольца которого получаются при локализации целых замыканий в поле L локальных колец O_P точек $P \in V$. Можно определить также и *приводимые накрытия*, взяв вместо поля L произведение $\prod L_i$ сепарабельных расширений L_i поля K (другими словами, *сепарабельную коммутативную алгебру* над полем K).

Так определяемое многообразие W снабжается проекцией π: $W \to V$. Мы будем говорить, что π: $W \to V$ — *накрытие многообразия V, соответствующее расширению L/K*. На W переносится вся терминология для расширений полей: W — накрытие Галуа, абелево, степени n и т. д., если это относится к расширению L/K.

Если поле рациональных функций многообразия W является расширением Галуа поля функций многообразия V с группой Галуа $\mathfrak{g}$, то элементы $\sigma \in \mathfrak{g}$ определяют автоморфизмы W, а многообразие V отождествляется с фактор-многообразием $W/\mathfrak{g}$ (см. гл. 3, п. 12). Наоборот, если $\mathfrak{g}$ — группа автоморфизмов нормального многообразия, то проекция $W \to W/\mathfrak{g}$ превращает W в накрытие Галуа многообразия $W/\mathfrak{g}$ с группой Галуа $\mathfrak{g}$.

Говорят, что точка $P \in V$ *неразветвлена* в W, если она является образом при π ровно n точек многообразия W (где $n = \deg W$). В случае когда каждая точка многообразия неразветвлена, говорят, что накрытие *всюду неразветвлено*. Если накрытие является накрытием Галуа с группой $\mathfrak{g}$, то это эквивалентно тому, что элементы группы $\mathfrak{g}$, отличные от единицы, действуют на W без неподвижных точек.

Пусть теперь V' — другое нормальное многообразие и f: $V' \to V$ — рациональное отображение, такое, что $f(V')$ не содержится в множестве точек разветвления многообразия V. Если выбросить эти точки, а также их прообразы при отображении f и те точки, в которых отображение f нерегулярно, то можно считать, что $W \to V$ всюду неразветвлено, а отображение f всюду регулярно. Определим многообразие W' как множество пар (v', w) в произведении, таких, что $W \times V'$. Немедленно проверяется, что каноническая проекция π': $W' \to V'$ превращает многообразие W' в неразветвленное накрытие V' той же степени, что и накрытие π: $W \to V$. Это будет накрытие Галуа, если W — таковое накрытие, с той же группой Галуа. Назовем это многообразие (как обычно в топологии) *прообразом* накрытия π при отображении f и обозначим его через $f^*(W)$. Разумеется, это накрытие не обязано быть неприводимым; в общем случае оно распадается на неприводимые компоненты, которые сопряжены друг другу, если W — накрытие Галуа. В частном случае, когда V' — подмногообразие V, а f — каноническое вложение, накрытие W' совпадает с $\pi^{-1}(V')$.

Все предыдущее относилось к алгебраически замкнутому полю $\bar{k}$. Если многообразия W и V снабжены структурой k-многообразий, а отображение π определено над полем k, то говорят, что накрытие определено над k. Этому накрытию соответствует расширение $k(W)/k(V)$. Заметим, что накрытие $W \to V$ может быть расширением Галуа над $\bar{k}$, не являясь таковым над полем k (см. предложение 6).

8. Построение накрытий как прообразов изогений

Пусть G — алгебраическая группа, N — ее конечная подгруппа, а $G/N = H$ факторгруппа являющаяся однородным пространством (мы не предполагаем, что группа G обязательно коммутативна). Каноническое отображение $\pi: G \to H$ превращает G в неразветвленное накрытие группы H, являющееся накрытием Галуа с группой Галуа N. Если группа G определена над полем k и каждая точка $n \in N$ рациональна над k, то это накрытие также определено над k и является над ним накрытием Галуа. В частном случае, когда группа G коммутативна, накрытие π является *изогенией* (см. п. 5).

Построим для каждой конечной группы N группу $G(N)$, содержащую N, определенную над простым полем $\mathbf{F}_p$ и обладающую свойством *универсальности* для всех накрытий Галуа с группой Галуа N. Точнее говоря, пусть $A(N)$ — *групповая алгебра* группы N (для простоты над универсальной областью), а $G(N)$ — множество обратимых элементов алгебры $A(N)$. Множество $G(N)$ является открытым подмножеством аффинного пространства $A(N)$ [так как состоит из таких систем $\{a_s\}_{s \in N}$, для которых $\det(a_{st}) \neq 0$], определенным над простым полем $\mathbf{F}_p$. Более того, оно является, очевидно, неприводимой алгебраической группой, содержащей группу N. Имеем

Предложение 7. *Если $\pi: W \to V$ — накрытие Галуа с группой Галуа N, то существует отображение $f: V \to G(N)/N$, такое, что многообразие W изоморфно накрытию $f^*(G(N))$. Если, кроме того, накрытие W определено над полем k и является накрытием Галуа над этим полем, то отображение f и изоморфизм $W \to f^*(G(N))$ можно определить над полем k.*

Рассматриваемое утверждение — чисто бирациональное. Пусть K — поле функций многообразия V, L — поле (или алгебра, если W приводимо) функций на W. Для того чтобы построить отображение f и изоморфизм $W \to f^*(G)$, требуется найти пару отображений $g: W \to G(N)$ и $f: V \to G(N)/N$, таких, что диаграмма

$$\begin{array}{ccc} W & \xrightarrow{g} & G(N) \\ \downarrow & & \downarrow \\ V & \xrightarrow{f} & G(N)/N \end{array}$$

коммутативна и отображение g коммутирует с операциями N. Это последнее условие, с учетом структуры группы $G(N)$, показывает, что отображение g имеет вид $x \to (\varphi^s(x))$, где φ — рациональная функция на многообразии W. Единственное условие, налагаемое на функцию φ, состоит в том, чтобы g отображало многообразие W в $G(N)$ [а не только в $A(N)$], т. е. чтобы $\det(\varphi^{st}(x))$ не был тождественно равен нулю. Существование такой функции следует из *теоремы о нормальном базисе*, примененной к расширению Галуа L/K (немедленно проверяется, что эта теорема распространяется на *алгебры Галуа* над полем). Что касается отображения f, то оно получается из g переходом к фактору.

В случае когда накрытие определено и является накрытием Галуа над полем k, аналогичное рассуждение применимо к расширению $k(W)/k(V)$.

Следствие. *Всякое абелево накрытие есть прообраз изогении.*

Этот результат был уже приведен в гл. 1 (теорема 4).

9. Частный случай

Группа $G(N)$ — частный случай групп, определенных как множества необратимых элементов конечномерной алгебры (это так называемые *„билинейные группы“* Эли Картана). Если радикал алгебры равен нулю и основное поле алгебраически замкнуто, то эти группы изоморфны произведениям линейных групп GL_n. Кроме этого случая, пока еще мало что известно. Мы ограничимся рассмотрением лишь двух частных случаев (достаточных, однако, для последующих приложений):

1) *N — циклическая группа порядка n, взаимно простого с характеристикой p.*

Алгебра $A(N)$ изоморфна $k[T]/(1-T^n)$. Если поле k содержит первообразный корень n-й степени из единицы, который мы обозначим через ε, то многочлен $1-T^n$ можно разложить на линейные множители. В этом случае группа $G(N)$ *изоморфна произведению групп G_m*. Таким образом, для произвольного поля группа $G(N)$ получается из тора $(G_m)^n$ с помощью спуска основного поля.

Если $\varepsilon \in k$, то одна из проекций $G(N) \to G_m$ задается отображением $T \to \varepsilon$. Если обозначить через θ изогению

$G_m \to G_m$, определенную равенством $\theta(\lambda) = \lambda^n$, то получим коммутативную диаграмму

$$\begin{tikzcd} G(N) \arrow[r] \arrow[d] & G_m \arrow[d, "\theta"] \\ G(N)/N \arrow[r] & G_m \end{tikzcd}$$

которая показывает, что изогения $G(N) \to G(N)/N$ является прообразом изогении θ: $G_m \to G_m$. Отсюда следует, что предложение 7 справедливо, если заменить отображение $G(N) \to G(N)/N$ на изогению θ. Это есть не что иное, как *теория Куммера.*

В случае когда не предполагается, что поле k содержит ε, теория Куммера уже неприменима. Однако иногда удается все же уменьшить размерность группы $G(N)$. Например, при $n = 3$ в качестве фактора группы $G(N)$ можно взять ортогональную группу G квадратичной формы $x^2 - xy + y^2$. Легко видеть, что эта группа содержит циклическую подгруппу N порядка 3, образованную рациональными над простым полем точками, а изогения $G \to G/N$ удовлетворяет свойству универсальности из предложения 7. С точки зрения теории полей дело сводится к следующему легко проверяемому непосредственно результату.

Если характеристика отлична от 3, *то каждое циклическое расширение степени* 3 *порождается элементом* g, *сопряженные к которому равны* $1/(1 - g)$ *и* $1 - 1/g$.

2) N — *циклическая группа порядка* p^n.

Имеем $A(N) = k[T]/(1 - T^{p^n})$. Заменяя T на $1 - T$, мы видим, что $A(N)$ изоморфна *алгебре* $k(T)/(T^{p^n})$ *формальных рядов по модулю* T^{p^n}. По следствию предложения 9 из гл. V группа $G(N)$ изоморфна в этом случае произведению группы G_m на группы Витта W_{n_i}. Все $n_i < n$, кроме одного, который равен n. Проектируя группу $G(N)$ на соответствующую группу W_n, получаем, как и выше, что в предложении 7 изогению $G(N) \to G(N)/N$ можно заменить изогенией $\wp$: $W_n \to W_n$, т. е. получаем *теорию Витта — Артина — Шрейера* (Витт [1]). Заметим, что в отличие от теории Куммера на поле k никаких предположений не налагается.

10. Случай неразветвленного накрытия

Вернемся к ситуации предложения 7. Пусть f — искомое отображение многообразия V в группу $G(N)/N$. Если отображение f регулярно в точке $P \in V$, то накрытие $f^*(G(N))$ не разветвлено в этой точке. Отсюда следует, что изоморфное ему накрытие $W \to V$ не разветвлено в точке P. Справедливо и обратное утверждение.

Предложение 8. *Если накрытие W не разветвлено в точке P многообразия V, то в предложении 7 отображение f можно выбрать так, чтобы оно в этой точке было регулярно.*

[Если накрытие π: $W \to V$ определено над полем k и является накрытием Галуа над ним, то надо, кроме того, требовать, чтобы отображение f и изоморфизм $W \to f^*(G(N))$ были определены над полем k.]

С учетом построения отображения f, данного при доказательстве предложения 7, нам остается доказать, что можно выбрать нормальный базис φ^s расширения L/K так, чтобы функция φ была регулярной в точках $Q \in W$, проектирующихся в точку P. Пусть $\mathfrak{O}_P$ — локальное кольцо точки P в поле $k(V)$, $\mathfrak{m}_P$ — его максимальный идеал, а $\mathfrak{O}'_P$ — целое замыкание кольца $\mathfrak{O}'_P$ в поле $k(W)$, т. е. пересечение колец $\mathfrak{O}_Q$, где Q проектируется в точку P. Пусть $k(P) = \mathfrak{O}_P/\mathfrak{m}_P$ и $k'(P) = \mathfrak{O}'_P/\mathfrak{m}_P\mathfrak{O}'_P$. Так как точка P не является точкой ветвления, $k'(P)$ — алгебра Галуа над полем $k(P)$, степень n которой совпадает со степенью накрытия. Обозначим через $\{\lambda^s\}_{s \in N}$ нормальный базис этой алгебры. Выберем представителя φ элемента λ в кольце $\mathfrak{O}'_P$, и пусть $\Psi = \det(\varphi^{st})$. Образ элемента Ψ в поле $k'(P)$ равен $\det(\lambda^{st})$ и, следовательно, обратим в этом поле. Поэтому Ψ обратим в кольце $\mathfrak{O}'_P$, а элементы φ^s образуют нормальный базис, обладающий требуемыми свойствами.

Замечание. Предложение 8, примененное в случае циклического накрытия, показывает, что образующие Куммера или Витта — Артина — Шрейера могут быть выбраны регулярными в точке P (разумеется, если только точка P неразветвлена в W). Это хорошо известный факт (см., например, Серр [5], п. 15).

11. Случай кривых

Хотя это и не существенно, мы предположим в этом пункте, что основное поле k алгебраически замкнуто. Наиболее интересный случай, остающийся при этом в стороне, — случай конечного поля — будет рассмотрен подробно в § 6.

Пусть X — полная неприводимая неособая кривая, определенная над полем k, и K — поле рациональных функций на X. Если $Y \to X$ — абелево накрытие кривой X с группой Галуа N, то следствие предложения 7 показывает, что Y имеет вид $f^*(G)$, где $G \to H$ — сепарабельная изогения с ядром N, а f — рациональное отображение кривой X в группу H. Согласно результатам гл. 5, отображение 5 разлагается на $X \to J_m \to H$, где $J_m \to H$ — гомоморфизм обобщенного якобиева многообразия кривой X в группу H (вообще говоря, это верно только с точностью до переноса, но в случае алгебраически замкнутого поля перенос не меняет изогении). Прообраз изогении $G \to H$ при гомоморфизме $J_m \to H$ есть изогения $J' \to J_m$, а накрытие $Y \to Z$ — прообраз этой изогении. Таким образом, доказано

Предложение 9. *Всякое абелево накрытие кривой X является прообразом сепарабельной изогении ее обобщенного многообразия.*

Мы дополним этот результат, доказав, что рассматриваемая изогения *единственна*. Для этого удобно ввести группу $\mathrm{Ext}(J_m, N)$ *классов расширений* J_m *с помощью группы* N (см. определение этой группы в гл. VII, п. 1). Пусть изогения $J' \to J$ с ядром N представляется элементом j' этой группы. Используя аналогичную конструкцию, можно определить группу $\mathrm{Rev}(X, N)$ накрытий кривой X с группой Галуа N. Имеем $\mathrm{Rev}(X, N) = \mathrm{Hom}(G_k, N)$, где G_k — группа Галуа максимального сепарабельного расширения поля K. Операция $J' \to \varphi^*(J')$ определяет гомоморфизм φ^* группы $\mathrm{Ext}(J_m, N)$ в группу $\mathrm{Rev}(X, N)$, после чего нужная нам единственность выражается следующим образом:

Предложение 10. *Для любого модуля* $\mathfrak{m}$ *и произвольной конечной абелевой группы* N *гомоморфизм*

$$\varphi^*\colon \operatorname{Ext}(J_{\mathfrak{m}}, N) \to \operatorname{Rev}(X, N)$$

инъективен.

Поскольку отображение φ^* является гомоморфизмом, достаточно показать, что из $\varphi^*(j') = 0$ следует $j' = 0$. Итак, пусть $J' \to J_{\mathfrak{m}}$ — изогения, прообраз которой Y разлагается на n неприводимых компонент $Y_1, \ldots, Y_n$ (где n — порядок группы N). Каждое из накрытий $Y_i \to X$ имеет степень 1, что показывает существование „сечения" $s\colon X \to Y$. Поскольку $Y = \varphi^*(J')$, сечение s определяет рациональное отображение $\psi\colon X \to J'$, поднимаемое до отображения $\varphi\colon X \to J_{\mathfrak{m}}$. Отображения φ и ψ регулярны вне носителя модуля $\mathfrak{m}$. Так как отображение φ обладает к тому же модулем $\mathfrak{m}$, то предложение 14 гл. 3 показывает, что и ψ обладает модулем $\mathfrak{m}$, а следовательно, представляется в виде $\theta \circ \varphi$, где θ — гомоморфизм $J_{\mathfrak{m}}$ в J' (с точностью до переноса). Композиция $J_{\mathfrak{m}} \to J' \to J_{\mathfrak{m}}$ тождественна (так как она тождественна на образе кривой X, который порождает группу $J_{\mathfrak{m}}$). Это показывает, что группа J' изоморфна произведению $J_{\mathfrak{m}} \times N$, другими словами, что изогения $J' \to J_{\mathfrak{m}}$ тривиальна.

Из предыдущего результата легко следует, что *число неприводимых компонент многообразия* $\varphi^*(J')$ *равно числу неприводимых компонент группы* J'.

12. Случай кривых; ведущий модуль

Мы сохраняем определения и предположения предыдущего пункта.

Предложение 11. *Пусть* $\pi\colon Y \to X$ *— абелево накрытие кривой* X. *Существует наименьший модуль* $\mathfrak{m}$, *такой, что кривая* Y *является прообразом изогении* $J' \to J_{\mathfrak{m}}$, *а носитель* $\mathfrak{m}$ *совпадает с множеством точек ветвления накрытия* π.

(Этот модуль называется *ведущим* для расширения L/K, соответствующего накрытию $Y \to X$.)

Лемма 1. *Пусть* $\mathfrak{m}'$ *и* $\mathfrak{m}''$ *— такие два модуля, что кривая* Y *является прообразом изогений групп* $J_{\mathfrak{m}'}$ *и* $J_{\mathfrak{m}''}$, *Тогда Y совпадает с прообразом изогении группы $J_{\mathfrak{m}}$, где* $\mathfrak{m} = \operatorname{Inf}(\mathfrak{m}', \mathfrak{m}'')$.

Допустим, что эта лемма доказана. Тогда существование наименьшего модуля $\mathfrak{m}$, такого, что кривая Y является прообразом изогении группы $J_{\mathfrak{m}}$, очевидно. Пусть S — носитель модуля $\mathfrak{m}$, а S' — множество точек ветвления накрытия $Y \to X$. Очевидно, что $S' \subset S$. Обратно, если $P \notin S'$, то предложение 8 показывает, что существует отображение $f\colon X \to H$ кривой X в коммутативную группу H и изогения $G \to H$, такая, что $f^*(G)$ изоморфна Y, а отображение f регулярно в точке P. Согласно результатам гл. 5, отображение f разлагается на $X \to J_{\mathfrak{m}'} \to H$, где $\mathfrak{m}'$ — модуль, носитель которого не содержит точки P. В силу минимальности $\mathfrak{m}$ имеем $\mathfrak{m}' \geqslant \mathfrak{m}$ и, значит, $P \notin S$, что и доказывает наше предложение. Перейдем теперь к доказательству леммы. Предположим, что $\deg(\mathfrak{m}') \geqslant 1$ и $\deg(\mathfrak{m}'') \geqslant 1$ (в противном случае нечего доказывать). Положим $\sup(\mathfrak{m}', \mathfrak{m}'') = \mathfrak{m}_1$. Обозначая через J обыкновенное якобиево многообразие X, получаем каноническую последовательность гомоморфизмов

$$
\begin{tikzcd}[row sep=small]
 & J_{\mathfrak{m}'} \arrow[dr] & & \\
J_{\mathfrak{m}_1} \arrow[ur] \arrow[dr] & & J_{\mathfrak{m}} \arrow[r] & J. \\
 & J_{\mathfrak{m}''} \arrow[ur] & &
\end{tikzcd}
$$

Обозначим через H', H'', H, H_1 ядра канонических гомоморфизмов $J_{\mathfrak{m}_1}$ в $J_{\mathfrak{m}'}$, $J_{\mathfrak{m}''}$, $J_{\mathfrak{m}}$, J. Имеем $H' \subset H$, $H'' \subset H$ и $H \subset H_1$. Структура всех этих групп легко определяется с помощью результатов гл. V, § 3, которые показывают, что они изоморфны произведениям групп вида $U_P^{(n)}/U_P^{(n')}$. Отсюда следует, что группы H' и H'' *порождают* группу H, а каноническое отображение $H' \times H'' \to H$ *является либо бирегулярным изоморфизмом* (при $\deg(\mathfrak{m}) \geqslant 1$), *либо отождествляет группу H с факторгруппой $H' \times H''/G_{\mathrm{m}}$* (при $\mathfrak{m} = 0$).

Пусть теперь $J' \to J_{\mathfrak{m}'}$ — изогения группы $J_{\mathfrak{m}'}$, имеющая в качестве прообраза кривую Y, а $J'' \to J_{\mathfrak{m}''}$ — изогения группы $J_{\mathfrak{m}''}$ с теми же свойствами. Прообразы этих изогений на группу $J_{\mathfrak{m}_1}$ обозначим через J_1' и J_1''; согласно предположению 10 (примененному к модулю $\mathfrak{m}_1$), эти группы изоморфны. Обозначим обе эти группы через J_1. Очевидно, изогения $J_1 \to J_{\mathfrak{m}_1}$ тривиальна на группах H' и H''. Пусть

$s'\colon H' \to J_1$ и $s''\colon H'' \to J_1$ — сечения-гомоморфизмы над этими подгруппами. Взяв их сумму, получаем гомоморфизм s группы $H' \times H''$ в группу J_1. Пусть Q — ядро отображения $H' \times H'' \to H$. Коммутативная диаграмма

$$\begin{tikzcd}
 & & J_1 \arrow[d, dash] \\
H' \times H'' \arrow[r] \arrow[urr, "s"] & H \arrow[r] & J_{\mathfrak{m}_1}
\end{tikzcd}$$

показывает, что гомоморфизм s отображает Q в ядро N изогении $J_1 \to J_{\mathfrak{m}_1}$. Так как группа Q связна (действительно, мы видели, что она или тривиальна, или изоморфна группе $G_{\mathfrak{m}}$), то $s(Q) = 0$, поскольку группа H отождествляется с группой $H' \times H''/Q$, гомоморфизм s определяет при переходе к фактору сечение-гомоморфизм H в J_1. Итак, изогения $J_1 \to J_{\mathfrak{m}_1}$ тривиальна на H Отсюда легко следует [это частный случай точной последовательности Ext (см. гл. VII, предложение 2)], что эта изогения совпадает с прообразом изогении $G \to J_{\mathfrak{m}_1}/H \to J_{\mathfrak{m}}$, что и доказывает наше предложение.

Следствие. *Неразветвленные абелевы накрытия алгебраической кривой взаимно однозначно соответствуют изогениям ее якобиевого многообразия.*

Это частный случай $\mathfrak{m} = 0$.

Примеры. 1. Предположим, что порядок группы Галуа N накрытия $Y \to X$ *взаимно прост с* p. В этом случае ведущий модуль $\mathfrak{m}$ равен просто *сумме точек ветвления*, каждая с коэффициентом 1; это следует из теории Куммера и предложения 6 гл. III (или из структуры обобщенных якобиевых многообразий).

2. Пусть N — циклическая группа порядка p и $P \in X$ — точка ветвления. Образующую Артина Шрейера f можно выбрать такой, чтобы она имела в точке P полюс порядка n, взаимно простого с p. Если c_P обозначает коэффициент при точке P в ведущем модуле то предложение V из гл. 3 показывает, что $c_P \leqslant n + 1$. Кроме того, легко

проверяется, что изогения группы $U_p^{(n)}/U_p^{(n+1)}$, определяемая с помощью функции f, не тривиальна. Следовательно, $c_p = n + 1$, что определяет ведущий модуль и показывает, что он совпадает с ведущим модулем Хассе [2].

§ 3. *Проективные системы, связанные с многообразием*

На протяжении всего этого параграфа k обозначает совершенное поле, $\bar{k}$ — его алгебраическое замыкание.

13. Максимальные отображения

Мы будем предполагать, что все многообразия, рассматриваемые в этом и в следующем пункте, определены над полем $\bar{k}$ и неприводимы. Термин *группа* обозначает коммутативную алгебраическую группу (разумеется, неприводимую и определенную над $\bar{k}$); термин *главное однородное пространство* обозначает главное однородное пространство (в смысле гл. V, п. 21) над такими группами.

Пусть H и H' — два главных однородных пространства относительно групп G и G'. Отображение $h\colon H \to H'$ называется *морфизмом*, если оно „аффинно", т. е. если

$$h(x+g) = h(x) + h_0(g), \quad x \in H, \ g \in G,$$

где $h_0\colon G \to G'$ — гомоморфизм (алгебраических групп). Говорят, что h — *изогения*, если h_0 — изогения, другими словами, если пространства H и H' имеют одинаковую размерность, а отображение h сюръективно. *Ядром* отображения h мы будем называть ядро отображения h_0; оно является, таким образом, подгруппой группы G.

Определение 1. *Пусть V — многообразие, а $\alpha\colon V \to H$ — рациональное отображение V в главное однородное пространство H. Говорят, что α максимально, если выполняется следующее условие:*

(M) *если α разлагается на $V \xrightarrow{\alpha'} H' \xrightarrow{h} H$, где $\alpha'\colon V \to H'$ — рациональное отображение, а $h\colon H' \to H$ — морфизм с конечным ядром, то h — изоморфизм H' на H.*

Примеры. Каноническое отображение многообразия V в его многообразие Альбанезе (см. Ленг [5]) максимально (действительно, поскольку ядро отображения h конечно, H' — абелево многообразие, а тот факт, что h — изоморфизм, следует из свойства универсальности многообразия Альбанезе). То же верно и для отображения кривой в любое из ее обобщенных якобиевых многообразий (см. § 6).

Разлагая h на сюръективное и инъективное отображение, мы видим, что условие (M) распадается на два условия:

(M_I) $\alpha(V)$ *порождает* H (другими словами, $\alpha(V)$ не содержится ни в каком аффинном подпространстве H, отличном от него самого);

(M_{II}) *отображение* α *не поднимается ни до какой нетривиальной изогении* H (иначе говоря, из $\alpha = h \circ \alpha'$, где h — изогения, следует, что h — изоморфизм).

Имеет место

Лемма 2. *Из условия* (M_{II}) *вытекает условие* (M_I) [*таким образом, условие* (M_{II}) *эквивалентно условию* (M)].

Допустим, что условие (M) не выполнено, т. е. что существует аффинное подпространство H_1 пространства H, отличное от H и содержащее $\alpha(V)$. Пусть G_1 — подгруппа группы G, соответствующая H_1. Если H_1 (а также и G_1) — максимальное подпространство, то структура коммутативных алгебраических групп (гл. III, п. 7) показывает, что группа G/G_1 изоморфна либо аддитивной группе поля G_1, либо мультипликативной G_m, либо простому абелеву многообразию A. Во всех этих трех случаях существует нетривиальная изогения $G'' \to G/G_1$ (для групп G_a и G_m это очевидно, а для группы A можно взять умножение на целое число > 1). Пусть G' — прообраз этой изогении при отображении $G \to G/G_1$, т. е. подгруппа группы $G \times G''$, образованная парами, имеющими одинаковый образ в G/G_1. Поскольку группа G' — расширение группы G'' с помощью группы G_1, она связна и изогения $G' \to G$ нетривиальна. Зафиксировав некоторую точку пространства H_1, отождествляем пространства H_1 и H с группами G_1 и G и, таким образом, получаем изогению h: $H' \to H$, соответствующую гомоморфизму $G' \to G$. Так как G_1 — подгруппа в G', то однородное пространство H_1 содержится в H', а отображение α разлагается на $V \to H' \to H$, что и требуется в условии (M_{II}).

Замечание. В предыдущем доказательстве изогению $h\colon H' \to H$ можно было бы выбрать сепарабельной или радикальной степени 1 (в случае характеристики $p \neq 0$).

Лемма 3. *Всякое рациональное отображение* $\alpha\colon V \to H$ *многообразия* V *в главное однородное пространство* H *разлагается на*

$$V \xrightarrow{\alpha'} H' \xrightarrow{h} H,$$

где α' *максимально, а* h — *морфизм. При этом можно считать, что ядро отображения* h *конечно.*

Пусть H_1 — аффинное подмногообразие H, минимальное среди всех подмногообразий, содержащих $\alpha(V)$. Заменяя многообразие H на H_1, можно считать, что $\alpha(V)$ *порождает* H. Если отображение α не максимально, то его можно разложить на

$$V \to H_1 \to H,$$

где $H_1 \to H$ — нетривиальная изогения. Аналогично, если отображение $V \to H_1$ не максимально, то его можно разложить на $V \to H_2 \to H_1$ и т. д. Все сводится к доказательству того, что этот процесс стабилизируется, другими словами, что не существует бесконечной последовательности разложений

$$V \to H_{n+1} \to H_n,$$

где $H_{n+1} \to H_n$ — нетривиальная изогения.

Обозначим через G и G_n группы, соответствующие однородным пространствам H и H_n.

Для каждого целого $r \geqslant 1$ обозначим через $S_r\alpha_n$ рациональное отображение многообразия V^{2r} в группу G_n, определяемое формулой

$$S_r\alpha_n(x_1,\ y_1,\ \ldots,\ x_2,\ y_2) = \sum_{i=1}^{r} (\alpha_n(x_i) - \alpha_n(y_i)).$$

Поскольку $\alpha(V)$ порождает H, существует такое целое число r, что $S_r\alpha$ является *почти всюду сюръективным* отображением многообразия V^{2r} в группу G. В силу того что $G_n \to G$ — изогения, то же справедливо и для отображений $S_r\alpha_n$ при всех n. Поле $\bar{k}(V^{2r})$ рациональных функций многообразия V^{2r} содержит в этом случае строго возрастающую последовательность подполей

$$\overline{k}(G)\subset\overline{k}(G_1)\subset\ldots\subset\overline{k}(G_n)\subset\ldots\subset\overline{k}(V^{2r}),$$

что невозможно, поскольку каждое подполе конечно порожденного поля конечно порождено (см. Ленг [4], стр. 64).

Лемма 4. *Пусть* α: $V\to H$ *и* α': $V'\to H'$ — *два максимальных отображения. Если существует морфизм* h: $H'\to H$, *для которого* $\alpha=h\circ\alpha'$, *то он определяется единственным образом. Кроме того, его ядро* N *связно, и он определяет при переходе к фактору изоморфизм* H'/N *на* H.

Если отображения h_1 и h_2 удовлетворяют равенствам $\alpha=h_1\circ\alpha'$ и $\alpha=h_2\circ\alpha'$, то множество точек, в которых эти отображения совпадают, является аффинным подмногообразием многообразия H'. Это подмногообразие содержит образ V и, поскольку отображение α' удовлетворяет условию (M_{I}), совпадает со всем многообразием H'. Обозначим через N_0 связную компоненту ядра N отображения h. Отображение h разлагается на $H'\to H'/N_0\to H$, причем ядро морфизма $H'/N_0\to H$ изоморфно N/N_0, а следовательно, конечно. Поскольку α удовлетворяют условию (M), отображение $H'/N_0\to H$ является изоморфизмом, откуда $N=N_0$. Лемма доказана.

Определение 2. *Если* α *и* α' — *два максимальных отображения, удовлетворяющих условию леммы* 4, *то говорят, что* α' *доминирует над* α, *и пишут* $\alpha'\geqslant\alpha$.

Обозначим через L множество максимальных отображений многообразия V в главные однородные пространства. Отношение $\alpha'\geqslant\alpha$ наделяет множество L *упорядоченностью*. Если $\alpha'\geqslant\alpha$ и $\alpha\geqslant\alpha'$, то мы пишем $\alpha\approx\alpha'$. Это означает, что существует изоморфизм h (необходимо единственный в силу леммы 4) пространства H' и H, такой, что $\alpha=h\circ\alpha'$.

Лемма 5. *Каждая пара элементов из* L *обладает верхней и нижней гранями.*

Покажем сначала, что множество L является *возрастающим фильтрованным множеством.* Пусть α_1: $V\to H_1$ и α_2: $V\to H_2$ — два максимальных отображения. Согласно лемме 3, отображение $\alpha_1\times\alpha_2$: $V\to H_1\times H_2$ можно разложить с помощью максимального отображения α. Ясно, что $\alpha \geqslant \alpha_1$ и $\alpha \geqslant \alpha_2$.

Покажем теперь, что для всех $\alpha \in L$ множество $L(\alpha)$ элементов $\beta \leqslant \alpha$ *сетчато*. В силу леммы 4 элементы этого множества находятся во взаимно однозначном соответствии с элементами множества связных подгрупп группы G, соответствующей однородному пространству H, а это множество сетчато. Для доказательства того, что L также сетчато, достаточно показать, что если $\alpha' \geqslant \alpha$, то операции Sup и Inf в множестве $L(\alpha)$ индуцируются операциями Sup и Inf в множестве $L(\alpha')$. Для операции Inf это очевидно. Пусть β, $\gamma \in L(\alpha)$ и δ (соответственно δ') — их верхняя грань в множестве $L(\alpha)$ (соответственно в $L(\alpha')$). Поскольку $L(\alpha) < L(\alpha')$, то $\delta \geqslant \delta'$, откуда следует, что $\delta' \in L(\alpha)$ и, значит, $\delta' \geqslant \delta$. Лемма доказана.

14. Некоторые свойства максимальных отображений

Пусть α: $V \to H$ — рациональное отображение неприводимого многообразия V в главное однородное пространство H и G — группа, ассоциированная с H. Пусть ω - дифференциальная форма первой степени на группе G, инвариантная относительно переносов (см. гл. III, п. 11). Фиксируя некоторую точку пространства H, мы отождествляем G и H. Форма ω определяет на пространстве H дифференциальную форму, которая не зависит от выбранной точки. Полученный дифференциал мы будем снова обозначать через ω. Прообраз $\alpha^*(\omega)$ дифференциала ω при отображении α является дифференциалом на многообразии V.

Предложение 12. *Если отображение α максимально, то из соотношения $\alpha^*(\omega) = 0$ следует $\omega = 0$.*

В случае когда характеристика поля k отлична от нуля, доказательство вытекает из того факта, что α — „максимальное радикальное" отображение, т. е. не поднимается ни до какой изогении $H' \to H$ (см. Серр [6], теорема 4). Если же характеристика равна нулю, то, используя тот факт, что $\alpha(V)$ порождает H, получаем почти всюду сюръективное отображение $S_r\alpha$: $V^{2r} \to G$ (см. доказательство леммы 3). Дифференциальная форма $(S_r\alpha)^*\omega$ определяется при помощи предложения 17 из гл. III: она является прямой суммой $2r$ членов, соответствующих $\pm\alpha^*(\omega)$, а следовательно, равна нулю, если $\alpha^*(\omega)=0$. Из того, что $S_r\alpha$ почти всюду сюръективно, следует, что $\omega=0$.

Прежде чем сформулировать следующее предложение, заметим, что если многообразие V нормально и отображение α: $V\to H$ разлагается на $V\xrightarrow{\alpha'}H'\xrightarrow{h}H$, где α' — рациональное отображение, а h — изогения, то отображение α' регулярно тогда (и только тогда), когда регулярно отображение α. Это непосредственно следует из „основной теоремы“ Зарисского (см. Ленг [4], гл. 5).

Предположим теперь, что многообразие V нормально, отображение α регулярно и $k=\mathbf{C}$. Имеет место

Предложение 13. *Для того чтобы отображение α было максимальным, необходимо и достаточно, чтобы гомоморфизм α_*: $H_1(V)\to H_1(H)$, определяемый этим отображением, был сюръективным.*

[Через $H_1(V)$ и $H_1(H)$ обозначены одномерные группы гомологий с целочисленными коэффициентами многообразий V и H.]

Доказательство этого предложения очень близко к доказательству предложения 11 из гл. V, поэтому мы ограничимся лишь несколькими замечаниями. Отображение α_* сюръективно в том и только том случае, когда группа $H_1(H)$ не имеет подгрупп конечного индекса >1, содержащих $\alpha_*(H_1(V))$, другими словами, когда отображение α не разлагается на $V\xrightarrow{\alpha'}H'\xrightarrow{h}H$, где α': $V\to H'$ — непрерывное отображение, а $H'\xrightarrow{h}H$ — конечное накрытие степени >1. По лемме 24 гл. V это накрытие является на самом деле изогенией и по лемме 25 той же главы отображение α' регулярно. Из этих лемм и из того факта, что рациональность отображения α' влечет его регулярность, следует предложение 13.

Замечание. Предыдущие два предложения дают новые доказательства хорошо известных результатов относительно многообразий Альбанезе и обобщенных якобиевых многообразий.

15. Максимальные отображения, определенные над полем k

Возвратимся к обозначениям и предположениям п. 13 и допустим, что многообразие V снабжено структурой *k-многообразия*. В этом случае можно рассматривать отображения $\alpha\colon V \to H$, определенные над полем k (группа G и однородное пространство H также определены над k). Здесь разница между группой и главным однородным пространством становится существенной, поскольку пространство H может не иметь рациональных точек над k. Говорят, что отображение $\alpha\colon V \to H$, определенное над k, *максимально*, если оно максимально над $\bar{k}$. Пусть L_k — множество таких отображений. Для элементов α и α' этого множества мы пишем $\alpha' \geqslant \alpha$, если существует такой морфизм h, определенный над k, что $\alpha = h \circ \alpha'$. Каноническое отображение $L_k \to L$, очевидно, возрастающее. Более точно:

Лемма 6. *Отношение упорядоченности в множестве L_k индуцировано отношением упорядоченности в множестве L.*

Надо доказать, что если $\alpha\colon V \to H$ и $\alpha'\colon V \to H'$ — два элемента множества L_k, такие, что существует морфизм h (определенный над $\bar{k}$), для которого $\alpha = h \circ \alpha'$, то этот морфизм определен также и над полем k. Обозначая через σ k-автоморфизм поля $\bar{k}$, имеем $V^\sigma = V$, $H^\sigma = H$, $H'^\sigma = H'$, $\alpha^\sigma = \alpha$ и $\alpha'^\sigma = \alpha'$. Отсюда следует, что $\alpha = h^\sigma \circ \alpha'$, и лемма 4 показывает, что $h^\sigma = h$. Это означает, что отображение h определено над k.

В частности, соотношение $\alpha \approx \alpha'$ *в множестве* L_k эквивалентно соотношению $\alpha \approx \alpha'$ *в множестве* L. Ввиду этого множество L_k можно рассматривать как подмножество множества L, что мы и будем делать в дальнейшем.

Лемма 7. *Для того чтобы элемент $\alpha \in L$ принадлежал подмножеству L_k, необходимо и достаточно, чтобы $\alpha^\sigma \approx \alpha$ для любого k-автоморфизма поля $\bar{k}$.*

Необходимость очевидна. Докажем достаточность. Заметим, что во всяком случае существует такое конечное расширение k_1 поля k, что $\alpha \in L_{k_1}$; при этом можно считать, что оно есть расширение Галуа. Обозначим через $\mathfrak{g}$ группу

Галуа для k_1/k. Если $\sigma \in \mathfrak{g}$, то по предположению $\alpha^\sigma \approx \alpha$. Обозначая через H однородное пространство над полем k, соответствующее элементу α, получаем, таким образом, изоморфизм h_σ: $H \to H^\sigma$. Согласно лемме 6, этот изоморфизм определен над k_1.

Формула $\alpha^\sigma = h_\sigma \circ \alpha$ показывает, что $\alpha^{\sigma\tau} = (h_\sigma)^\tau \circ \alpha^\tau = (h_\sigma)^\tau \circ h_\tau \circ \alpha = h_{\sigma\tau} \circ \alpha$, откуда (см. лемму 4) $h_{\sigma\tau} = (h_\sigma)^\tau \circ h_\tau$. Теорема *о спуске основного поля* (гл. V, п. 20, следствие 2 предложения 12) показывает тогда, что пространство H k_1-изоморфно главному однородному пространству H_0, определенному над полем k, откуда и следует лемма 7.

Лемма 8. *Множество L_k кофинально в множестве L.* Пусть $\alpha \in L$. Выберем такое конечное расширение Галуа k_1 поля k, что $\alpha \in L_{k_1}$. Пусть $\mathfrak{g}$ — группа Галуа расширения k_1/k и $\alpha^\sigma (\sigma \in \mathfrak{g})$ — элементы, сопряженные к α. Положим $\beta = \sup (\alpha^\sigma)$. Тогда $\beta \geqslant \alpha$ и, так как $\beta \approx \beta^\sigma$ для всех $\sigma \in \mathfrak{g}$, лемма 7 показывает, что $\beta \in L_k$.

§ 4. *Поля классов*

В этом параграфе k обозначает конечное поле из q элементов, V — неприводимое k-многообразие. Обозначим через K поле $k(V)$ рациональных функций на V, определенных над k. Мы найдем группу Галуа *максимального абелевого расширения* поля K.

16. Формулировка основной теоремы

Пусть α: $V \to H$ — элемент из множества L_k, т. е. максимальное отображение, определенное над k. Пусть G — группа, ассоциированная с пространством H. Через G_k (соответственно H_k) будем обозначать множество точек G (соответственно H), рациональных над полем k. Следствие 1 предложения 3 показывает, что множество H_k непусто; оно является, следовательно, „главным однородным пространством“ над группой G_k. Обозначим через $I_k(H)$ свободную абелеву группу, порожденную множеством H_k; эта группа наделяется каноническим сюръективным гомоморфизмом $\varepsilon\colon I_k(H) \to \mathbf{Z}$.

Пусть I_0 — ядро отображения ε. Элемент $x \in I_0$ записывается в виде формальной линейной комбинации $x = \sum n_i x_i$, $x_i \in H_k$, $n_i \in \mathbf{Z}$, $\sum n_i = 0$. Этому элементу можно сопоставить такую же сумму, но *вычисленную в группе* G_k; так мы получаем сюръективный гомоморфизм $I_0 \to G_k$. Обозначим через N ядро этого гомоморфизма и положим

$$H(k) = I_k(H)/N.$$

Гомоморфизм ε определяет при переходе к фактору сюръективный гомоморфизм $H(k) \to \mathbf{Z}$, который также обозначим через ε. Ядро этого гомоморфизма отождествляется с группой G_k. Другими словами, имеет место следующая точная последовательность:

$$0 \to G_k \to H(k) \xrightarrow{\varepsilon} \mathbf{Z} \to 0. \tag{1}$$

Прообраз элемента $1 \in \mathbf{Z}$ в группе $H(k)$ канонически отождествляется с множеством H_k (так как оно имеет структуру главного однородного пространства над G_k).

[Разумеется, предыдущая конструкция не имеет ничего общего с теорией алгебраических групп. Ее можно применять ко всем главным однородным пространствам над коммутативными группами: это есть обыкновенное „барицентрическое исчисление".]

Пусть теперь $\alpha'\colon V \to H'$ — элемент из множества L_k, для которого $\alpha' \geqslant \alpha$, а $h\colon H' \to H$ - соответствующий ему морфизм. Отображение h определяет гомоморфизм групп $H'(k) \to H(k)$. Кроме того, имеем коммутативную диаграмму

$$\begin{tikzcd}
0 \arrow[r] & G'_k \arrow[r] \arrow[d, "h_0"] & H'(k) \arrow[r] \arrow[d, "h"] & \mathbf{Z} \arrow[r] \arrow[d, "\mathrm{Id}"] & 0 \\
0 \arrow[r] & G_k \arrow[r] & H(k) \arrow[r] & \mathbf{Z} \arrow[r] & 0
\end{tikzcd}$$

Согласно лемме 4, ядро отображения $h_0\colon G' \to G$ связно. Следствие 2 предложения 3 показывает теперь, что отображение $G'_k \to G_k$ сюръективно, а значит, сюръективно и отображение $H'(k) \to H(k)$.

Определение 3. *Назовем группой классов циклов многообразия V и обозначим через $A_k(V)$ проективный предел групп $H_\alpha(k)$, где α пробегает упорядоченное фильтрованное множество L_k.*

Обозначим, кроме того, через $A_k^0(V)$ проективный предел групп G_k. В силу того что группы G_k *конечные*, проективный предел точной последовательности (1) есть точная последовательность

$$0 \to A_k^0(V) \to A_k(V) \to \mathbf{Z} \to 0. \qquad (2)$$

Заметим, что определение максимального отображения *бирационально*: построения и определения не зависят от *модели* V поля K. По этой причине вместо $A_k(V)$ и $A_k^0(V)$ мы будем писать $A(K)$ и $A^0(K)$.

Обозначим теперь через Ω алгебраическое замыкание поля K, а через K_a — *максимальное абелево расширение* поля K, т. е. наибольшее абелево расширение K, содержащееся в поле Ω. Хорошо известно, что поле $\bar{k}$ абелево над k. Его группа Галуа изоморфна $\hat{\mathbf{Z}}$ пополнению группы $\mathbf{Z}$ относительно топологии, определяемой подгруппами конечного индекса; отображение σ: $\lambda \to \lambda^q$ является *образующей* (в топологическом смысле) этой группы. Поскольку многообразие V предполагается *неприводимым* (в абсолютном смысле, т. е. над полем $\bar{k}$), расширения $\bar{k}/k$ и K/k линейно свободны над k. Это показывает, что композит $K\bar{k}$ абелев над K и что группа Галуа расширения $K\bar{k}/K$ изоморфна $\hat{\mathbf{Z}}$. В частности, имеем $K \subset \bar{k}K \subset K_a$. Обозначим через $\mathfrak{g}(K)$ подгруппу группы Галуа расширения K_a/K, образованную элементами, индуцирующими на поле $K\bar{k}$ элементы из $\mathbf{Z}$ (а не из $\hat{\mathbf{Z}}$); через $\mathfrak{g}^0(K)$ обозначим группу Галуа расширения $K_a/K_{\bar{k}}$. Таким образом, имеет место точная последовательность

$$0 \to \mathfrak{g}^0(K) \to \mathfrak{g}(K) \to \mathbf{Z} \to 0. \qquad (3)$$

Снабдим группу $\mathfrak{g}^0(K)$ естественной топологией Галуа, превращающей ее в компактную группу. После этого группа $\mathfrak{g}(K)$ топологизируется условием, что $\mathfrak{g}^0(K)$ — открытая подгруппа (другими словами, ее факторгруппа $\mathbf{Z}$ должна быть снабжена дискретной топологией). Группа $\mathfrak{g}(K)$ — „почти" группа Галуа расширения K_a/K (более точно последняя является пополнением группы $\mathfrak{g}(K)$ относительно топологии, определяемой открытыми подгруппами конечного индекса).

Теперь мы можем сформулировать главный результат этой главы.

Теорема 1. *Существует канонический изоморфизм точной последовательности* (2) *на точную последовательность* (3).

(Разумеется, этот изоморфизм тождествен на $\mathbf{Z}$.)

В частности, „геометрическая" группа Галуа $\mathfrak{g}^0(K)$ изоморфна группе $A^0(K)$ классов нульмерных циклов.

Остальная часть этого параграфа посвящена доказательству теоремы 1. Прежде всего для каждого $\alpha \in L_k$ мы построим расширение $E_\alpha/K\bar{k}$, группа Галуа которого над полем K изоморфна группе $H_\alpha(k)$. Далее мы покажем, что если $\alpha \geqslant \beta$, то $E_\alpha \supset E_\beta$, причем соответствующий гомоморфизм групп Галуа есть каноническое отображение $H_\alpha(k) \to H_\beta(k)$. Наконец, мы докажем, что всякое конечное абелево расширение поля K содержится в одном из полей E_α, откуда, очевидно, следует утверждение теоремы 1.

17. Построение расширений

Пусть α: $V \to H$ — элемент из множества L_k, и G — соответствующая ему группа.

Предложение 14. *Прообраз сепарабельной изогении h: $H' \to H$ при отображении α определяет неприводимое абелево накрытие многообразия V.*

Пусть $V' = \alpha^*(H')$; ясно, что V' — абелево накрытие V с группой Галуа, изоморфной ядру N отображения h. Обозначим через V_1' одну из неприводимых компонент многообразия V', а через N_1 — подгруппу группы N, образованную элементами $s \in N$, такими, что $s(V_1') = V_1'$. Положим $V'' = V'/N_1$ и $H'' = H'/N_1$. Имеем $V'' = \alpha^*(H'')$, и по построению накрытие $V'' \to V$ тривиально. Следовательно, существует сечение f: $V \to V''$, или же отображение α'': $V \to H''$, поднимающее отображение α: $V \to H$. Поскольку α максимально, отображение $H'' \to H$ является изоморфизмом, откуда $N_1 = N$, $V_1' = V'$, и накрытие V' неприводимо. Предложение доказано. (См. доказательство предложения 10, п. 11.)

Выберем теперь точку $h \in H_k$ и определим отображение $\wp_h$: $G \to H$ формулой

$$\wp_h(x) = x^q - x + h.$$

Отождествляя пространство H с группой G с помощью выбора точки h в качестве начальной, мы видим, что последнее отображение совпадает с изогенией $\wp$: $G \to G$, рассмотренной в п. 6. Ее прообраз W_h при отображении α определяет *абелево накрытие многообразия* V, которое *определено* над полем k и абсолютно неприводимо в силу предыдущего предложения. Группа Галуа этого накрытия изоморфна группе G_k, действующей посредством переносов. Обозначим через K_h поле рациональных функций на многообразии W_h и положим $E_h = K_h\bar{k}$, так как многообразие W_h абсолютно неприводимо, поля K_h и $K\bar{k}$ линейно свободны над полем K. Отсюда следует, что поле E_h является расширением Галуа поля K с группой Галуа, изоморфной произведению $G_k \times \mathbf{Z}$ (здесь, как и прежде, речь идет о группе Галуа, полученной посредством замены группы $\hat{\mathbf{Z}}$ на $\mathbf{Z}$).

Лемма 9. *Расширение E_h/K не зависит от выбора точки $h \in H_k$.*

Надо доказать, что накрытия $W_h \to V$ и $W_{h'} \to V$ *изоморфны над $\bar{k}$* для любых h, $h' \in H_k$. Поскольку отображение $\wp$: $G \to G$ сюръективно, существует элемент $c \in G$, такой, что $c^q - c = h - h'$. Если обозначить через θ: $G \to G$ перенос на элемент c, то $\wp_h = \wp_{h'} \circ \theta$, чем, очевидно, и устанавливался искомый изоморфизм.

Заметим, что если $h \neq h'$, то *невозможно* точку c выбрать рациональной над полем k. Это показывает, что расширения K_h и $K_{h'}$ неизоморфны.

Определение 4. Будем обозначать через E_α расширение E_h/K, где h — произвольная точка пространства H.

(Лемма 9 показывает, что это определение корректно.)

Нам осталось установить канонический изоморфизм между группой Галуа $\mathfrak{g}_\alpha$ расширения E_α/K и группой $H(k)$. Выберем снова точку $h \in H_k$. После отождествления E_α с E_h группа $\mathfrak{g}_\alpha$ отождествляется, как мы видели, с произведением $G_h \times \mathbf{Z}$. С другой стороны, выбор точки h отождествляет группу $H(k)$ также с группой $G_h \times \mathbf{Z}$, так как каждый элемент из $H(k)$ записывается однозначным образом в виде $g + nh$, $g \in G_k$, $n \in \mathbf{Z}$. Отсюда следует изоморфизм ρ_h: $H(k) \to \mathfrak{g}_\alpha$.

Лемма 10. *Изоморфизм ρ_h не зависит от выбора точки $h \in H_k$.*

Прежде всего ясно, что если h и h' — две точки пространства H_k, то изоморфизмы ρ_h и $\rho_{h'}$ совпадают на группе $G_k \subset H(k)$. Все сводится, следовательно, к доказательству того, что эти изоморфизмы совпадают на элементе степени 1 группы $H(k)$, например на h. Положим $\omega = \rho_h(h)$ и $\omega' = \rho_{h'}(h)$. Надо показать, что эти элементы совпадают при отождествлении полей $K_h\bar{k}$ и $K_{h'}\bar{k}$ с помощью изоморфизма θ: $K_{h'}\bar{k} \to K_h\bar{k}$, введенного при доказательстве леммы 9. Другими словами, надо установить формулу $\omega \circ \theta = \theta \circ \omega'$. Но по определению прообраза W_h и $W_{h'}$ являются подмногообразиями произведения $V \times G$, а элементы полей $K_h\bar{k}$ и $K_{h'}\bar{k}$ интерпретируются как функции двух переменных $f(v, x)$, $v \in V$, $x \in G$ со значениями в поле $\bar{k}$. Отображения θ, ω, ω' записываются тогда следующим образом:

$$(\theta f)(v, x) = f(v, x + c),$$

$$(\omega f)(v, x) = f(v^{1/q}, x^{1/q})^q,$$

$$(\omega' f)(v, x) = f(v^{1/q}, x^{1/q} + h - h')^q.$$

Вычисляя $(\omega\theta f)(v, x)$ и $(\theta\omega' f)(v, x)$, в обоих случаях получим $f(v^{1/q}, x^{1/q} + c)^q$, чем и показано, что $\theta \circ \omega' = \omega \circ \theta$.

Из леммы 10 следует

Предложение 15. *Группа Галуа расширения E_α/K канонически изоморфна группе $H_\alpha(k)$.*

Замечание. Лемму 10 можно доказать и без вычислений, основываясь на законе взаимности (см. § 5).

Пусть теперь $\alpha'\colon V \to H'$ — другой элемент из множества L_k, такой, что $\alpha' \geqslant \alpha$, и $f\colon H' \to H$ — морфизм, определяемый этим элементом.

Предложение 16. *Если $\alpha' \geqslant \alpha$, то поле $E_{\alpha'}$ содержит поле E_α и имеет место коммутативная диаграмма*

$$\begin{array}{ccc} H'(k) & \to & \mathfrak{g}_{\alpha'} \\ \downarrow & & \\ H(k) & \to & \mathfrak{g}_\alpha \end{array}$$

Пусть $h' \in H'_k$ и $h = f(h')$. Согласно построению полей E_α и $E_{\alpha'}$ и определению изоморфизмов ρ_h и $\rho_{h'}$, достаточно доказать, что $K_h \subset K_{h'}$ и что соответствующий гомоморфизм группы Галуа совпадает с каноническим гомоморфизмом группы G'_k на группу G_k. Но если $f_0\colon G' \to G$ - гомоморфизм, соответствующий отображению f, то имеет место коммутативная диаграмма

$$\begin{array}{ccc} G' & \xrightarrow{f_0} & G \\ {\scriptstyle \wp_{h'}}\downarrow & & \downarrow{\scriptstyle \wp_h} \\ H' & \xrightarrow{f} & H \end{array}$$

Эта диаграмма показывает, что прообраз изогении $\wp_h$ при отображении f совпадает с фактором изогении $\wp_{h'}$, соответствующей гомоморфизму $f_0\colon G'_k \to G_k$. Отсюда немедленно следует предложение 16.

18. Окончание доказательства теоремы 1. Первый способ

Пусть K' — объединение расширений E_α, $\alpha \in L_k$. Предложения 15 и 16 показывают, что поле K' является абелевым расширением поля K, содержащим поле $\bar{k}$ и имеющим в качестве (видоизмененной) группы Галуа группу $A(K)$ классов циклов многообразия V. Имеем $K' \subset K_a$. Все сводится к доказательству того, что $K_a \subset K'$.

Пусть $\hat{\mathfrak{g}}(K)$ — группа Галуа расширения K_a/K; эта группа является расширением группы $\hat{\mathbf{Z}}$ с помощью $\mathfrak{g}^0(K)$. Пусть

σ — образующая группы $\mathbf{Z}$. Выбор представителя σ в группе $\widehat{\mathfrak{g}}(K)$ определяет сечение-гомоморфизм s: $\mathbf{Z} \to \widehat{\mathfrak{g}}(K)$; этот гомоморфизм продолжается по непрерывности на группу $\widehat{\mathbf{Z}}$, поскольку $\widehat{\mathfrak{g}}(K)$ — компактная всюду разрывная группа. Таким образом, группа $\widehat{\mathfrak{g}}(K)$ разлагается (разумеется, не канонически) в произведение $\mathfrak{g}^0(K) \times \widehat{\mathbf{Z}}$, чему соответствует разложение $K_a = L_0\bar{k}$, где поля L_0 и $\bar{k}$ линейно свободны над k. Поскольку $\bar{k} \subset K'$, достаточно показать, что $L_0 \subset K'$.

Пусть $L'K$ — конечное расширение, содержащееся в поле L_0. Так как это расширение и $\bar{k}$ линейно свободны, ему соответствует абелево неприводимое и определенное над k накрытие π: $W \to V$, где W — неприводимое k-многообразие. Пусть N — группа Галуа этого накрытия. Согласно следствию предложения 7 из § 2, накрытие W является прообразом над полем k сепарабельной изогении $G' \to G$ при рациональном отображении f: $V \to G$. По лемме 3 отображение f можно разложить на

$$V \xrightarrow{\alpha} H_\alpha \xrightarrow{\varphi} G,$$

где φ — морфизм, а α — максимальное отображение. Лемма 8 показывает, что отображение α можно выбрать из множества L_k. Если σ — k-автоморфизм поля $\bar{k}$, то $f = f^\sigma$, откуда $\varphi \circ \alpha = \sigma \circ \alpha$. Это показывает, что $\varphi^\sigma = \varphi$, т. е. что отображение φ определено как k. Пусть $H' \to H_\alpha$ — прообраз изогении $G' \to G$ при отображении φ. Поскольку φ определено над полем k, то и эта изогения определена над k и ее ядро состоит из элементов, рациональных над этим полем (так как это верно для изогении $G' \to G$). Имеем $\alpha^*(H') = W$ и так как многообразие W неприводимо, то неприводимо и H'. Пусть h' — точка H', рациональная над k; такая точка существует в силу следствия 1 предложения 3. Пусть h — ее образ в H. Беря эти точки за начальные, отождествим пространства H' и H с их группами. Тогда предложение 6 из § 1 показывает, что отображение $H' \to H_\alpha$ является факторнакрытием накрытия $\wp_h$: $G_\alpha \to H_\alpha$ (где G_α обозначает группу, ассоциированную с пространством H_α). Накрытие $W = \alpha^*(H')$ поэтому тоже является факторнакрытием накрытия W_h, прообраза изогении $\wp_h$. Это показывает, что $L \subset K_h$, а значит $L \subset E_\alpha$, что и завершает доказательство.

Замечание. В силу того факта, что группа $G(N)$ из предложения 7 *линейная*, в предыдущем доказательстве использовались только линейные группы. Таким образом, *проективный предел групп $H_\alpha(k)$ не изменится, если ограничиться лишь максимальными отображениями $\alpha \in L_k$, соответствующими линейным группам.* Этот результат любопытен тем более, что такие максимальные отображения не образуют *кофинальной системы* в множестве L_k.

19. Окончание доказательства теоремы 1. Второй способ

Введем сперва следующее определение:

Определение 5. *Пусть α: $V \to H_\alpha$ — элемент из множества L и F — конечное расширение поля $K\bar{k}$. Говорят, что F типа α, если оно является прообразом сепарабельной изогении $H' \to H_\alpha$.*

Это определение является „геометрическим" (т. е. относится к структуре „многообразия", а не „k-многообразия"). Если взять в качестве α каноническое отображение многообразия V в его многообразие Альбанезе, то получим расширение „*типа Альбанезе*", введенное Ленгом [2].

Теорема 1 вытекает из следующих двух предложений:

Предложение 17. *Для каждого конечного абелева расширения F поля $K\bar{k}$ существует такой элемент $\alpha \in L$, что F имеет тип α.*

Здесь мы опять имеем дело с „геометрической" формулировкой. Предложение доказывается рассуждениями, аналогичными приведенным в предыдущем пункте (но более просто): применяя следствие предложения 7 из § 2, видим, что F является прообразом сепарабельной изогении при отображении f: $V \to G$ (вместо этого следствия можно также воспользоватся теориями Куммера и Артина — Шрейера, поскольку поле $\bar{k}$ содержит все корни из единицы). Остается лишь разложить отображение f на $V \xrightarrow{\alpha} H_\alpha \to G$, где α максимально (см. лемму 3).

Про конечное расширение E/K говорят, что оно *типа* α, если типа α расширение $E\bar{k}/K\bar{k}$.

Предложение 18. *Пусть* $\alpha \in L_k$. *Для того чтобы абелево расширение* E/K *имело тип* α, *необходимо и достаточно, чтобы оно содержалось в поле* E_α.

(Обратить внимание на тот факт, что E предполагается *абелевым над* K!)

Достаточность условия очевидна. Докажем его необходимость. Композит $E\bar{k}$ является абелевым расширением поля K (как композит двух абелевых расширений). Рассуждения, примененные в предыдущем пункте к полю K_a, показывают, таким образом, что $E\bar{k} = E'\bar{k}$, где расширение E' поля K и поле $\bar{k}$ линейно свободны. Таким образом, расширение E' определяет неприводимое накрытие π: $W \to V$. Остается показать, что E' содержится в E_α.

По предположению накрытие W имеет вид $\alpha^*(H')$, где $H' \to H_\alpha$ — изогения H_α. Это верно, a priori над полем $\bar{k}$, но не над k. Пусть k — конечное расширение поля k с группой Галуа $\mathfrak{g}$, такое, что это верно над k_1. Если $\sigma \in \mathfrak{g}$, то накрытие W является прообразом накрытия H'^σ. Но так как отображение α максимально, две изогении H_α, имеющие одинаковые прообразы при отображении α^*, изоморфны (см. доказательство предложения 11). Полученный так изоморфизм φ_σ: $H' \to H'^\sigma$, очевидно, определяется единственным образом, а следовательно, он определен над k_1. Немедленно проверяется справедливость соотношения $(\varphi_\sigma)^\tau \circ \varphi_\tau = \varphi_{\sigma\tau}$, что позволяет спустить основное поле пространства H' с k_1 до k. Воспользовавшись тогда, как и в предыдущем пункте, предложением 6 из § 1, находим, что E' содержится в расширении K_h, откуда и следует требуемый результат.

[Укажем вариант предыдущего доказательства, не использующий спуска основного поля.

Пусть, как и выше, k_1 — конечное расширение поля k, такое, что $W = \alpha^*(H')$, где $H' \to H_\alpha$ — изогения, определенная над k_1. Во всяком случае поле $E'k_1$ содержится в расширении E'_α/Kk_1, соответствующем максимальному отображению α и основному полю k. Все сводится, таким образом, к доказательству того, что *наибольшее абелево расширение поля K, содержащееся в E'_α, совпадает с E_α*. Это вопрос теории Галуа: имеем „башню“ полей $k \subset k_1 \subset E_\alpha \subset E'_\alpha$, и надо доказать, что группа Галуа $\mathfrak{t}$ расширения E'_α/E_α содержится в коммутаторе группы Галуа расширения E'_α/K. Последняя группа является расширением группы $\mathfrak{g}$ с помощью $H_\alpha(k)$. Прямое вычисление показывает, что внутренние автоморфизмы, соответствующие элементам группы $\mathfrak{g}$, действуют на $H_\alpha(k')$ тривиально. Отсюда следует, что коммутатор группы G содержит подгруппу в $H_\alpha(k')$, порожденную элементами $x - x^q$, $x \in H_\alpha(k_1)$. С другой стороны, группа $\mathfrak{t}$ изоморфна ядру канонического гомоморфизма $H_\alpha(k') \to H_\alpha(k)$, определяемого соответствием

$$x \to x + x^q + \ldots + x^{q^{d-1}} = \operatorname{Tr}(x), \text{ где } d = [k_1 : k].$$

Для доказательства того, что $\mathfrak{t}$ содержится в коммутаторе группы G, достаточно, следовательно, доказать, что всякий элемент $x \in H_\alpha(k_1)$, для которого $\operatorname{Tr}(x) = 0$, записывается в виде $y - y^q$. Последнее следует из того, что отображение $y \to y - y^q$ сюръективно.]

20. Абсолютное поле классов

Значение предложения 18 заключается в том, что оно позволяет определять тип абелевого расширения E/K *геометрическими* средствами (т. е. определяя его над $\bar{k}$). Рассмотрим для примера случай неразветвленного расширения.

Пусть V — *проективное, неособое* многообразие, α: $V \to A$ — каноническое отображение этого многообразия в его многообразие Альбанезе. Поскольку V неособо, α всюду определено; кроме того, очевидно, что всякое накрытие V типа α (или, как говорят, „типа Альбанезе“) *абелево и неразветвлено*. Посмотрим, верно ли обратное утверждение. Дело немедленно сводится к изучению следующих двух случаев:

а) *Циклическое накрытие порядка n, взаимно простого с p.*

Теория Куммера показывает, что это накрытие соответствует элементу порядка n группы $C(V)$ классов дивизоров многообразия V относительно *линейной* эквивалентности (см. Серр [5], п. 15). Группа $C(V)$ содержит в качестве подгруппы $P(V)$ группу классов дивизоров, алгебраически эквивалентных нулю. Факторгруппа

$$N(V)=C(V)/P(V)$$

есть *группа Нерона — Севери. Группа* $P(V)$ изоморфна многообразию Пикара многообразия V (относительно его групповой структуры) или, что сводится к тому же, многообразию, двойственному A (см. Ленг [5], гл. 6). Имеем $P(A)=P(V)$, и группа $N(A)$ не имеет кручения (см. Барсотти [3] или Серр [6]). Отсюда следует, что рассматриваемый элемент d имеет тип α тогда и только тогда, когда он принадлежит группе $P(V)$. Для того чтобы каждый элемент группы $C(V)$ взаимно простого с p порядка принадлежал группе $P(V)$, необходимо и достаточно [группа $P(V)$ делима], чтобы группа $N(V)$ не содержала элементов с порядком, взаимно простым с p.

б) *Циклическое накрытие порядка, равного степени p.* Рассмотрим случай, когда порядок равен p. Теория Артина — Шрейера (см. Серр [5], п. 16) показывает, что такому накрытию соответствует элемент $x \in H^1(V, \mathfrak{S}_V)$, неподвижный относительно преобразования Фробениуса F. Это накрытие имеет тип Альбанезе тогда и только тогда, когда x принадлежит образу гомоморфизма $\alpha^*: H^1(A, \mathfrak{S}_A) \to H^1(V, \mathfrak{S}_V)$; последний гомоморфизм инъективен (см. гл. 8, а также Серр [6], п. 9). Обозначая через $H^1(A, \mathfrak{S}_A)_s$ *полупростую часть* группы $H^1(A, \mathfrak{S}_A)$ (Серр [5], п. 16), видим, что α^* отображает $H^1(A, \mathfrak{S}_A)$ *на* $H^1(V, \mathfrak{S}_V)_s$. Обратно, если это условие достаточно, то всякое неразветвленное циклическое накрытие порядка p^n многообразия V имеет тип Альбанезе (следует применить индукцию, используя тот факт, что всякое накрытие типа Альбанезе порядка p^{n-1} является образом накрытия того же типа и циклического порядка p^n). Окончательно получаем

Предложение 19. *Для того чтобы всякое абелево неразветвленное накрытие многообразия V имело тип Альбанезе, необходимо и достаточно, чтобы группа Нерона —*

Севери многообразия V не имела кручения порядка, взаимно простого с p, и чтобы отображение $\alpha^*: H^1(A, \mathfrak{O}_A)_s \to H^1(V, \mathfrak{O}_V)$ было сюръективным.

В этом случае предложение 18 показывает, что группа Галуа (модифицированная) *максимального абелева неразветвленного расширения* поля k изоморфна группе $H_\alpha(k)$, т. е. расширению $\mathbf{Z}$ с помощью группы A_k точек A, рациональных над k. Это есть аналог *абсолютного поля классов* из теории чисел.

Замечания. 1. Условие предложения 19 будет выполнено, *если группа Нерона - Севери многообразия V не имеет кручения и если* $h^{0,1}(V) = \dim(A)$ (где, как обычно,

$$h^{0,1}(V) = \dim H^1(V, \mathfrak{O}_V)).$$

Действительно, $\dim H^1(A, \mathfrak{O}_A) = \dim A$ (см. гл. VII), и отображение α^* в этом случае сюръективно. Оба эти условия выполняются, когда V — кривая.

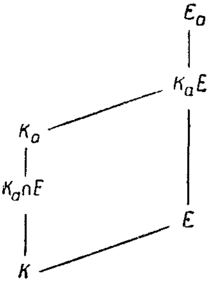
2. В общем случае можно было бы попытаться дать внутренний критерий того, что заданное накрытие является неразветвленным абелевым накрытием типа Альбанезе. В случае циклических расширений порядка n, взаимно простого с p, очевидно, для этого необходимо и достаточно, чтобы это накрытие содержалось в циклическом накрытии порядка, равного произвольной степени n (следует использовать тот факт, что группа Нерона — Севери конечно порождена). Я не знаю, верен ли тот же критерий, когда n равно степени p [1]).

21. Добавление: след отображения

Пусть E — конечное расширение Галуа поля K с группой Галуа $\mathfrak{g}$. Если обозначить через E_a максимальное абелево расширение поля E, то $K_a E \subset E_a$; с другой стороны, $K_a \cap E$ —

[1]) Как сообщил автор, ответ на поставленный вопрос положительный. Это следует из результата Мамфорда: если π_1^{ab} —фактор-группа фундаментальной группы по коммутанту, то гомоморфизм $\pi_1^{ab}(V) \to \pi_1^{ab}(A)$ сюръективен и его ядро есть подгруппа кручения группы $\pi_1^{ab}(V)$ (которая конечна). — *Прим. ред.*

наибольшее абелево расширение, содержащееся в E (см. диаграмму ниже):



Переходя к группам Галуа и принимая во внимание теорему 1, получаем точную последовательность

$$A(E) \to A(K) \to \mathfrak{g}/\mathfrak{g}' \to 0,$$

где $\mathfrak{g}/\mathfrak{g}'$ обозначает коммутатор группы $\mathfrak{g}$.

К этой точной последовательности мы еще вернемся в § 7. Гомоморфизм $A(E) \to A(K)$, фигурирующий в ней, соответствует в классическом случае операции взятия *следа*, обозначаемой Tr.

Можно попытаться определить отображение Tr в более или менее явном виде. Для этого рассмотрим два случая: 1) $E = Kk'$, где k'/k — конечное расширение; 2) расширение E/K и поле $\bar{k}$ линейно свободны („геометрическое" расширение, по выражению Ленга).

Первый случай: $E = k'K$. Группу $A(E)$ можно определить как проективный предел групп $H_\alpha(k'), \alpha \in L_k$, поскольку известно, что множество L_k кофинально в L. Но для каждого $\alpha \in L_k$ имеем гомоморфизм следа Tr: $H_\alpha(k') \to H_\alpha(k)$, определенный приведенной выше формулой

$$\mathrm{Tr}(x) = x + x^q + \ldots + x^{q^{d-1}}, \text{ где } d = [k' : k].$$

Переходя к пределу, получаем искомый гомоморфизм Tr: $A(E) \to A(K)$. Заметим, что этот гомоморфизм *увеличивает степень в d раз.*

Второй случай: *E — геометрическое расширение.* Пусть $x = \{x_{\alpha'}\}$ — элемент из группы $A(E)$, где α' пробегает множество L'_k максимальных отображений модели V' для E. Для того чтобы определить элемент $\mathrm{Tr}(x) \in A(K)$, необходимо определить $\mathrm{Tr}(x)_\alpha \in H_\alpha(x)$ для каждого $\alpha \in L_k$. Но композиция отображений $W \longrightarrow V \xrightarrow{\alpha} H_\alpha$ разлагается на $W \xrightarrow{\alpha'} H' \xrightarrow{\varphi} H_\alpha$, где отображения α' и φ можно определить над k. Полагая

$$\mathrm{Tr}(x)_\alpha = \varphi(x_{\alpha'}),$$

легко проверить, что получается искомый гомоморфизм.

Заметим, что этот гомоморфизм *сохраняет степень*.

§ 5. Отображение взаимности

Обозначения и предположения те же, что и в § 4.

22. Автоморфизм Фробениуса

Пусть P — точка V, алгебраическая над k, и $d = [k(P) : k]$. Точка P имеет d сопряженных над полем k точек

$$P,\ P^q,\ \ldots,\ P^{q^{d-1}}.$$

Сумма $\mathfrak{p}$ этих точек определяет *простой рациональный над полем k цикл*; целое число d называется *степенью* этого цикла. Локальные кольца точек P^{q^i} совпадают; обозначим их через $\mathfrak{O}_P$ или $\mathfrak{O}_\mathfrak{p}$. Мы будем писать также $k(\mathfrak{p})$ вместо $k(P)$.

Пусть теперь L/K — конечное расширение Галуа степени n и $\mathfrak{g}_{L/K}$ (или просто $\mathfrak{g}$) — его группа Галуа. Предположим, что P не является *точкой ветвления* в L. Обозначим через $\mathfrak{O}'_\mathfrak{p}$ целое замыкание кольца $\mathfrak{O}_\mathfrak{p}$ в поле L. Полулокальное кольцо $\mathfrak{O}'_\mathfrak{p}$ изоморфно пересечению локальных колец $\mathfrak{O}'_{\mathfrak{p}_i}$ $(i = 1, \ldots, r)$. Пусть $\mathfrak{m}_\mathfrak{p}$ — максимальный идеал кольца $\mathfrak{O}_\mathfrak{p}$. Известно, что $\mathfrak{O}'_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}\mathfrak{O}'_\mathfrak{p}$ — полупростая алгебра размерности n над полем $k(\mathfrak{p})$, имеющая в качестве группы Галуа группу $\mathfrak{g}$. Эта алгебра распадается на прямую сумму полей $k(\mathfrak{p}_i)$, которые изоморфны полям вычетов колец $\mathfrak{O}'_{\mathfrak{p}_i}$. Пусть $\mathfrak{g}_i$ — подгруппа в $\mathfrak{g}$, образованная из элементов, оставляющих на месте кольцо $\mathfrak{O}'_{\mathfrak{p}_i}$; эта группа изоморфна группе Галуа расширения $k(\mathfrak{p}_i)/k(\mathfrak{p})$; она является, таким образом, циклической группой порядка $f=[k(\mathfrak{p}_i):k(\mathfrak{p})]$, порождаемой элементом $(\mathfrak{p}_i, L/K)$, который соответствует возведению в степень q^d в поле $k(\mathfrak{p}_i)/k(\mathfrak{p})$. Элемент $(\mathfrak{p}_i, L/K)$ называется *автоморфизмом Фробениуса точки* $\mathfrak{p}_i$ в расширении L/K; он является элементом группы Галуа $\mathfrak{g}_{L/K}$ и имеет порядок $f=n/r$.

При замене $\mathfrak{p}_i$ на $\mathfrak{p}_j$ элемент $(\mathfrak{p}_i, L/K)$ преобразуется в сопряженный элемент. Если группа $\mathfrak{g}_{L/K}$ *абелева* (для дальнейшего это наиболее важный случай), то $(\mathfrak{p}_i, L/K)$ не зависит, следовательно, от i, и поэтому его можно обозначить через $(\mathfrak{p}, L/K)$. Мы будем называть этот элемент *автоморфизмом Фробениуса цикла* $\mathfrak{p}$ *для расширения* L/K. Вместо $(\mathfrak{p}, L/K)$ мы будем писать также $(P, L/K)$.

Для того чтобы $(\mathfrak{p}, L/K)=0$, необходимо и достаточно, чтобы цикл $\mathfrak{p}$ *полностью распадался* в расширении L/K, т. е. чтобы $f=1$, или $k(\mathfrak{p}_i)=k(\mathfrak{p})$ для всех i. „Функториальные" свойства автоморфизмов Фробениуса те же, что и в теории чисел (см. Хассе [1], II, § 1). Мы приведем лишь следующее свойство.

(*Транзитивность.*) Если $K\subset E\subset L$, где L — конечное абелево расширение поля K, то образ $(\mathfrak{p}, L/K)$ в группе $\mathfrak{g}_{E/K}$ равен $(\mathfrak{p}, E/K)$.

(Предполагается, разумеется, что P не является точкой ветвления в L/K.)

Это свойство позволяет определить символ $(\mathfrak{p}, L/K)$ для *бесконечных* абелевых расширений L поля K; соответствующий пример будет приведен далее.

23. Геометрическая интерпретация автоморфизма Фробениуса

Рассмотрим сначала случай, когда L получается с помощью расширения основного поля, а затем случай, когда L — „геометрическое" расширение.

1) $L=Kk'$, *где* k'/k — *расширение степени* n.

В этом случае алгебра $\mathfrak{O}'_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}\mathfrak{O}'_\mathfrak{p}$ отождествляется с $k(\mathfrak{p})\otimes_k k'$.

Отсюда следует, что элемент $(\mathfrak{p}, L/K)$ принадлежит группе Галуа $\mathfrak{g}=\mathfrak{g}_{k'/k}=\mathbf{Z}/n\mathbf{Z}$ и сравним с $d \pmod n$.

Переходя к пределу по k', получаем изящную формулу

$$(\mathfrak{p},\ K\bar{k}/K) = \deg(\mathfrak{p}).$$

2) *Поля L и $K\bar{k}$ линейно свободны.*

В этом случае поле L соответствует неприводимому над $\bar{k}$ накрытию $W \to V$. Прообраз в W цикла $\mathfrak{p}$ является рациональным циклом над k, который разлагается в сумму простых рациональных циклов

$$\mathfrak{p} = \sum \mathfrak{p}_i \quad (\text{на } W).$$

Для всякой точки $P \in \mathfrak{p}$ ее прообраз в W распадается на классы сопряженных точек, причем каждый класс порождает одну и только одну из точек $\mathfrak{p}_i$. Если точка $Q \in \mathfrak{p}_i$ проектируется в P, то в нее же проектируется и точка Q^{q^d}, поскольку $P^{q^d} = P$. Следовательно, существует элемент $b \in \mathfrak{g}$, определяемый единственным образом, такой, что $\sigma(Q) = Q^{q^d}$. Этот элемент совпадает с *автоморфизмом Фробениуса* $(Q,\ L/K) = (\mathfrak{p}_i,\ L/K)$. Действительно, если $f \in \mathfrak{O}_Q$, то $f^{\sigma}(Q) = f(\sigma \cdot Q) = f(Q^{q^d}) = f(Q)^{q^d}$. Это показывает, что σ индуцирует при переходе к фактору возведение в q^d-ю степень.

Заметим, что утверждение „$\mathfrak{p}$ полностью распадается в L“ эквивалентно утверждению „$k(Q) = k(P)$ для всех точек Q, проектирующихся в P“.

24. Определение автоморфизма Фробениуса в расширении типа α

Пусть α: $V \to H_\alpha$ — элемент из множества L_k и $\mathfrak{p} = P + \ldots + P^{q^{d-1}}$ — простой рациональный цикл на V, такой, что *отображение α регулярно в точке P*. Это последнее условие означает, что $\mathfrak{p}$ не является точкой ветвления в расширении E_α/K, соответствующем α (см. п. 17). Таким образом, можно говорить об элементе $(\mathfrak{p},\ E_\alpha/K)$, принадлежащем группе Галуа $\mathfrak{g}_{E_\alpha/K}$; однако эту группу мы уже вычислили (п. 17): она изоморфна пополнению (относительно топологии, определяемой подгруппами конечного индекса) группы $H_\alpha(k)$. Более точно положим

$$\alpha(\mathfrak{p}) = \sum_{i=0}^{d-1} \alpha(P^{q^i}),$$

где сумма вычисляется в группе $H_\alpha(\bar{k})$, определенной в п. 13. Так как цикл $\mathfrak{p}$ инвариантен относительно всех k-автоморфизмов поля $\bar{k}$, точка $\alpha(\mathfrak{p})$ также инвариантна. Это показывает, что $\alpha(\mathfrak{p}) \in H_\alpha(k)$. Результат, который мы имели в виду, формулируется следующим образом:

Теорема 2. *Если отождествить, как делалось выше, группу $H_\alpha(k)$ с всюду плотной подгруппой группы $\mathfrak{g}_{E_\alpha/K}$, то $(\mathfrak{p}, E_\alpha/K) = \alpha(\mathfrak{p})$.*

Ввиду транзитивности автоморфизма Фробениуса достаточно доказать, что для подрасширений E, порождающих поле E_α, элемент $\alpha(\mathfrak{p})$ индуцирует $(\mathfrak{p}, E/K)$.

Положим сначала $E = K\bar{k}$. Как известно, $(\mathfrak{p}, E/K) = \deg(\mathfrak{p})$. С другой стороны, образ $\alpha(\mathfrak{p})$ в $\mathbf{Z}$ равен также $\deg(\mathfrak{p})$, откуда и следует искомый результат.

Далее положим $E = K_h$, где $h \in H_k$. Группа $\mathfrak{g}_{E/K}$ совпадает с G_k (где G обозначает группу, ассоциированную с пространством H), причем $H_\alpha(k) \to G_k$ есть гомоморфизм, ставящий в соответствие элементу $\sum n_i h_i$ элемент $\sum n_i(h_i - h)$ группы G_k. В частности, образом $\alpha(\mathfrak{p})$ будет

$$\sigma = \sum_{i=0}^{d-1} \alpha(P)^{q^i} - dh.$$

Покажем, что $\sigma = (\mathfrak{p}, E/K)$, т. е. что σ преобразует точку Q, проектирующуюся в P, в точку Q^q. Накрытие W_h, соответствующее K_h, является подмногообразием произведения $V \times G$. Точку Q можно, следовательно, отождествить с парой (P, Q_1), где $Q_1 \in G$ и удовлетворяет тождеству

$$Q_1^q - Q_1 + h = \alpha(P).$$

Возводя это тождество в q^i-ю степень ($i=0, \ldots, d-1$), получаем

$$Q_1^{q^{i+1}} - Q_1^{q^i} + h = \alpha(P)^{q^i}.$$

Суммируя d так полученных тождеств, находим

$$Q_1^{q^d} - Q_1 + dh = \sum_{i=0}^{d-1} \alpha(P)^{q^i},$$

откуда

$$Q_1^{q^d} - Q_1 = \sigma.$$

Таким образом, $\sigma(Q) = (P, Q_1 + \sigma) = (P, Q_1^{q^d}) = Q^{q^d}$. Это показывает, что $\sigma = (\mathfrak{p}, E/K)$. Так как расширения $K\bar{k}/K$ и K_h/K порождают поле E_α, теорема доказана.

Следствие. *Пусть $\wp$: $G \to G$ — изогения $x \to x^q - x$, а $\mathfrak{p}$ — простой рациональный цикл на G. Результат применения автоморфизма Фробениуса к $\mathfrak{p}$ в накрытии $\wp$ равен элементу группы G_k, который совпадает с суммой (в группе G) точек цикла $\mathfrak{p}$.*

В частности, если $d = 1$, т. е. если $\mathfrak{p}$ сводится к точке $P \in G_k$, мы видим, что *автоморфизм Фробениуса точки P* (рассматриваемой как простой цикл) *равен самой точке P* (рассматриваемой как элемент группы Галуа).

Замечание. Рассуждения теоремы 2 можно применить к любому накрытию $W \to V$, являющемуся прообразом изогении $G' \to H$. Тот факт, что отображение α: $V \to H$ предполагается максимальным, не играет существенной роли

25. Отображение взаимности. Формулировка результатов

Пусть, как и прежде, L/K — конечное абелево расширение и V — модель поля K, все точки которой неразветвлены в L (такая модель всегда существует; достаточно взять произвольную модель и исключить точки ветвления, поскольку известно, что последние образуют собственное алгебраическое подмножество). Группа циклов V, рациональных над k, обозначаемая через $Z_k(V)$, имеет в качестве базиса множество простых рациональных циклов. Отображение $\mathfrak{p} \to (\mathfrak{p}, L/K)$, доопределенное по линейности, приводит тогда к гомоморфизму группы $Z_k(V)$ в $\mathfrak{g}_{L/K}$, который называется *отображением взаимности.*

Теорема 3. *Для любой модели V поля K, не имеющей точек ветвления в L, отображение взаимности $Z_k(V) \to \mathfrak{g}_{L/K}$ сюръективно.*

Мы докажем эту теорему немного позднее. Сперва дадим эквивалентные ей формулировки.

Пусть сначала α: $V \to H$ — элемент из L_k; можно продолжить отображение $\mathfrak{p} \to \alpha(\mathfrak{p}) \in H_\alpha(k)$ до гомоморфизма $c \to \alpha(c)$ группы $Z_k(V)$ в $H_\alpha(k)$.

Теорема 3′. *Для любой модели V поля K, такой, что отображение α определено во всех точках V, гомоморфизм $Z_k(V) \to H_\alpha(k)$ сюръективен.*

Предположим, что теорема 3 верна, и пусть H' — образ группы $Z_k(V)$ в $H_\alpha(k)$. Допустим, что $H' \neq H_\alpha(k)$. Так как $H_\alpha(k)$ - абелева группа конечного типа, то она содержит подгруппу H'' конечного индекса $n > 1$, которая содержит H'. Этой подгруппе соответствует конечное расширение L/K степени n, в котором отображение взаимности тривиально (теорема 2), что противоречит теореме 3. Обратно, пусть верна теорема 3′ для всех $\alpha \in L_k$ (или только для кофинального семейства таких α); в этом случае всякое конечное расширение L/K содержится в E_α/K, откуда сразу же следует теорема 3.

[Теорема 3′ оправдывает наименование „группы классов циклов“ для проективного предела $A(K)$ групп $H_\alpha(k)$; она доказывает фактически, что $H_\alpha(k)$ — факторгруппа группы $Z_k(V)$ рациональных циклов на V по отношению эквивалентности, определяемому отображением α. Например, если α: $V \to J$ — каноническое отображение кривой в ее якобиево многообразие, то эта группа есть группа классов дивизоров V по отношению линейной эквивалентности; см. § 6.]

Теорема 3″. *Пусть F/K — произвольное конечное расширение (не обязательно расширение Галуа), а V — такая* *модель поля K, что всякий простой рациональный цикл V не разветвлен и полностью распадается в F. Тогда $F = K$.*

Пусть r — целое число $\geqslant 1$. Обозначим через 3_r (соответственно $3_r''$) формулировку теоремы 3 (соответственно $3''$) для всех полей K степени трансцендентности r над k; обозначим также через $3_r''$-G и $3_r''$-A варианты теоремы $3''$, где предполагается, что расширение F/K — расширение Галуа или абелево. Покажем, что имеют место эквивалентности

$$3_r'' \Leftrightarrow 3_r''\text{-}G \Leftrightarrow 3_r''\text{-}A \Leftrightarrow 3_r.$$

Пусть F/K — расширение, удовлетворяющее условиям теоремы $3''$, а F'/K — наименьшее расширение Галуа, содержащее это расширение. Поскольку поле F' является композитом полей F и ему сопряженных, расширение F'/K также удовлетворяет условиям теоремы. Если $[F:K] > 1$, то $[F':K] > 1$, и группа Галуа $\mathfrak{g}_{F'/K}$ содержит нетривиальную подгруппу $\mathfrak{g}''$. Пусть K'' — подполе, соответствующее подгруппе $\mathfrak{g}''$. Расширение F'/K'' удовлетворяет условиям теоремы $3''$, откуда $3_r''$-$A \Rightarrow 3_r''$. Так как импликации $3_r'' \Rightarrow 3_r''$-$A \Rightarrow 3_r''$-G тривиальны, мы получаем, что все три утверждения эквивалентны.

Пусть теперь L/K — абелево расширение с группой Галуа $\mathfrak{g}$ и $\mathfrak{g}' \subset \mathfrak{g}$ — образ отображения взаимности. Если обозначить через K' подполе, соответствующее подгруппе $\mathfrak{g}'$, то транзитивность автоморфизма Фробениуса показывает, что $(\mathfrak{p}, K'/K) = 0$ для всех $\mathfrak{p}$, и цикл $\mathfrak{p}$ полностью распадается в K'. Если принять утверждение $3_r''$-A, то $K' = K$, откуда $\mathfrak{g}' = \mathfrak{g}$, что доказывает теорему 3_r. Импликация $3_r \Rightarrow 3_r''$-A очевидна.

26. Сведéние доказательств теорем 3, $3'$ и $3''$ к случаю кривых

В § 6 мы дадим непосредственное доказательство теоремы 3 в частном случае, когда V — *кривая* ($r = 1$). Покажем как с помощью индукции перейти к общему случаю. Воспользуемся формулировкой $3_r''$-A; другими словами, зададимся абелевым расширением F/K с группой Галуа $\mathfrak{g}$, удовлетворяющим условиям теоремы $3''$, и покажем, что $F = K$.

Обозначим через k' алгебраическое замыкание поля k в F. Наша задача сводится к изучению двух расширений F/Kk' и Kk'/K. Таким образом, нам надо разобрать два случая:

1) *Случай, когда* $F = Kk'$ *и* $[k' : k] = n$.

Надо показать, что если $n > 1$, то многообразие V *содержит рациональный цикл степени* $\not\equiv 0 \pmod{n}$. Заменяя V его открытым подмножеством, можем считать, что V — локально замкнутое подмногообразие проективного пространства $\mathbf{P}_m$. Применим к вложению $V \to \mathbf{P}_m$ следующую „теорему Бертини".

Лемма 11. *Пусть f: $V \to \mathbf{P}_m$ — регулярное отображение неприводимого многообразия V в проективное пространство, причем* $\dim f(V) \geqslant 2$. *Тогда в двойственном пространстве $\overset{*}{\mathbf{P}}_m$ существует алгебраическое подмножество Y, отличное от $\overset{*}{\mathbf{P}}_m$ и такое, что для всякой гиперплоскости $E \in \overset{*}{\mathbf{P}}_m - Y$ множество $f^{-1}(E)$ является неприводимым подмногообразием в V размерности $r-1$.*

Напомним идею доказательства. С помощью одной леммы из теории полей (см. Ленг [4], стр. 213) доказывается, что $f^{-1}(E)$ неприводимо для общей точки E пространства $\overset{*}{\mathbf{P}}_m$; далее с помощью координат Чжоу доказывается, что условие „$f^{-1}(E)$ неприводимо" алгебраично в точке E. Подробности см. у Зарисского [1] или у Матусаки [1].

Пусть теперь Y — подпространство в $\overset{*}{\mathbf{P}}_m$, существование которого утверждается в предыдущей лемме; Y определено над $\bar{k}$. Выберем целое число $s > 1$, взаимно простое с $n = [k' : k]$, и пусть k_s — композит всех расширений поля k, степень которых равна s. Имеем $k \subset k_s \subset \bar{k}$, причем поле k_s бесконечно. Согласно одной элементарной теореме (см. Бурбаки, Алгебра, IV, § 2, п. 5), существует гиперплоскость $E \subset \overset{*}{\mathbf{P}}_m$, рациональная над k_s и не входящая в Y. Многообразие $V' = V \cap E$ неприводимо и определено над расширением k'' поля k, степень которого есть s^a. В силу предположения индукции многообразие V' содержит рациональный над k'' цикл степени $d \not\equiv 0 \pmod{n}$. Сумма этого цикла и ему сопряженных над полем k определяет рациональный над k

цикл c многообразия V, степень которого $s^a d \not\equiv 0 \pmod{n}$, откуда и следует нужный результат для данного случая.

2) *Поля F и $K\bar{k}$ линейно свободны над K.*

В этом случае расширение F/K определяет накрытие $W \to V$; как и в первом случае, можно считать, что V погружено в проективное пространство $\mathbf{P}_m$. Применяя к отображению $W \to \mathbf{P}_m$ лемму 11, видим, что существует гиперплоскость E, определенная над конечным расширением k' поля k, для которой прообраз W' многообразия $V' = V \cap E$ является неприводимым (над $\bar{k}$) k'-многообразием. Степень накрытия $W' \to V'$ совпадает со степенью накрытия $W \to V$ (заметим, что накрытие $W \to V$ всегда можно считать неразветвленным, для чего стоит лишь уменьшить V). Если эта степень > 1, то предположение индукции показывает, что существует пара (P', Q') с $P' \in V'$, $Q' \in W'$, причем точка Q' проектируется в P', такая, что $k'(P') \neq k'(Q')$. Тем более имеем $k(P') \neq k(Q')$. Это показывает, что точка P' полностью не распадается в L/K, чем и завершается доказательство.

27. Ядро отображения взаимности

Пусть α: $V \to H_\alpha$ — максимальное отображение, определенное над k. Предположим, как и прежде, что α всюду регулярно на V. Пусть L/K — конечное абелево расширение типа α, т. е. расширение, содержащееся в расширении E_α/K. Его группа Галуа $\mathfrak{g}$ изоморфна факторгруппе $H_\alpha(k)/N$, где N обозначает подгруппу конечного индекса в $H_\alpha(k)$. Пусть k' — алгебраическое замыкание поля k в поле L; нормальная модель W многообразия V в L/K является k'-многообразием, для которого определена *группа циклов* $Z_{k'}(W)$. При помощи композиции

$$Z_{k'}(W) \to Z_{k'}(V) \xrightarrow{\mathrm{Tr}} Z_k(V)$$

получаем гомоморфизм группы циклов многообразия W в группу циклов многообразия V. Этот гомоморфизм играет роль следа и поэтому обозначается через Tr.

Предложение 20. *Ядро гомоморфизма взаимности $Z_k(V) \to \mathfrak{g}$ порождается ядром отображения* α: $Z_k(V) \to H_\alpha(k)$ *и образом отображения* Tr: $Z_{k'}(W) \to Z_k(V)$.

Очевидно, все сводится к тому, чтобы доказать, что образ группы $Z_{k'}(W)$ при композиции отображений $Z_{k'}(W) \to Z_k(V) \to H_\alpha(k)$ равен N. Ясно, что группа N содержит этот образ (след всегда содержится в ядре отображения взаимности). Покажем, что имеет место равенство. Для этого разберем отдельно следующие два случая:

1) $L = Kk'$, *где* k' — *конечное расширение поля* k.

В этом случае надо показать, что образ группы $Z_{k'}(V)$ в группе $H_\alpha(k)$ совпадает со множеством I_d элементов, степень которых делится на $d = [k' : k]$. Но гомоморфизм $Z_{k'}(V) \to H_\alpha(k)$ можно разложить на

$$Z_{k'}(V) \to H_\alpha(k') \xrightarrow{\mathrm{Tr}} H_\alpha(k).$$

По теореме 3′ первый гомоморфизм сюръективен и, согласно следствию предложения 5 из § 1, образ второго отображения совпадает с множеством I_d, откуда и следует наше утверждение.

2) *Поля* L *и* $K\bar{k}$ *линейно свободны.*

В этом случае расширению L/K соответствует накрытие $W \to V$, являющееся прообразом изогении $H' \to H_\alpha$, которая в свою очередь является фактор-изогенией изогении $\wp_n$: $G \to H_\alpha$. Группу N можно охарактеризовать тогда как образ группы $H'(k)$ в $H_\alpha(k)$; все сводится поэтому к доказательству того, что отображение α': $Z_k(W) \to H'(k)$ сюръективно. Последнее вытекает из теоремы 3 и следующей леммы:

Лемма 12. *Отображение* α': $W \to H'$ *максимально.*

Пусть $H'' \to H$ — такая изогения, что α' поднимается до отображения s: $W \to H''$. Покажем, что эта изогения тривиальна. Если $\mathfrak{g}$ обозначает ядро отображения $H' \to H_\alpha$, которое является также группой Галуа накрытия $W \to V$, то образ $s(\sigma \cdot w)$ в группе H' ($\sigma \in \mathfrak{g}$, $w \in W$) равен $\alpha'(w) + \sigma$. Отсюда следует, что отображение $w \to s(\sigma \cdot w) - s(w)$ принимает значения в ядре отображения $H'' \to H$, а следовательно, совпадает с постоянным отображением σ''. Отображение $\sigma \to \sigma''$ является изоморфизмом группы $\mathfrak{g}$ в группу G'', соответствующую пространству H''. Если положить $H''' = H''/\mathfrak{g}$, то отображение s определяет при переходе к фактору отображение $t\colon V \to H'''$. Так как отображение α максимально, это означает, что отображение $H'' \to H$ есть изоморфизм, а следовательно, изоморфизмом является и отображение $H'' \to H'$, что завершает доказательство.

§ 6. *Случай кривых*

Помимо предположений § 4 и 5, допустим, что V — *алгебраическая кривая* ($r = 1$), и обозначим через X определяемую однозначным образом неособую и полную модель поля $K = k(V)$.

28. Сравнение групп классов дивизоров с обобщенными якобиевыми многообразиями

Пусть $\mathfrak{m}$ — модуль на X, рациональный над полем k (см. гл. V), и $J_{\mathfrak{m}}$ — соответствующее обобщенное якобиево многообразие. Как известно (гл. V, п. 22), $J_{\mathfrak{m}}$ определено над k, а X снабжена каноническим отображением

$$\varphi_{\mathfrak{m}}\colon X \to H_{\mathfrak{m}}$$

в главное однородное пространство $H_{\mathfrak{m}}$ над группой $J_{\mathfrak{m}}$ (мы обозначаем это однородное пространство через $H_{\mathfrak{m}}$ вместо $J_{\mathfrak{m}}^{(1)}$ для согласования с обозначениями § 3).

Предложение 21. 1) *Отображение* $\varphi_{\mathfrak{m}}\colon X \to H_{\mathfrak{m}}$ *принадлежит множеству* L_k, *т. е. является максимальным отображением, определенным над* k.

2) *Когда* $\mathfrak{m}$ *пробегает множество модулей на* X, *рациональных над* k, *отображения* $\varphi_{\mathfrak{m}}$ *образуют кофинальную систему в* L_k.

Пусть $H' \to H_{\mathfrak{m}}$ — изогения. Предположим, что $\varphi_{\mathfrak{m}}$ поднимается до рационального отображения $\psi\colon X \to H'$. Так как отображение $\varphi_{\mathfrak{m}}$ регулярно вне носителя S модуля $\mathfrak{m}$, отображение ψ также будет регулярно вне S (гл. 3, предложение 14). Таким образом, ψ разлагается на $\theta \circ \varphi_{\mathfrak{m}}$, где

θ: $H_{\mathfrak{m}} \to H'$ — морфизм. Композиция $H_{\mathfrak{m}} \xrightarrow{\theta} H' \to H_{\mathfrak{m}}$ тождественна на $\varphi_{\mathfrak{m}}(X)$, а следовательно, и на всем $H_{\mathfrak{m}}$. Это показывает, что изогения $H' \to H_{\mathfrak{m}}$ тривиальна. Так как отображение $\varphi_{\mathfrak{m}}$ определено над k, первое утверждение доказано.

Докажем второе утверждение. Пусть α: $X \to H_{\alpha}$ — произвольный элемент из L_k. Известно, что α обладает модулем $\mathfrak{m}$. После замены в случае необходимости $\mathfrak{m}$ на сумму ему сопряженных модулей можно считать $\mathfrak{m}$ рациональным над k. Предложение 13 из гл. V (или теорема 2 гл. V вместе с леммой 6 из § 3) показывает, что $\varphi_{\mathfrak{m}} \geqslant \alpha$. откуда и следует утверждение 2).

К прежним обозначениям присоединим еще одно. Обозначим через $C_{\mathfrak{m}}(k)$ *группу классов рациональных над k дивизоров по модулю $\mathfrak{m}$-эквивалентности.* Дивизор D, рациональный над k и равный нулю на носителе S модуля $\mathfrak{m}$, $\mathfrak{m}$-эквивалентен нулю, если $D = (g)$, где $g \in K^*$ и $g \equiv 1 \pmod{\mathfrak{m}}$. Для каждого расширения k'/k можно аналогично определить группу $C_{\mathfrak{m}}(k')$. Группа Галуа $\mathfrak{g}$ расширения k'/k естественным образом действует на $C_{\mathfrak{m}}(k)$.

Лемма 13. *Каноническое отображение группы $C_{\mathfrak{m}}(k)$ в $C_{\mathfrak{m}}(k')$ инъективно, а его образ совпадает с множеством элементов группы $C_{\mathfrak{m}}(k')$, инвариантных относительно $\mathfrak{g}$.*

Пусть $K^*_{\mathfrak{m}}$ — подполе поля K^*, состоящее из элементов $g \equiv 1 \pmod{\mathfrak{m}}$, и $D_{\mathfrak{m}}$ — группа рациональных дивизоров, равных нулю на S. Обозначим через $K^*_{\mathfrak{m}}$ и $D'_{\mathfrak{m}}$ группы, соответствующие полю k'. Если $\mathfrak{m} \neq 0$, то соотношение $(g) = 0$ означает $g = 1$ для $g \in K'_{\mathfrak{m}}$. Таким образом, имеет место точная последовательность $\mathfrak{g}$-модулей

$$0 \to K'^*_{\mathfrak{m}} \to D'_{\mathfrak{m}} \to C_{\mathfrak{m}}(k') \to 0. \qquad (*)$$

Ясно, что $H^0(\mathfrak{g}, K'^*_{\mathfrak{m}}) = K^*_{\mathfrak{m}}$ и $H^0(\mathfrak{g}, D'_{\mathfrak{m}}) = D_{\mathfrak{m}}$. Точная последовательность групп когомологий, соответствующая (*), имеет следующий вид:

$$0 \to K^*_{\mathfrak{m}} \to D_{\mathfrak{m}} \to H^0(\mathfrak{g}, C_{\mathfrak{m}}(k')) \to H^1(\mathfrak{g}, K'_{\mathfrak{m}}),$$

или

$$0 \to C_{\mathfrak{m}}(k) \to H^{\prime}(\mathfrak{g}, C_{\mathfrak{m}}(k')) \to H^1(\mathfrak{g}, K'^*_{\mathfrak{m}}).$$

Для доказательства леммы 13 достаточно, следовательно, доказать, что $H^1(\mathfrak{g}, K'^*_{\mathfrak{m}}) = 0$ — результат, аналогичный классической „теореме 90“ [1]). Приведем, впрочем, доказательство этой теоремы для нашего случая. Выберем $a \in k'$, для которого $\mathrm{Tr}_{k'/k}(a) = 1$; если f_σ — 1-коцикл со значениями в $K'^*_{\mathfrak{m}}$, то положим

$$g = \sum_{\sigma \in \mathfrak{g}} a^\sigma f_\sigma.$$

Так как можно написать $g = 1 + \sum a^\sigma (f^\sigma - 1)$, то $g \equiv 1 \pmod{\mathfrak{m}}$; с другой стороны, непосредственное вычисление показывает, что $f = g/g^\sigma$. Поэтому $H^1(\mathfrak{g}, K'^*_{\mathfrak{m}}) = 0$.

В случае $\mathfrak{m} = 0$ имеем $K^*_{\mathfrak{m}} = K^*$, и ядро отображения $K'^* \to D'$ совпадает с k'^*. Теперь нужно слегка изменить предыдущие рассуждения, используя тот факт, что $H^1(\mathfrak{g}, k'^*) = H^r(\mathfrak{g}, k'^*) = 0$, поскольку k' — конечное поле.

Если D — дивизор, равный нулю на S, то его образ при отображении $\varphi_{\mathfrak{m}}$ есть вполне определенный элемент группы $H_{\mathfrak{m}}(\bar{k})$, ассоциированной с однородным пространством $H_{\mathfrak{m}}$.

Предложение 22. *Отображение $\varphi_{\mathfrak{m}}$ определяет изоморфизм группы $C_{\mathfrak{m}}(k)$ на группу $H_{\mathfrak{m}}(k)$.*

Известно (гл. V, теорема 1), что отображение $\varphi_{\mathfrak{m}}$ определяет изоморфизм группы $C_{\mathfrak{m}}(\bar{k})$ на $H_{\mathfrak{m}}(\bar{k})$. Если обозначить через G группу Галуа расширения k'/k, то лемма 13 показывает, что группа $C_{\mathfrak{m}}(k)$ отождествляется с подгруппой группы $C_{\mathfrak{m}}(\bar{k})$, образованной элементами, инвариантными относительно G. С другой стороны, очевидно, что этим же свойством обладает и $H_{\mathfrak{m}}(k)$, откуда и следует искомое утверждение.

Следствие. *Теоремы* 3, 3′ *и* 3″ *из* п. 25 *справедливы для алгебраической кривой.*

[1]) Гильберта. — *Прим. ред.*

Докажем теорему 3′. Поскольку отображения $\varphi_{\mathfrak{m}}$ кофинальны в L_k, дело сводится к доказательству того, что для любой модели V поля K отображение

$$\varphi_{\mathfrak{m}}\colon Z_k(V) \to H_{\mathfrak{m}}(k)$$

сюръективно. Так как многообразие V бирегулярно изоморфно кривой X вне конечного множества S ее точек, то надо доказать, что если S' — конечное подмножество в X, содержащее S, то всякий элемент $x \in H_{\mathfrak{m}}(k)$ является образом при отображении $\varphi_{\mathfrak{m}}$ дивизора, рационального над k и равного нулю на S. Согласно предложению 22, во всяком случае имеем $x = \varphi_{\mathfrak{m}}(D)$, где $D = 0$ на S. В силу теоремы о независимости нормирований можно найти функцию $g \in K^*$, такую, что $g \equiv 1 \pmod{\mathfrak{m}}$ и $v_P(g) = v_P(D)$ для всех $P \in S' - S$. Дивизор $D' = D - (g)$ как раз и является прообразом элемента x при отображении $\varphi_{\mathfrak{m}}\colon Z_k(V) \to H_{\mathfrak{m}}(k)$.

[*Другой способ*: выберем модуль $\mathfrak{m}'$, рациональный над k, такой, что его носитель содержит S' и $\mathfrak{m}' \geqslant \mathfrak{m}$. Согласно п. 16, элемент $x \in H_{\mathfrak{m}}(k)$ является образом элемента $x' \in H_{\mathfrak{m}'}(k)$, который в силу предложения 22 является образом дивизора D', рационального над k и равного нулю на S; тем более имеем $\varphi_{\mathfrak{m}}(D') = x$.]

29. Группа классов иделей

Напомним сначала определение этой группы.

Пусть I — группа $\bar{k}$-иделей кривой X, т. е. группа, образованная системами $(g_P)_{P \in X}$, $g_P \in \hat{L}_P$, $v_P(g_P) = 0$ для почти всех точек $P \in X$ (через L обозначено поле $K\bar{k}$, а через $\hat{L}_P$ — его пополнение по топологии, определяемой v_P). На группе I действует группа G k-автоморфизмов поля $\bar{k}$, инвариантные элементы которой образуют группу $I(k)$ *k-иделей*. Для того чтобы элемент (g_P) принадлежал группе $I(k)$, необходимо и достаточно, чтобы $g_P \in \hat{K}_P$ и $g_P = g_{P'}$ для всех точек P', сопряженных P над полем k. Группа K^* отождествляется с подгруппой группы $I(k)$, а факторгруппа называется *группой классов k-иделей* (над k) и обозначается через $C(k)$.

Если $\mathfrak{m} = \sum n_P P$ — рациональный над k модуль, то через $I_{\mathfrak{m}}(k)$ обозначается подгруппа группы $I(k)$, образованная такими иделями (g_P), для которых $v_P(1 - g_P) \geqslant n_P$ при $P \in \operatorname{Supp}(\mathfrak{m})$ и $v_P(g_P) = 0$ при $P \notin \operatorname{Supp}(\mathfrak{m})$. Таким образом, получается возрастающее фильтрованное семейство подгрупп группы $I(k)$, причем, как легко проверяется, группа $C(k)$ отождествляется с проективным пределом групп $I(k)/K^* I_{\mathfrak{m}}(k)$. С другой стороны, имеем $I(k)/K^* I_{\mathfrak{m}}(k) = C_{\mathfrak{m}}(k)$, а предложение 22 позволяет отождествить группу $C_{\mathfrak{m}}(k)$ с $H_{\mathfrak{m}}(k)$. Так как отображения $\varphi_{\mathfrak{m}}$ образуют кофинальную систему в L_k, проективный предел групп $H_{\mathfrak{m}}(k)$ совпадает с группой $A(K)$ классов циклов кривой X (см. п. 16). Другими словами, справедливо

Предложение 23. *Группа $C(k)$ классов иделей кривой X канонически изоморфна группе $A(k)$ классов циклов X.*

Теорема 1 из п. 16 позволяет перенести основную теорему теории полей классов на поле функций от одной переменной.

Теорема 4. *Группа классов иделей кривой X канонически изоморфна (модифицированной) группе Галуа максимального абелева расширения поля K.*

Разумеется, имеет место также и тот факт, что этот изоморфизм задается отображением взаимности.

Кроме того, получаются результаты относительно ведущего модуля конечного абелева расширения L/K. Если $\mathfrak{g}$ обозначает группу Галуа этого расширения, то $\mathfrak{g} = C(k)/N = I(k)/N'$, где N' — открытая подгруппа группы $I(k)$, содержащая K^*. Ведущий модуль (в арифметическом смысле) расширения L/K совпадает с наименьшим модулем $\mathfrak{m}$, таким, что $I_{\mathfrak{m}}(k) \subset N'$. Остается лишь добавить, что этот модуль является наименьшим модулем $\mathfrak{m}$, для которого $\mathfrak{g}$ изоморфна факторгруппе $C_{\mathfrak{m}}(k)$. Так как $C_{\mathfrak{m}}(k) = H_{\mathfrak{m}}(k)$—группа Галуа поля $E_{\mathfrak{m}}$, определенного с помощью максимального отображения $\varphi_{\mathfrak{m}}$, мы видим, что этот ведущий модуль совпадает с наименьшим модулем $\mathfrak{m}$, таким, что расширение L/K имеет „тип $\varphi_{\mathfrak{m}}$“ в смысле п. 19. Наконец, сравнивая эти результаты с предложением 11, получаем:

Предложение 24. *Ведущий модуль (в арифметическом смысле) конечного абелева расширения L/K совпадает с ведущим модулем (в геометрическом смысле) расширения $L\bar{k}/K\bar{k}$. Его носитель есть множество точек ветвления расширения L/K.*

30. Явные законы взаимности

Пусть L/K — конечное абелево расширение с группой Галуа $\mathfrak{g}$. Согласно теореме 4, имеем сюръективный гомоморфизм $C(k)\to\mathfrak{g}$, откуда получаем непрерывный гомоморфизм $I(k)\to\mathfrak{g}$. Если $\mathfrak{p}$ — простой рациональный цикл на X и g — элемент из поля $\widehat{K}_{\mathfrak{p}}$ пополнения поля K по топологии, определяемой кольцом нормирований $\mathfrak{O}_{\mathfrak{p}}$, то можно рассмотреть идель g, компонента которого в точке P равна g при $P\in\mathfrak{p}$ и 1 при $P\notin\mathfrak{p}$. Обозначим его образ в группе $\mathfrak{g}$ через $(L/K,g)_P$. Так как каждый идель сравним по модулю $I_{\mathfrak{m}}(k)$ с произведением иделей предыдущего типа, то *знание локальных символов $(L/K, g)_P$ дает возможность определять гомоморфизм группы $C(k)$ классов иделей в группу Галуа* $\mathfrak{g}$. Если $\mathfrak{m}$ — ведущий модуль расширения L/K, а S — его носитель, то:

1) $(L/K,\ gg')_{\mathfrak{p}}=(L/K,\ g)_{\mathfrak{p}}+(L/K,\ g')_{\mathfrak{p}}$;

2) $(L/K,\ g)_{\mathfrak{p}}=0$, *если* $\mathfrak{p}\subset S$ *и* $g\equiv 1 \pmod{\mathfrak{m}}$ *в* $\mathfrak{p}$;

3) $(L/K,\ g)_{\mathfrak{p}}=v_{\mathfrak{p}}(g)(\mathfrak{p},\ L/K)$, *если* $\mathfrak{p}\subset X-S$;

4) $\sum\limits_{\mathfrak{p}}(L/K,\ g)_{\mathfrak{p}}=0$ *для всех* $g\in K^*$.

Свойство 1) выражает тот факт, что отображение $I(k)\to\mathfrak{g}$ гомоморфно; свойства 1) и 2)—что этот гомоморфизм равен нулю на $I_{\mathfrak{m}}(k)$ и определяет при переходе к фактору гомоморфизм группы дивизоров, равных нулю на S, в группу $\mathfrak{g}$, причем этот гомоморфизм совпадает с отображением взаимности; наконец, свойство 4) показывает, что отображение $I(k) \to \mathfrak{g}$ равно нулю на K^*.

Таким образом, мы видим, что $(L/K, g)_{\mathfrak{p}}$ играет роль *локального символа* (в смысле гл. III, § 1) по отношению к автоморфизму Фробениуса $(\mathfrak{p}, L/K)$.

Уточним это для одного частного случая.

Предположим, что расширение L/K является прообразом изогении $G' \to G$ при рациональном отображении $f\colon X \to G$ (разумеется, предполагается, что G, G' и f определены над k, а изогения $G' \to G$ абелева над k). Согласно предположению 6 из § 1, изогения $G' \to G$ является факторизогенией изогении $\wp\colon G \to G$. Обозначим через π канонический гомоморфизм группы G_k на $\mathfrak{g}$.

Предложение 26. *Для любого простого рационального цикла* $\mathfrak{p}$ *и любой функции* $g \in K^*$ *имеем*

$$(L/K, g)_{\mathfrak{p}} = \pi\left(\sum_{P \in \mathfrak{p}} (f, g)_P\right). \qquad (*)$$

[Можно было бы брать g из $\widehat{K}^*_{\mathfrak{p}}$, при этом ничего не изменилось бы согласно свойству (3) локальных символов.]

Пусть $S' \supset S$ — множество точек, в которых отображение f нерегулярно. Если цикл $\mathfrak{p}$ равен нулю на S', то рассуждения п. 24 показывают, что

$$(\mathfrak{p}, L/K) = f(\mathfrak{p}) = \sum_{P \in \mathfrak{p}} f(P),$$

откуда получается формула (*) для данного случая.

Если $\mathfrak{p} \subset S'$, то выбираем вспомогательную функцию $g_1 \in K^*$, приближающую g в точках $\mathfrak{p}$ и 1 в точках $S' - \mathfrak{p}$. Применяя к этой функции только что доказанный результат и пользуясь свойством 4), получаем требуемое соотношение.

Примеры. 1. *Расширения Артина—Шрейера.* Пусть L/K — циклическое расширение степени p; выберем образующую группы Галуа, отождествляя последнюю с группой $F_p = \mathbf{Z}/p\mathbf{Z}$. Расширение L/K является тогда прообразом изогении $x \to x^p - x$ группы G_a при рациональном отображении $f\colon X \to G_a$. Вычислим явно локальный символ $(L/K, g)_{\mathfrak{p}}$, который мы будем также обозначать через $(f, g)_{\mathfrak{p}}$. Воспользуемся предложением 26; гомоморфизм $\pi\colon G_k \to \mathfrak{g}$ сводится в данном случае к операции следа $\mathrm{Tr}_{k/\mathbf{F}_p}$: $k \to \mathbf{F}_p$. С другой стороны, как известно (гл. III, предложение 5), $(f, g)_P = \mathrm{Res}_P(f\,dg/g)$, что является элементом поля $k(P)$. Отсюда следует

$$(f,\ g)_P = \mathrm{Tr}_{k/\mathbf{F}_p}\left(\sum_{P \in \mathfrak{p}} \mathrm{Res}_P\left(\frac{f\,dg}{g}\right)\right) = \\ = \mathrm{Tr}_{k/\mathbf{F}_p}\left(\mathrm{Tr}_{k(P)/k}\,\mathrm{Res}_P\left(\frac{f\,dg}{g}\right)\right),$$

откуда наконец получаем

$$(f,\ g)_P = \mathrm{Tr}_{k(P)/\mathbf{F}_p}\left(\mathrm{Res}_P\left(\frac{f\,dg}{g}\right)\right), \quad \text{где} \quad P \in \mathfrak{p}.$$

2. *Расширение Куммера.* Предположим, что L/K — циклическое расширение степени n, взаимно простой с характеристикой, и что поле k содержит первообразный корень степени n из единицы (другими словами, что q делится на $n-1$). Отождествим группу Галуа $\mathfrak{g}$ с группой корней степени n из единицы. Расширение L/K является прообразом изогении $x \to x^n$ группы G_m при рациональном отображении f: $X \to G_m$. Соответствующий локальный символ $(L/K,\ g)_{\mathfrak{p}}$ обозначается через $(f,\ g)_{\mathfrak{P}}$; он совпадает с *символом норменного вычета* Гильберта и легко вычисляется с помощью предложения 26. Гомоморфизм π: $G_k \to \mathfrak{g}$ сводится к отображению $x \to x^{(q-1)/n}$ поля k на группу корней степени n из единицы. Значения же локального символа $(f,\ g)_{\mathfrak{p}}$ известны (гл. III, предложение 6). Итак, получаем

$$(f,\ g)_{\mathfrak{p}} = \left(N_{k(P)/k}\,(-1)^{\alpha\beta}\,\frac{f^{\beta}}{g^{\alpha}}\,(p)\right)^{(q-1)/n},$$

$$\text{где } \alpha = v_P(f),\ \beta = v_{\mathfrak{p}}(g).$$

Эти формулы были получены Шмидом [1].

§ 7. *Когомологии*

Известно, что теория полей классов была обогащена недавно когомологическими свойствами, которые находят концентрированное выражение в следующем утверждении.

(*) Отображение, ставящее в соответствие каждому полю (чисел или функций над конечным полем) группу иделей, является „формацией классов“ в смысле Артина - Тейта.

Интересно выяснить, удовлетворяет ли условию (*) „группа классов циклов“, которую мы определили в § 4. Известно, что в случае размерности 1 ответ положительный. Мы увидим, впрочем, что это немедленно следует из теоремы 4 § 6. Наоборот, в размерностях > 1, как мы убедимся, группа классов циклов *не является* формацией классов.

31. Критерий существования формаций классов

Вернемся к ситуации § 4 и обозначим через $K = k(V)$ поле алгебраических функций над конечным полем k. Пусть E и F — два конечных расширения поля K, причем F — расширение Галуа поля E с группой Галуа $\mathfrak{g}_{F/E}$. Обозначим через F_a (соответственно E_a) максимальное абелево расширение поля F (соответственно E), а через $A(F)$ (соответственно $A(E)$) — его модифицированную группу Галуа (см. п. 16).

Расширение F_a/E является расширением Галуа и содержит расширение $E\bar{k}/k$. Обозначим через $\hat{G}_{F/E}$ его группу Галуа (в обычном смысле), а через $G_{F/E}$ — его модифицированную группу Галуа (см. п. 16); по определению $G_{F/E}$ — подгруппа группы $\hat{G}_{F/E}$, состоящая из элементов σ, для которых существует такое $n \in \mathbf{Z}$, что $\sigma(a) = a^{q^n}$ при $a \in \bar{k}$. Группа $G_{F/E}$ топологизируется таким образом, чтобы группа Галуа $G^0_{F/E}$ расширения $F_a/E\bar{k}$ была открытым подмножеством. Эта группа обладает свойствами, очень близкими к свойствам группы Галуа; ее замкнутые подгруппы соответствуют полям L, для которых $F_a \supset L \supset E$, причем $L \cap \bar{k}$ равно либо $\bar{k}$, либо конечному расширению поля k. Группа $\hat{G}_{F/E}$ получается пополнением группы $G_{F/E}$ по топологии, определяемой замкнутыми подгруппами конечного индекса.

Группа $G_{F/E}$ является расширением группы $A(F)$ с помощью группы $\mathfrak{g}_{F/E}$; этому расширению соответствует класс когомологий $u_{F/E} \in H^2(\mathfrak{g}_{F/E}, A(F))$. Уточним теперь формулировку (*) следующим образом.

Определение 6. Говорят, что отображение $E \to A(E)$ является *формацией классов*, если для всякой пары F/E, где $F \supset E \supset K$, причем F конечно над K и является расширением Галуа поля E, имеем:

1) $H^1(\mathfrak{g}_{F/E}, A(F)) = 0$;

2) $H^2(\mathfrak{g}_{F/E}, A(F))$ — циклическая группа порядка $[F: E]$, порождаемая элементом $u_{F/E}$.

Замечание. Пусть $\hat{A}(F)$—группа Галуа (в обычном смысле) расширения F_a/F. Факторгруппа $\hat{A}(F)/A(F)$ изоморфна группе $\hat{\mathbf{Z}}/\mathbf{Z}$, *делимой и не имеющей кручения*; отсюда следует, что отображение $E \to \hat{A}(E)$ *является формацией классов тогда и только тогда, когда таковым является отображение* $E \to A(E)$. Более того, так как группа $\hat{A}(F)$ компактна, то компактны и группы $H^q(\mathfrak{g}_{F/E}, \hat{A}(F))$. Это показывает, что группы $H^q(\mathfrak{g}_{F/E}, A(F))$, снабженные индуцированной с $A(F)$ топологией, суть отделимые группы.

Вернемся теперь к расширению

$$1 \to A(F) \to G_{F/E} \to \mathfrak{g}_{F/E} \to 1.$$

Группа $A(F)$ имеет конечный индекс в группе $G_{F/E}$. Но, как известно, если H—абелева подгруппа конечного индекса в G, то можно определить гомоморфизм T: $G/G' \to H$, называемый *перенесением* (G' обозначает коммутатор группы G). Напомним определение этого гомоморфизма (подробности см. у Цассенхауза [1], гл. V, и Картана и Эйленберга [1], гл. XII). Пусть G/H — однородное пространство правых смежных классов группы G по H. Выберем сечение s: $G/H \to G$; если $g \in G$ и $x \in G/H$, то $s(x \cdot g) \equiv s(x) \cdot g \pmod{H}$, откуда следует существование элемента $h_{g, x} \in H$, такого, что $s(x) \cdot g = h_{g, x} \cdot s(xg)$. Положим тогда

$$T(g) = \prod_{x \in G/H} h_{g, x}.$$

Непосредственное вычисление показывает, что получается гомоморфизм группы G/G' в группу H, не зависящий от выбора сечения s.

Таким образом, мы получили гомоморфизм $T\colon G_{F/E}/G'_{F/E} \to A(F)$. Этот гомоморфизм непрерывен, а его ядро содержит замыкание $G^c_{F/E}$ группы $G'_{F/E}$. Но так как E_a — наибольшее абелево расширение поля E, содержащееся в F_a, подгруппа $G^c_{F/E}$ замкнута в группе $G_{F/E}$ и соответствует расширению E_a, а следовательно, $A(F) = G_{F/E}/G^c_{F/E}$.

В результате мы получаем непрерывный гомоморфизм

$$\mathrm{Ver}\colon\ A(E) \to A(F).$$

Образ этого гомоморфизма содержится в группе $H^0(\mathfrak{g}_{F/E}, A(F))$, состоящей из элементов множества $A(F)$, инвариантных относительно группы $\mathfrak{g}_{F/E}$. Более того, композиция

$$A(F) \to A(E) \to A(F)$$

совпадает со *следом* (первый гомоморфизм был определен в п. 21).

Теорема 5. *Для того чтобы отображение $E \to A(E)$ было формацией классов, необходимо и достаточно, чтобы для любой пары F/E, удовлетворяющей условиям определения 6, гомоморфизм*

$$\mathrm{Ver}\colon\ A(E) \to A(F)$$

был инъективен, а его образ был изоморфен группе $H^0(\mathfrak{g}_{F/E}, A(F))$.

Эта теорема неявно встречается в работах Вейля [7] и Хохшильда и Накаямы [1]; явно же она была получена Артином и Тейтом (не опубликовано). Необходимость условия фигурирует также у Кавады [2]. Приведем набросок доказательства.

Предположим, что $A(E)$ — формация классов. Если обозначать через $\hat{H}^q(\mathfrak{g})$ *модифицированную* группу когомологий $\mathfrak{g}$ (см. Картан — Эйленберг [1], гл. XII)[1]), то теорема Тейта [83] показывает, что

$$\hat{H}^q(\mathfrak{g}_{F/E}, A(F)) = \hat{H}^{q-2}(\mathfrak{g}_{F/E}, \mathbf{Z}) \quad \text{для всех} \quad q \in \mathbf{Z}.$$

[1]) Через $\hat{H}^q(\mathfrak{g})$ обозначаются группы когомологий, получающиеся из полной производной последовательности для $\mathfrak{g}$. — *Прим. ред.*

Положим для упрощения записи $\mathfrak{g} = \mathfrak{g}_{F/E}$; в частности, имеем

$$\hat{H}^{-1}(\mathfrak{g},\ A(F)) = \hat{H}^{-3}(\mathfrak{g},\ \mathbf{Z}) = H_2(\mathfrak{g},\ \mathbf{Z})$$

и

$$\hat{H}^0(\mathfrak{g},\ A(F)) = \hat{H}^{-2}(\mathfrak{g},\ \mathbf{Z}) = H_1(\mathfrak{g},\ \mathbf{Z}) = \mathfrak{g}/\mathfrak{g}'.$$

Но, согласно определению групп $\hat{H}^{-1}$ и $\hat{H}^0$, имеет место точная последовательность

$$0 \to \hat{H}^{-1}(\mathfrak{g},\ A(F)) \to H_0(\mathfrak{g},\ A(F)) \to$$
$$\to H^0(\mathfrak{g},\ A(F)) \to \hat{H}^0(\mathfrak{g},\ A(F)) \to 0,$$

которую можно переписать в следующем виде:

$$H_2(\mathfrak{g},\ \mathbf{Z}) \to H_0(\mathfrak{g},\ A(F)) \to H^0(\mathfrak{g},\ A(F)) \to \mathfrak{g}/\mathfrak{g}' \to 0. \quad (^{**})$$

С другой стороны, точная последовательность групп когомологий, соответствующая расширению $G_{F/E}/A(F) = \mathfrak{g}$, дает (см. Картан — Эйленберг [1], стр. 358)

$$H_2(\mathfrak{g},\ z) \to H_0(\mathfrak{g},\ A(F)) \to G_{F/E}/G'_{F/E} \to \mathfrak{g}/\mathfrak{g}' \to 0. \quad (^{***})$$

Из этой точной последовательности и из того факта, что $H_0(\mathfrak{g},\ A(F))$ — отделимая топологическая группа (см. выше), следует, что $G'_{F/E}$ *замкнута* в $G_{F/E}$, откуда имеем

$$G_{F/E}/G'_{F/E} = A(E).$$

Сравнивая теперь точные последовательности (**) и (***) и принимая во внимание, что перенесение Ver: $A(E) \to H^0(\mathfrak{g},\ A(F))$ удовлетворяет необходимым условиям согласованности, получаем, что перенесение биективно. Это доказывает первую часть теоремы.

Остается доказать *достаточность* условия теоремы 5; это будет сделано в следующих двух пунктах.

32. Некоторые свойства класса когомологий

Лемма 14. *Если $F \supset F' \supset E$, где F - конечное расширение Галуа над E, то образ $u_{F/E}$ в группе $H^2(\mathfrak{g}_{F/F'},\ A(F))$ совпадает с $u_{F/E}$.*

(Речь идет о гомоморфизме $H^2(\mathfrak{g}_{F/E}, A(F)) \to H^2(\mathfrak{g}_{F/F'}, A(F))$, который индуцируется вложением $\mathfrak{g}_{F/F'} \to \mathfrak{g}_{F/E'}$)

Из „башни“ полей $E \subset F' \subset F \subset F_a$ следует коммутативная диаграмма:

$$\begin{array}{ccccccccc} 1 & \to & A(F) & \to & G_{F/F'} & \to & \mathfrak{g}_{F/F'} & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & A(F) & \to & G_{F/E} & \to & \mathfrak{g}_{F/E} & \to & 1 \end{array}$$

Отсюда немедленно вытекает

Лемма 15. *Пусть $\mathfrak{g}$ — некоторая группа, $\mathfrak{f}$ — ее инвариантная подгруппа конечного порядка n и $\sigma = \sum_{x \in \mathfrak{f}} x$ — элемент групповой алгебры $\mathbf{Z}[\mathfrak{g}]$ группы $\mathfrak{g}$. Если M — $\mathfrak{g}$-модуль, то эндоморфизм группы $H^q(\mathfrak{g}, M)$, определенный с помощью отображения* $\sigma\colon M \to M$, совпадает с умножением на n.

Поскольку $\mathfrak{f}$ инвариантна в $\mathfrak{g}$, элемент σ равен сумме классов, а следовательно, принадлежит *центру* алгебры $\mathbf{Z}[\mathfrak{g}]$; более того, образ σ при гомоморфизме „пополнения“ $\mathbf{Z}[\mathfrak{g}] \to \mathbf{Z}$ равен n. Лемма вытекает теперь из формулы определения групп когомологий (Картан и Эйленберг [1], гл. X)

$$H^q(\mathfrak{g}, M) = \mathrm{Ext}^q_{\mathbf{Z}[\mathfrak{g}]}(\mathbf{Z}, M).$$

[Здесь применяется то рассуждение, которое в теории алгебр Ли показывает, что оператор Казимира тривиально действует на когомологиях.]

Лемма 16. *Если $F \supset F' \supset E$, где F и F' — расширения Галуа над E, то образ u' элемента $u_{F'/E}$ в группе $H^2(\mathfrak{g}_{F/E}, A(F))$ совпадает с $[F : F']\, u_{F/E}$.*

(Речь идет о гомоморфизме $H^2(\mathfrak{g}_{F'/E}, A(F')) \to H^2(\mathfrak{g}_{F/E}, A(F))$, который индуцируется гомоморфизмами $\mathfrak{g}_{F/E} \to \mathfrak{g}_{F'/E}$ и $\mathrm{Ver}\colon A(F') \to A(F)$.)

Опять имеем коммутативную диаграмму

$$\begin{array}{ccccccccc} 1 & \to & A(F) & \to & G_{F/E} & \to & \mathfrak{g}_{F/E} & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & A(F') & \to & G_{F'/E} & \to & \mathfrak{g}_{F'/E} & \to & 1 \end{array}$$

Из нее следует, что элементы $u_{F/E}$ и $u_{F'/E}$ имеют одинаковый образ u'' в группе $H^2(\mathfrak{g}_{F/E}, A(F'))$. Но образ элемента u'' в группе $H^2(\mathfrak{g}_{F/E}, A(F))$ при гомоморфизме Ver: $A(F') \to A(F)$ равен u'. Отсюда следует, что u' получается из $u_{F/E}$ при гомоморфизме $A(F) \to A(F') \to A(F)$, который совпадает со взятием следа относительно операций из $\mathfrak{g}_{F/F'}$. Применяя лемму 15 к инвариантной подгруппе $\mathfrak{g}_{F/F'}$ группы $\mathfrak{g}_{F/E}$, получаем $u' = [F: F']\, u_{F/E}$.

33. Доказательство теоремы 5

Надо доказать *достаточность* условия теоремы 5. Предположим, что для каждого конечного расширения Галуа F/E, где E — конечное расширение поля K, гомоморфизм перенесения Ver: $A(E) \to A(F)$ инъективен, а его образ совпадает с множеством элементов группы $A(F)$, инвариантных относительно группы $\mathfrak{g}_{F/E}$.

Лемма 17. $H^1(\mathfrak{g}_{F/E}, A(F)) = 0$.

Предположение о гомоморфизме перенесения позволяет отождествить группу $A(E)$ с подгруппой группы $A(F)$, что мы и будет делать в дальнейшем. Обычное рассуждение с использованием силовских подгрупп (см., например, Шевалле [2] или Хохшильд и Накаяма [1]) показывает, что достаточно доказать тривиальность группы $H^1(\mathfrak{g}_{F/E}, A(F))$ в случае, когда $\mathfrak{g}_{F/E}$ — циклическая группа. Пусть σ — образующая этой группы. Тогда имеем расширение

$$1 \to A(F) \to G_{F/E} \to \mathfrak{g}_{F/E} \to 1,$$

и коммутатор $G'_{F/E}$ группы $G_{F/E}$ совпадает с подгруппой группы $A(F)$, образованной элементами вида $b - \sigma(b)$, где

$b \in A(F)$. По предположению перенесение Ver: $G_{F/E}/G'_{F/E} \to$ $\to A(F)$ инъективно. Следовательно, если $a \in A(F)$ — элемент, след которого равен нулю, то $a \in G'_{F/E}$, т. е. $a = b - \sigma(b)$, что эквивалентно тривиальности группы $H^1(\mathfrak{g}_{F/E}, A(F))$.

Лемма 18. *Порядок элемента* $u_{F/E}$ *равен* $[F: E]$.

Известно, что порядок $u_{F/E}$ *делит* $[F: E]$; остается доказать, что он не меньше $[F: E]$.

Предположим сначала, что F/E — циклическое расширение простого порядка l. Если порядок элемента $u_{F/E}$ отличен от l, то $u_{F/E} = 0$; другими словами, группа $G_{F/E}$ является *полупрямым произведением* группы $\mathfrak{g}_{F/E}$ на $A(F)$. В этом случае нетрудно явно определить гомоморфизм перенесения: он равен нулю на группе $\mathfrak{g}_{F/E}$ (отождествленной с подгруппой группы $G_{F/E}$) и совпадает со следом на группе $A(F)$. С другой стороны, поскольку $\mathfrak{g}_{F/E}$ — циклическая группа, коммутатор группы $G_{F/E}$, как мы видели, содержится в $A(F)$ и, значит, не содержит группу $\mathfrak{g}_{F/E}$. Гомоморфизм перенесения

$$\text{Ver: } G_{F/E}/G'_{F/E} \to A(F)$$

имеет, следовательно, ненулевое ядро, что противоречит сделанному предположению.

Пусть теперь степень расширения F/E равна l^n. Применим индукцию по n. Если порядок элемента $u_{F/E}$ отличен от l^n, то $l^{n-1}u_{F/E} = 0$. В силу свойств p-групп существует подполе F' поля F, циклическое и степени l над E. Тогда $[F: F'] = l^{n-1}$ и лемма 16 показывает, что образ $u_{F'/F}$ в группе $H^2(\mathfrak{g}_{F/E}, A(F))$ равен нулю. Но лемма 17 вместе с хорошо известной точной последовательностью показывает, что гомоморфизм $H^2(\mathfrak{g}_{F'/E}, A/F') \to H^2(\mathfrak{g}_{F/E}, A(F))$ инъективен. Следовательно, $u_{F'/E} = 0$, что противоречит только что доказанному.

Общий случай получается отсюда немедленно, если использовать силовские подгруппы $\mathfrak{g}_{F/E}$, а также лемму 14.

Предыдущая лемма показывает, что группа $H^2(\mathfrak{g}_{F/E}, A(F))$ содержит циклическую подгруппу порядка $[F: E]$. Для завершения доказательства теоремы 5 достаточно, таким образом, доказать следующий результат.

Лемма 19. *Порядок группы* $H^2(\mathfrak{g}_{F/E}, A/F))$ *не превышает* $[F:E]$.

Снова можно ограничиться случаем циклического расширения F/E простого порядка l. Пусть B — подмножество множества $A(F)$, образованное элементами, инвариантными относительно группы $\mathfrak{g}_{F/E}$, а T — подмножество в B, состоящее из образов отображения Tr: $A(F) \to A(F)$. Имеем $H^2(\mathfrak{g}_{F/E}, A(F)) > B/T$. Поэтому надо показать, что $(B:T) \leqslant l$. Но по предположению гомоморфизм Ver: $A(E) \to B$ сюръективен, и если взять его композицию с гомоморфизмом $A(F) \to A(E)$, то получим отображение следа. Отсюда следует, что B/T совпадает с образом коядра отображения $A(F) \to A(E)$, так как это коядро — циклическая группа порядка l; искомый результат получен.

34. Отображение в группу классов циклов

Пусть r — размерность многообразия V, т. е. степень трансцендентности расширения K/k.

Теорема 6. *Для того чтобы* $A(E)$ *было формацией классов, необходимо и достаточно, чтобы* $r \leqslant 1$.

В случае $r = 0$ имеем $A(E) = \mathbf{Z}$, и то, что получается формация классов,очевидно.

При $r = 1$ теорема 4 из § 6 показывает, что $A(E) = C_E$, группе классов иделей поля E. Гомоморфизм Ver: $A(E) \to A(F)$ превращается в гомоморфизм

$$\mathrm{Ver}\colon C_E \to C_F.$$

Простые вычисления с автоморфизмами Фробениуса, с помощью которых Артин доказал впервые теорему о главных идеалах (см., например, Хассе [1]), показывают, что отображение Ver: $C_E \to C_F$ совпадает с *каноническим вложением* первой группы во вторую. Теорема 90 [1]) показывает тогда,

[1]) Гильберта. *Прим. ред.*

что каждый элемент группы C_F, инвариантный относительно группы $\mathfrak{g}_{F/E}$, принадлежит группе C_E (см. Вейль [7], § 1). Отсюда следует в силу теоремы 5, что $A(E)$ — формация классов.

(Таким образом, в случае полей функций теория когомологий приводит лишь к классическим результатам. Другое положение для числовых полей, где наличие связной компоненты группы классов иделей мешает построению удобного отображения группы Галуа в группу классов иделей, см. Вейль [7].)

Покажем теперь, что $A(E)$ при $r \geqslant 2$ *не является формацией классов*. Допустим противное. Положим $K_1 = K\bar{k}$ и обозначим через $A(K_1)$ группу Галуа максимального абелева расширения поля K_1. Определим также для каждого расширения E_1 поля K_1 группу $A(E_1)$. Покажем, что $A(E_1)$ — *формация классов*. Действительно, пусть F_1/E_1 — конечное расширение Галуа с группой Галуа $\mathfrak{g}$. Можно найти конечное расширение k'/k и расширения $F' \supset E' \supset Kk'$ с $F_1 = F'\bar{k}$, $E_1 = E'\bar{k}$, такие, что F'/E' — расширение Галуа с группой Галуа $\mathfrak{g}$. Отсюда следует, что группа $A(F_1)$ есть предел групп $A(F', k'')$, где k'' — конечное расширение поля k'. Далее, диаграмма

$$\begin{array}{ccc} A(E') & \rightarrow & A(E'k'') \\ {\scriptstyle \mathrm{Ver}}\downarrow & & \downarrow{\scriptstyle \mathrm{Ver}} \\ A(F') & \rightarrow & A(F'k'') \end{array}$$

коммутативна. Так как функтор „проективный предел“ точен слева, получаем, что отображение Ver: $A(E_1) \to H^0(\mathfrak{g}, A(F_1))$ биективно, откуда и следует наше утверждение.

Поле $K_1 = K\bar{k}$ содержит все корни из единицы; поэтому к нему применима *теория Куммера*. Точнее, если разложить группу $A(K_1)$ на ее p-примарные компоненты $A_p(K_1)$ и компоненты $A_*(K_1)$, взаимно простые с p, то двойственная группа к компактной группе $A_*(K_1)$ совпадает с проективным пределом $B(K_1)$ групп $B_n(K_1) = K_1^*/K_1^{*n}$, причем предел берется по множеству целых чисел n, взаимно простых с p (гомоморфизм $K^*/K^{*n} \to K^*/K^{*nm}$ является возведением в m-ю степень). При переходе к пределу перенесение переходит в гомоморфизм N: $B(F_1) \to B(E_1)$, совпадающий с *нормой*. Вспоминая, что образ отображения Ver совпадает с множеством элементов $A(F_1)$, инвариантных относительно группы $\mathfrak{g}$, получаем, что для элемента $a \in F_1$, такого, что $Na \in E_1^{*n}$, существует целое число m, взаимно простое с p, такое, что a^m сравнимо по модулю F_1^{*nm} с произведением элементов вида $b^{1-\sigma}$, $b \in \mathfrak{g}$, $b \in F_1^*$. В частности, предположим, что $[F_1 : E_1] = n$ взаимно просто с p, и возьмем $a \in E_1^*$. Тогда $Na = a^n$ и предыдущее условие будет выполнено. Имеем, следовательно,

$$a^m = c^{mn} \prod b^{1-\sigma}; \qquad b, \ c \in F_1^*.$$

Взяв норму обеих частей, получим

$$a^{mn} = (Nc)^{mn},$$

откуда

$$a = \varepsilon \cdot Nc,$$

где ε — корень степени mn из единицы. Но такой корень в поле $\bar{k}$ является n-й степенью и, значит, нормой. Итак, мы получили, что a — *норма*, т. е. что *каждый элемент из поля E_1 является нормой элемента из поля F_1*, если *F_1/E_1 — расширение Галуа, степень которого взаимно проста с p.*

Это было бы верно, если бы $r = 1$ (так как это эквивалентно тому, что группа Брауэра поля K_1 не содержит элементов порядка, взаимно простого с p, а теорема Тзена показывает, что эта группа нулевая).

Но это противоречит предположению $r \geqslant 2$. Действительно, из этого предположения следует, как известно, что существует нормирование v поля E_1, группа значений которого равна $\mathbf{Z} + \mathbf{Z}$. Пусть $a \in E$ — такой элемент, что $v(a) = (1, 0)$, а F_1 — поле, получаемое присоединением к полю E_1 корня степени n из a (n взаимно просто с p). Имеем $[F_1 : E_1] = n$, и нормирование v разветвлено в поле F_1. Если обозначить через v_1 одно из его продолжений, то группа значений этого нормирования на поле F_1 содержит группу

$\frac{1}{n}\mathbf{Z}+\mathbf{Z}$. В сочетании с формулой $\sum e_i f_i \leqslant n$ это показывает, что v_1 — единственное продолжение v и что группа значений нормирования v_1 в точности равна $\frac{1}{n}\mathbf{Z}+\mathbf{Z}$. Но значение нормирования любой нормы входит в группу $n(v_1(F_1^*))$, а значит, и в $\mathbf{Z}+n\mathbf{Z}$. В частности, элемент E_1, нормирование которого равно (0, 1), не является нормой Это противоречие завершает доказательство.

Библиографические замечания

Теория полей классов для поля функций от одной переменной над конечным полем была впервые построена Ф. К. Шмидом и Виттом по аналогии с теорией для числовых полей, т. е. путем утомительного вычисления индексов. В 1940 г. Вейль сделал попытку получить заново эти результаты с геометрической точки зрения; на это указывает его заметка относительно гипотезы Римана (Вейль А. [2]), а также последние страницы его работы об алгебраических кривых (Вейль А, [4]). Но обыкновенных якобиевых многообразий, которыми он располагал, было для этого недостаточно. Требовались обобщенные якобиевы многообразия, а для многообразий высших размерностей — могообразия Альбанезе. Это заметил Ленг [1]—[3], результаты и методы которого и составляют содержание этой главы. Именно он обратил внимание на то, что поля классов можно строить как прообразы изогений типа $\wp$, что сделало очевидным закон взаимности Артина; едва ли стоит говорить, что это не имеет никакой аналогии в числовых полях (за исключением полей рациональных чисел и мнимых квадратичных полей). Ленг развил также аналитическую теорию (L-рядов), на которой мы здесь не останавливаемся.

Отметим недавнюю работу Морикавы [1], которая содержит изложение вопроса для случая кривых и непосредственно примыкает к первой работе Ленга [2]. Морикава дает прямое доказательство (без использования теоремы Розенлихта из гл. III) того факта, что всякое абелево накрытие кривой является прообразом изогении обобщенного якобиева многообразия.

Из литературы о полях классов отметим прежде всего работы Хассе [1] и Хербранда [1], где изложена „классическая“ теория Такаги — Артина. Теория когомологий, разработанная Вейлем [7], Хохшильдом — Накаямой (Хассе [1]) и Тейтом [1], составляет содержание курса Шевалле [2]. Многочисленные другие результаты можно найти в часто упоминаемых заметках Артина — Тейта (*Алгебраические числа и алгебраические функции* II); читатель, не желающий дожидаться их публикации, может обратиться к работам Кавады [1]—[3] и Кавады — Сатаке [1].

ГЛАВА

VII

РАСШИРЕНИЯ ГРУПП И КОГОМОЛОГИИ

В этой главе мы предполагаем, что основное поле k алгебраически замкнуто.

Все рассматриваемые алгебраические группы *коммутативны* (но не обязательно связны).

§ 1. Расширения групп

Пусть $\mathscr{C}$ — категория коммутативных групп (в обычном смысле, т. е. не снабженных структурой алгебраических групп). Если $A, B \in \mathscr{C}$, то можно определить группу $\operatorname{Ext}(A, B)$ абелевых расширений A с помощью B либо непосредственно (Бэр [1]), либо как первый производный функтор функтора $\operatorname{Hom}(A, B)$ (Картан и Эйленберг [1], гл. XIV); известо также, что элементы $\operatorname{Ext}(A, B)$ можно интерпретировать как классы систем симметрических факторов.

Цель настоящего параграфа — перенести определение $\operatorname{Ext}(A, B)$ и его главные свойства на категорию $\mathscr{C}_A$ алгебраических коммутативных групп.

1. Группы $\operatorname{Ext}(A, B)$

Пусть A, B, C — три алгебраические (коммутативные) группы. Последовательность (алгебраических) гомоморфизмов

$$0 \to B \to C \to A \to 0 \qquad (1)$$

называется *строго точной*, если она точна в обычном смысле и если гомоморфизмы $B \to C$ и $C \to A$ сепарабельны, иначе говоря, если алгебраическая структура B (соответственно A) индуцируется структурой C (соответственно является ее факторструктурой). При этом группу B можно отождествить с подгруппой в C, а группу A — с C/B.

Обозначим через $\mathfrak{t}$ (соответственно через $\mathfrak{t}_B$, $\mathfrak{t}_C$) касательное пространство к A (соответственно к B, к C) в начале координат. Последовательность (1) порождает последовательность

$$0 \to \mathfrak{t}_B \to \mathfrak{t}_C \to \mathfrak{t}_A \to 0. \qquad (2)$$

Лемма 1. *Последовательность алгебраических групп* (1) *строго точна в том и только в том случае, когда она точна и точна последовательность векторных пространств* (2).

Эта лемма является переформулировкой следствий 2 и 3 предложения 16 гл. III.

Строго точная последовательность (1) называется *расширением* A с помощью B (для краткости часто говорят, что C является расширением A с помощью B). Два расширения C и C' *изоморфны*, если существует гомоморфизм $f\colon C \to C'$, приводящий к коммутативной диаграмме

$$\begin{array}{ccccccccc} 0 & \to & B & \to & C & \to & A & \to & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \to & B & \to & C' & \to & A & \to & 0 \end{array} \qquad (3)$$

В таком случае f является автоматически *изоморфизмом*. В самом деле, ясно, что гомоморфизм f биективен, а аналогичная (3) диаграмма, образованная касательными пространствами $\mathfrak{t}_A$, $\mathfrak{t}_B$, $\mathfrak{t}_C$, $\mathfrak{t}_{C'}$, показывает, что f определяет изоморфизм $\mathfrak{t}_C$ на $\mathfrak{t}_{C'}$, откуда по лемме 1 и следует наше утверждение.

Множество *классов расширений* A с помощью B (где отношением эквивалентности является изоморфизм) обозначается $\mathrm{Ext}(A, B)$. Это *функтор, контравариантный по* A *и ковариантный по* B:

a) Если $f\colon B \to B'$ - гомоморфизм и $C \in \mathrm{Ext}(B, A)$, то определим $f_*(C)$ (обозначается также fC) как фактор $C \times B'$ по подгруппе, образованной парами $(-b, f(b))$, где b пробегает B Канонические отображения $B' \to C \times B$ и $C \times B' \to C$ определяют при переходе к фактору последовательность

$$0 \to B' \to f_*(C) \to A \to 0. \qquad (4)$$

Эта последовательность строго точна, в чем можно убедиться с помощью леммы 1. Следовательно, $f_*(C) \in \operatorname{Ext}(A, B')$. Можно также $f_*(C)$ характеризовать как однозначно определяемое расширение C' группы A с помощью B', такое, что существует гомоморфизм $F: C \to C'$, приводящий к коммутативной диаграмме

$$\begin{array}{ccccccccc} 0 & \to & B & \to & C & \to & A & \to & 0 \\ & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 0 & \to & B' & \to & C' & \to & A & \to & 0 \end{array} \tag{5}$$

б) Аналогично, если $g: A' \to A$ — гомоморфизм и $C \in \operatorname{Ext}(A, B)$, то определим $g^*(C)$ (обозначается также через Cg) как подгруппу в $A' \times C$, образованную парами (a', c) элементов, имеющих одинаковый образ в A. Эта группа принадлежит $\operatorname{Ext}(A', B)$ и ее также можно характеризовать с помощью диаграммы, аналогичной (5) (обозначаем ее далее (6)). Вообще пусть $C \in \operatorname{Ext}(A, B)$, $C' \in \operatorname{Ext}(A', B')$ и $f: B \to B'$, $g: A \to A'$ — гомоморфизмы. Соотношение

$$g^*(C') = f_*(C) \quad \text{в} \quad \operatorname{Ext}(A, B') \tag{7}$$

эквивалентно существованию гомоморфизма F, приводящего к коммутативной диаграмме

$$\begin{array}{ccccccccc} 0 & \to & B & \to & C & \to & A & \to & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle g} & & \\ 0 & \to & B' & \to & C' & \to & A' & \to & 0 \end{array} \tag{8}$$

Немедленно проверяется, что $\operatorname{Ext}(A, B)$ — функтор, иначе говоря, что $1_* = 1$, $(ff')_* = f_* f'_*$, $1^* = 1$, $(gg')^* = g'^* \cdot g^*$. Кроме того, $f_* g^* = g^* f_*$ (что оправдывает обозначения fC и Cg).

Снабдим теперь $\operatorname{Ext}(A, B)$ законом композиции. Для этого воспользуемся методом Бэра [1]. Если C и C' — два элемента из $\operatorname{Ext}(A, B)$, то произведение $C \times C'$ можно рассматривать как элемент из $\operatorname{Ext}(A \times A, B \times B)$. Если обозначить через $d: A \to A \times A$ и $s: B \times B \to B$ соответственно диагональное отображение A и закон композиции B, то

$$C + C' = d^* s_* (C \times C') \tag{9}$$

— закон композиции в $\operatorname{Ext}(A, B)$.

Предложение 1. *Закон композиции* (9) *превращает* Ext(A, B) *в абелеву группу. Если через* $\mathscr{C}_A$ *обозначить аддитивную категорию алгебраических коммутативных групп, то функтор* Ext(A, B) — *аддитивный бифунктор на* $\mathscr{C}_A \times \mathscr{C}_A$.

Доказательство состоит в проверке того, что конструкция Бэра [1], примененная к нашему случаю, приводит к алгебраическим группам (что очевидно) и к строго точным последовательностям (следует применить лемму 1). Эта проверка, хотя и не представляет никаких затруднений, немного скучновата. Мы ограничимся краткими указаниями.

а) *Нейтральный элемент*, обозначаемый через 0, группы Ext(A, B) есть тривиальное расширение $C = A \times B$. Заметим, что это расширение характеризуется существованием сечения $A \to C$ (соответственно проекции $C \to B$), являющегося гомоморфизмом.

б) *Коммутативность* Ext(A, B) очевидна из определения.

в) *Ассоциативность* Ext(A, B) доказывается с использованием отображения взятия суммы s^3: $B \times B \times B \to B$ и диагонального отображения d_3: $A \to A \times A \times A$, а также того факта, что каждая из компонент $(C + C') + C''$ и $C + (C' + C'')$ равна $d_3^* S^3_*(C \times C' \times C'')$.

г) *Аддитивность* функтора Ext(A, B), т. е. тот факт, что $f_*(C)$ билинейно по f и C (и то же самое для $g^*(C)$), проверяется построением диаграмм (5) и (6).

д) Существование *обратного элемента* к элементу $C \in$ Ext(A, B) доказывается рассмотрением элемента $(-1)^*(C)$, где -1 обозначает эндоморфизм $a \to -a$ группы A.

Выпишем два частных случая предложения 1:

$$\begin{aligned} \operatorname{Ext}(A \times A', B) &= \operatorname{Ext}(A, B) \times \operatorname{Ext}(A', B), \\ \operatorname{Ext}(A, B \times B') &= \operatorname{Ext}(A, B) \times \operatorname{Ext}(A, B'). \end{aligned} \tag{10}$$

2. Первая точная последовательность для Ext

Пусть A, B — алгебраические группы. Обозначим через Hom(A, B) группы (алгебраических) гомоморфизмов A в B. Мы увидим, что Hom(A, B) и Ext(A, B) связаны точной последовательностью, аналогичной той, которая имеет место в категории $\mathscr{C}$ абелевых групп.

Пусть $0 \to A' \to A \to A'' \to 0$ — строго точная последовательность. Тогда $A \in \operatorname{Ext}(A'', A')$. Если $\varphi \in \operatorname{Hom}(A', B)$, то $\varphi_*(A) \in \operatorname{Ext}(A'', B)$. Положим $d(\varphi) = \varphi_*(A)$. Отображение

$$d\colon \operatorname{Hom}(A', B) \to \operatorname{Ext}(A'', B),$$

определенное таким образом, является гомоморфизмом.

Предложение 2. *Пусть* $0 \to A' \to A \to A'' \to 0$ — *строго точная последовательность и* B — *алгебраическая группа.* Последовательность

$$\begin{gathered}0 \to \operatorname{Hom}(A'', B) \to \operatorname{Hom}(A, B) \to \operatorname{Hom}(A', B) \xrightarrow{d} \\ \xrightarrow{d} \operatorname{Ext}(A'', B) \to \operatorname{Ext}(A, B) \to \operatorname{Ext}(A', B)\end{gathered} \tag{11}$$

точна.

(Все гомоморфизмы этой точной последовательности, кроме d, канонически определяются отображениями $A' \to A$ и $A \to A''$.)

Надо проверить точность в членах $\operatorname{Hom}(A'', B)$, ..., $\operatorname{Ext}(A, B)$.

1) *Точность в* $\operatorname{Hom}(A, B)$. Она означает, что гомоморфизм $A'' \to B$ является нулевым в том и только в том случае, когда композиция $A \to A'' \to B$ нулевая, что очевидно, поскольку $A \to A'$ — сюръективное отображение.

2) *Точность в* $\operatorname{Hom}(A, B)$. Она означает, что гомоморфизм $A \to B$ индуцирует нулевой гомоморфизм на A' в том и только в том случае, когда он разлагается на $A \to A'' \to B$, что очевидно, поскольку A'' является фактором A по A'.

3) *Точность в* $\operatorname{Hom}(A', B)$. Пусть $\varphi \in \operatorname{Hom}(A', B)$. Надо показать, что φ продолжается на A тогда и только тогда, когда расширение $C = \varphi_*(A) \in \operatorname{Ext}(A'', B)$ тривиально. Но по определению $C = A \times B/D_\varphi$, где D_φ обозначает подгруппу $A \times B$, образованную парами $(-a', \varphi(a'))$, $a' \in A'$. Продолжение φ на A приводит к гомоморфизму $\Phi\colon A \times B \to B$, который равен нулю на D_φ, т. е. к гомоморфизму $C \to B$, являющемуся проекцией, так что C — тривиальное расширение. Обратно, такая проекция определяет Φ, откуда следует существование продолжения φ на A.

4) *Точность в* $\operatorname{Ext}(A'', B)$. Пусть $C \in \operatorname{Ext}(A'', B)$. Надо убедиться в том, что образ C_1 группы C в $\operatorname{Ext}(A, B)$ три-

виален тогда и только тогда, когда C имеет вид $\varphi_*(A)$, где $\varphi \in \mathrm{Hom}(A', B)$. Но C_1 тривиальна в том и только в том случае, когда существует сечение $A \to C_1$, являющееся гомоморфизмом, т. е. когда $A \to A''$ представляется в виде $A \xrightarrow{\psi} C \to A''$. Если $C = \varphi_*(A) = A \times B/D_\varphi$, то такое разложение очевидно. Обратно, если имеет место такое разложение, то определим φ: $A' \to B$ как ограничение ψ на A'. Легко проверяется, что гомоморфизм $A \times B \to C$, определенный с помощью ψ, отождествляет C с $A \times B/D_\varphi$, т. е. с $\varphi_*(A)$.

5) *Точность в* $\mathrm{Ext}(A, B)$. Так как композиция $A' \to A \to A''$ нулевая, то нулевой будет и композиция $\mathrm{Ext}(A'', B) \to \to \mathrm{Ext}(A, B) \to \mathrm{Ext}(A', B)$. Нам надо показать, что, обратно, если $C_1 \in \mathrm{Ext}(A, B)$ дает 0 в $\mathrm{Ext}(A', B)$, то расширение C_1 получается из расширения $c \in \mathrm{Ext}(A'', B)$. Но по предположению существует сечение-гомоморфизм $A' \to C$. Полагая $C = C_1/A'$, получаем расширение C группы A'' с помощью B. Диаграмма (6) из п. 1 показывает, что образ C в $\mathrm{Ext}(A, B)$ равен C_1, чем и завершается доказательство предложения 1.

3. Другие точные последовательности

Пусть $0 \to B' \to B \to B'' \to 0$ — строго точная последовательность. Если A—алгебраическая группа и $\varphi \in \mathrm{Hom}(A, B'')$, то $\varphi^*(B) \in \mathrm{Ext}(A, B')$. Полагая $d(\varphi) = \varphi^*(B)$, получаем гомоморфизм

$$d\colon \mathrm{Hom}(A, B'') \to \mathrm{Ext}(A, B').$$

Предложение 3. *Пусть* $0 \to B' \to B \to B'' \to 0$ — *строго точная последовательность и* A — *алгебраическая группа. Последовательность*

$$\begin{gathered} 0 \to \mathrm{Hom}(A, B') \to \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, B'') \xrightarrow{d} \\ \xrightarrow{d} \mathrm{Ext}(A, B') \to \mathrm{Ext}(A, B) \to \mathrm{Ext}(A, B'') \end{gathered} \tag{12}$$

точна.

(Все фигурирующие в этой точной последовательности гомоморфизмы, за исключением d, канонически определяются отображениями $B' \to B$ и $B \to B''$.)

Доказательство состоит из серии проверок, аналогичных проведенным в предыдущем пункте.

Замечания. 1. В случае характеристики $p \neq 0$ существует точная последовательность, аналогичная последовательности (11), относительно радикальной изогении $A'' = A/\mathfrak{n}$ высоты 1, где $\mathfrak{n}$ обозначает векторное подпространство $\mathfrak{t}_A$, инвариантное относительно возведения в p-ю степень (Серр [6], п. 8):

$$0 \to \operatorname{Hom}(A/\mathfrak{n}, B) \to \operatorname{Hom}(A, B) \to \operatorname{Hom}(\mathfrak{n}, \mathfrak{t}_B) \to$$
$$\to \operatorname{Ext}(A/\mathfrak{n}, B) \to \operatorname{Ext}(A, B) \to \operatorname{Ext}(\mathfrak{n}, \mathfrak{t}_B). \qquad (13)$$

2. Категория $\mathscr{C}_A$ алгебраических (коммутативных) групп аддитивна; она является *абелевой* категорией (в смысле Гротендика [1] в случае, когда характеристика поля k равна 0, и только в этом случае. Кроме того, $\mathscr{C}_A$ не содержит в достаточном количестве проективных и инъективных объектов. Последнее обстоятельство и не дало нам возможности определить $\operatorname{Ext}(A, B)$ с помощью общих методов гомологической алгебры (Картан — Эйленберг [1], Гротендик [1]). Во всяком случае, можно было бы применить к $\mathscr{C}_A$ метод Ионеды [1] и определить $\operatorname{Ext}^q(A, B)$ $(q \geqslant 2)$ с помощью продолжений точных последовательностей (11) и (12) (см. также п. 23).

4. Системы факторов

Пусть A, B — коммутативные группы. Напомним, что *системой факторов* на A со значениями в B называется всякое отображение $f\colon A \times A \to B$, удовлетворяющее тождеству

$$f(y, z) - f(x+y, z) + f(x, y+z) - f(x, y) = 0 \quad (x, y, z \in A). \qquad (14)$$

Если g: $A \to B$ — произвольное отображение, то функция δg, определяемая формулой

$$\delta g(x, y) = g(x+y) - g(x) - g(y), \tag{15}$$

является системой факторов. Такая система факторов называется *тривиальной*.

Группа классов систем факторов по модулю тривиальных систем факторов обозначается через $H^2(A, B)$.

Система факторов f называется *симметрической*, если выполняется тождество

$$f(x, y) = f(y, x). \tag{16}$$

Классы симметрических факторов образуют подгруппу $H^2(A, B)_s$ группы $H^2(A, B)$.

Хорошо известные рассуждения (по существу тривиальные) показывают, что $H^2(A, B)$ изоморфна группе классов *центральных* расширений A с помощью B, причем подгруппе $H^2(A, B)_s$ соответствуют *коммутативные* расширения (см. Картан — Эйленберг [1], гл. XIV, § 4). (Все это имеет место в более общем случае, когда A не предполагается коммутативной.)

Предположим теперь, что A и B — алгебраические (как всегда, коммутативные) группы. Кроме того, будем считать их связными. *Рациональное* отображение f: $A \times A \to B$, удовлетворяющее тождеству (14), будем называть *системой рациональных факторов*; такая система называется *тривиальной*, если существует рациональное отображение g: $A \to B$, такое, что $f = \delta g$. Классы систем рациональных факторов образуют группу, которая обозначается через $H^2_{\mathrm{rat}}(A, B)$; системы симметрических факторов образуют ее подгруппу $H^2_{\mathrm{rat}}(A, B)_s$. Вместо рациональных отображений можно рассматривать *регулярные* отображения; таким образом определяются группы $H^2_{\mathrm{reg}}(A, B)$ и $H^2_{\mathrm{reg}}(A, B)_s$.

Предложение 4. а) *Группа $H^2_{\mathrm{reg}}(A, B)_s$ изоморфна подгруппе в* $\mathrm{Ext}(A, B)$, *образованной расширениями, которые обладают регулярным сечением.*

б) *Группа* $H^2_{\mathrm{rat}}(A, B)_s$ *изоморфна подгруппе в* $\mathrm{Ext}(A, B)$, *образованной расширениями, которые обладают рациональным сечением.*

Доказательство. а) Если $C \in \mathrm{Ext}(A, B)$ обладает регулярным сечением s: $A \to C$, то положим $f(x, y) = s(x+y) - s(x) - s(y)$. Отображение f является регулярным отображением A в ядро отображения $C \to A$, т. е. в B. Оно удовлетворяет тождествам (14) и (16). Далее, замена сечения s на другое сечение приводит к прибавлению к этому отображению системы тривиальных факторов. Если обозначить через $\mathrm{Ext}(A, B)_*$ подмножество в $\mathrm{Ext}(A, B)$, образованное расширениями, которые обладают регулярным сечением, то получаем отображение θ: $\mathrm{Ext}(A, B)_* \to H^2_{\mathrm{reg}}(A, B)_s$. Непосредственно проверяется, что $\mathrm{Ext}(A, B)_*$ является подгруппой в $\mathrm{Ext}(A, B)$ и что θ — гомоморфизм. Если $\theta(C)=0$, то расширение C обладает сечением s, которое является гомоморфизмом, т. е. C — тривиальное расширение. Следовательно, θ инъективно. С другой стороны, пусть f — система симметрических факторов. Определим закон композиции на $A \times B$, полагая

$$(x, b)*(x', b') = (x + x', b + b' + f(x, x')). \tag{17}$$

Непосредственно проверяется, что этот закон композиции превращает $A \times B$ в алгебраическую коммутативную группу, расширение A с помощью B, которое соответствует системе факторов f. Таким образом, θ *биективно.*

б) Пусть $\mathrm{Ext}(A, B)_{**}$ — подмножество в $\mathrm{Ext}(A, B)$, образованное расширениями, которые имеют рациональное сечение. Легко проверяется, что $\mathrm{Ext}(A, B)_{**}$ — подгруппа. Как и выше, определяется гомоморфизм $\theta: \mathrm{Ext}(A, B)_{**} \to H^2_{\mathrm{rat}}(A, B)_s$. Ядро гомоморфизма θ состоит из расширений C, имеющих рациональное сечение s: $A \to C$, являющееся гомоморфизмом Такое сечение обязательно должно быть регулярным (см., например, гл. V, п. 5, лемма 6). Это означает, что $C=0$ и что θ *инъективно.* Для доказательства сюръективности θ определим на $A \times B$ закон композиции формулой (17) где f система симметрических факторов. Этот закон превращает $A \times B$ в „бирациональную группу“. Согласно результатам Вейля, указанным в гл. V, п. 5, существует алгебраическая группа C, бирационально изоморфная многообразию $A \times B$ с законом композиции (17). Эта группа связна и коммутативна (поскольку система факторов симметрическая). Проекция $A \times B \to A$ определяет сюръективный гомоморфизм $C \to A$. Пусть b — общая точка B. Выберем независимые общие точки $a \in A'$, $b' \in B$. Обозначая через F: $A \times B \to C$ введенный выше бирациональный изоморфизм, можем положить $\varphi(b) = F(a, b + b') - F(a, b')$; это имеет смысл, поскольку $(a, b + b')$ и (a, b') — общие точки $A \times B$. Легко проверяется, что $\varphi(b)$ не зависит от выбора (a, b'), что φ — гомоморфизм B в C и что последовательность $0 \to B \to C \to A \to 0$ строго точна. Кроме того, система факторов, соответствующая C, равна f. Это завершает доказательство того, что гомоморфизм θ *биективен.*

Следствие. *Канонический гомоморфизм $H^2_{\mathrm{reg}}(A, B)_s \to H^2_{\mathrm{rat}}(A, B)_s$ инъективен.*

В самом деле, обе эти группы отождествляются с подгруппами в $\mathrm{Ext}(A, B)$.

Замечания. 1. Если не предполагать коммутативности A, то предыдущие рассуждения показывают, что $H^2_{\mathrm{reg}}(A, B)$ (соответственно $H^2_{\mathrm{rat}}(A, B)$) отождествляется с подгруппой классов *центральных* расширений A помощью B, обладающих регулярным (соответственно рациональным) сечением.

2. Следствие предложения 4 можно проверить непосредственно. Если g: $A \to B$ — рациональное отображение, такое, что $g(x + y) - g(x) - g(y) = f(x, y)$ регулярно на $A \times A$, то отображение g регулярно на непустом открытом множестве U группы A, а следовательно, и на $U + U = A$ в силу предыдущего тождества.

5. Главное расслоенное пространство, определяемое расширением

Пусть, как и в предыдущем пункте, A и B — связные (коммутативные) алгебраические группы. Пусть $C \in \mathrm{Ext}(A, B)$ — расширение, обладающее рациональным сечением s: $A \to C$. Это сечение регулярно на открытом непустом множестве U

многообразия A. Так как переносы U покрывают A, то существуют покрытие $\{U_i\}$ группы A и регулярные сечения s_i группы C над U_i. Ограничение C на U_i бирегулярно изоморфно $U_i \times B$. Это означает, что C можно рассматривать как *главное расслоенное пространство* с базой A и структурной группой B. Если $\mathscr{B}_A$ обозначает пучок ростков регулярных отображений A в B, то группа $H^1(A, \mathscr{B}_A)$ есть группа классов расслоений предыдущего типа. Элемент $c \in H^1(A, \mathscr{B}_A)$, соответствующий C, определяется 1-коциклом $b_{ij}(C) = s_j - s_i$. Принимая во внимание предложение 4, видим, что определено каноническое отображение

$$\pi\colon H^2_{\mathrm{rat}}(A, B)_s \to H^1(A, \mathscr{B}_A).$$

Предложение 5. *Отображение π является гомоморфизмом, ядро которого равно $H^2_{\mathrm{reg}}(A, B)_s$.*

Первая часть проверяется непосредственным вычислением (или следует из того факта, что π имеет „функториальный“ характер, т. е. коммутирует с гомоморфизмами f_* и g^*, определяемыми отображениями $f\colon B \to B'$ и $g\colon A' \to A$). Ядро π образовано расширениями C, являющимися *тривиальными* расслоенными пространствами, т. е. обладающими регулярным сечением. Согласно предложению 4, это ядро равно $H^2_{\mathrm{reg}}(A, B)_s$.

В § 3 мы определим образ π в случае, когда A — *абелево многообразие*, а B — *линейная* группа; именно мы покажем, что этот образ равен $H^1(A, \mathscr{B}_A)$, если B — *унипотентная* группа.

6. Случай линейных групп

Как и в двух предыдущих пунктах, мы предполагаем, что A и B — связные группы.

Предложение 6. *Если B — линейная группа, то $H^2_{\mathrm{rat}}(A, B)_s = \mathrm{Ext}(A, B)$.*

Согласно предложению 4, надо доказать, что всякое расширение C группы A с помощью группы B обладает рациональным сечением s. Пусть x — общая точка A над k, а B_x — ее прообраз в C. Многообразие B_x является главным однородным пространством над B, определенным над полем $K = k(x)$. Утверждение „C обладает рациональным сечением s“ равносильно утверждению „B_x обладает точкой $s(x)$, рациональной над $k(x)$“, т. е. является *тривиальным* главным однородным пространством.

С другой стороны, согласно структуре линейных коммутативных групп (Борель [2] или Розенлихт [4]), группа B обладает композиционным рядом, факторы которого изоморфны либо мультипликативной группе G_m, либо аддитивной группе G_a. Предложение 6 получается теперь из следующей леммы (Розенлихт [4]).

Лемма 2. *Пусть K — поле и B — K-группа, одладающая композиционным рядом из подгрупп (определенных над K), факторы которого k-изоморфны G_m или G_a. Тогда любое главное однородное k-пространство над группой B тривиально.*

Пусть K_s — сепарабельное замыкание поля K и $\mathfrak{g}_s$ — группа Галуа расширения K_s/K, действующая естественным образом на группе B_s точек B, рациональных над K_s. Известно (Ленг и Тейт [1]; см. гл. V, п. 21), что группа главных однородных K-пространств над B изоморфна $H^1(\mathfrak{g}_s, B_s)$. Таким образом, осталось доказать, что эта последняя группа тривиальна. По индукции относительно размерности B можно считать, что $B = G_m$ или G_a. В первом случае $B_s = K_s^*$ и утверждение о тривиальности группы $H^1(\mathfrak{g}_s, K_s^*)$ совпадает с классической „теоремой 90“ Гильберта. Во втором случае $B_s = K_s$ и тривиальность группы $H^1(\mathfrak{g}_s, K_s)$ (и групп когомологий более высоких размерностей) — не менее классический результат; он следует, например, из теоремы о нормальном базисе.

Если A тоже линейная группа, то можно доказать

Предложение 7. *Если A и B — линейные группы, то $H^2_{\text{reg}}(A, B)_s = \operatorname{Ext}(A, B)$.*

Известно (см. гл. III, п. 7), что всякая линейная связная группа является произведением унипотентной группы на группы G_m. В силу аддитивности функтора Ext доказательство предложения сводится к случаю, когда A и B равны U или G_m. Имеем

$$\operatorname{Ext}(G_m, U) = \operatorname{Ext}(U, G_m) = \operatorname{Ext}(G_m, G_m) = 0.$$

Действительно, это очевидно для первых двух групп, а для третьей следует из структуры торов. Итак, остается доказать, что $\mathrm{Ext}(A, B) = 0$, если A и B — унипотентные группы. В силу предложений 5 и 6 достаточно доказать, что $H^1(A, \mathscr{B}_A) = 0$. Применим индукцию по $n = \dim B$. Если $n = 1$, то $B = G_a$, откуда $\mathscr{B}_A = \mathfrak{G}_A$, пучку локальных колец A, и $H^1(A, \mathfrak{G}_A) = 0$ в силу того, что A — аффинное многообразие (см. АКП, гл. II, § 3). Если $n > 1$, то, как известно (Розенлихт [4]), B имеет связную подгруппу B', такую, что $B/B' = G_a$. Так как расширение B имеет рациональное сечение (предложение 6), получаем точную последовательность пучков

$$0 \to \mathscr{B}'_A \to \mathscr{B}_A \to \mathfrak{G}_A \to 0 \tag{18}$$

и точную последовательность когомологий

$$H^1(A, \mathscr{B}'_A) \to H^1(A, \mathscr{B}_A) \to H^1(A, \mathfrak{G}_k). \tag{19}$$

По предположению индукции обе крайние группы равны нулю, а значит, равна нулю и $H^1(A, \mathscr{B}_A)$.

Следствие. *Всякая связная унипотентная группа бирегулярно изоморфна (как алгебраическое многообразие) аффинному пространству.*

Пусть U—такая группа. Применим индукцию по $n = \dim U$. Если $\dim U = 1$, то $U = G_a$. Если $\dim U \geqslant 1$, то имеется связная подгруппа U' группы U, такая, что $U/U' = G_a$. Согласно предыдущему предложению, примененному к $\mathrm{Ext}(G_a, U')$, многообразие U бирегулярно изоморфно $G_A \times U'$, откуда результат следует по предположению индукции.

Замечания. 1. По нашему обычному соглашению, группа U предполагалась *коммутативной*. Фактически это условие не использовалось, что видно из предыдущего доказательства.

2. Следствие можно немного уточнить, показав, что в унипотентной группе U существуют координаты $(x_1, \ldots, x_n)$, такие, что сумма $\vec{z} = (z_1, \ldots, z_n)$ двух элементов $\vec{x} = (x_1, \ldots$ $\ldots, x_n)$ и $\vec{y} = (y_1, \ldots, y_n)$ задается формулой вида

$$z_i = x_i + y_i + P_i(x_1, y_1, \ldots, x_{i-1}, y_{i-1}) \quad (1 \leqslant i \leqslant n), \tag{20}$$

где P_i — полиномы.

§ 2. Структура связных (коммутативных) унипотентных групп

7. Группа $\operatorname{Ext}(G_a, G_a)$

Всякая связная унипотентная группа является кратным расширением групп типа G_a, поэтому для определения структуры этих групп необходимо сперва определить группу $\operatorname{Ext}(G_a, G_a)$. Согласно предложению 7, эта группа равна $H^2_{\mathrm{reg}}(G_a, G_a)_s$, группе классов систем регулярных симметрических факторов. Так как регулярное отображение $G_a \times G_a$ в G_a есть *полином* $f(x, y)$ *от двух переменных*, остается определить полиномы, которые симметричны и удовлетворяют тождеству (14).

В случае когда характеристика $p > 0$, нетривиальным примером такого полинома является

$$F(x, y) = \frac{1}{p}(x^p - y^p - (x^p + y^p)). \tag{21}$$

Предложение 8. *В случае когда характеристика равна* 0, $H^2_{\mathrm{reg}}(G_a, G_a) = 0$. *Для характеристики* $p > 0$ *векторное пространство* $H^2_{\mathrm{reg}}(G_a, G_a)$ *над полем* k *имеет своим базисом* p^i*-е степени* $(i = 0, 1, \ldots)$ *системы факторов* F, *определенной формулой* (21).

Записывая $f(x, y)$ в виде $\sum a_{ij} x^i y^i$, видим, что формула (14) приводит к соотношениям, связывающим a_{ij}, которые позволяют явно определить все системы факторов (в частности, те из них, которые симметричны). Подробности см. у Лазара [1], § III.

Следствие. *При нулевой характеристике всякая связная (коммутативная) унипотентная группа изоморфна произведению групп* G_a.

Пусть U — такая группа. Применим индукцию по $n = \dim U$; случай $n = 0$ тривиален. Если $n \geqslant 1$, то группа U содержит связную подгруппу U', такую, что $U/U' = G_a$. По предположению индукции, $U' = (G_a)^{n-1}$, откуда $\operatorname{Ext}(G_a, U') = 0$, поскольку $\operatorname{Ext}(G_a, G_a) = 0$ по предыдущему предложению. Следовательно,

$$U = U' \times (G_a) = (G_a)^n.$$

Начиная с этого места и до п. 12, *будем считать, что характеристика поля k равна $p > 0$.*

8. Группы Витта

Цель этого пункта — привести некоторые понятия и обозначения, которые будут использоваться в остальной части этого параграфа.

Обозначим через W_n *группу Витта* размерности n; элемент $\vec{x} \in W_n$ определяется n компонентами $(x_0, \ldots, x_{n-1})$, причем закон композиции задается формулами вида (20). Полиномы, фигурирующие в этой формуле, строятся с помощью способа, указанного Виттом [1].

В группах W_n имеются три следующие операции:

а) гомоморфизм Фробениуса F: $W_n \to W_n$, переводящий точку $(x_0, \ldots, x_{n-1})$ в $(x_0^p, \ldots, x_{n-1}^p)$ (см. гл. VI, п. 1);

б) гомоморфизм сдвига V: $W_n \to W_{n+1}$, переводящий точку $(x_0, \ldots, x_{n-1})$ в $(0, x_0, \ldots, x_{n-1})$;

в) гомоморфизм проекции R: $W_{n+1} \to W_n$, переводящий $(x_0, \ldots, x_n)$ в $(x_0, \ldots, x_{n-1})$.

Эти гомоморфизмы коммутируют между собой. Их произведение совпадает с операцией умножения на p.

Если n и m — два целых числа $\geqslant 1$, то имеет место строго точная последовательность

$$0 \to W_m \xrightarrow{V^n} W_{n+m} \xrightarrow{R^m} W_n \to 0. \tag{22}$$

Соответствующий элемент из $\operatorname{Ext}(W_n, W_m)$ будет обозначаться через α_n^m.

Легко определить действие операций V и R на элементы α_n^m. Например, коммутативная диаграмма

$$\begin{array}{ccccccccc}
0 \to & W_m & \to & W_{n+m} & \to & W_n & \to 0 \\
& \downarrow{\scriptstyle R} & & \downarrow{\scriptstyle R} & & \downarrow{\scriptstyle \mathrm{Id}} & \\
0 \to & W_{m-1} & \to & W_{n+m} & \to & W_n & \to 0
\end{array}$$

показывает, что

$$R\alpha_n^m = \alpha_n^{m-1}. \tag{23}$$

Аналогичным образом проверяются формулы

$$V\alpha_n^m = \alpha_{n-1}^{m+1}R, \qquad \alpha_n^m V = \alpha_{n-1}^m. \tag{24}$$

[Мы используем здесь обозначения $V\alpha_n^m$ и $\alpha_n^m V$ вместо $V_*(\alpha_n^m)$ и $V^*(\alpha_n^m)$ соответственно; см. п. 1.]

Обозначим через A_n кольцо эндоморфизмов алгебраической группы W_n. Операции fC и Cg вносят в $\operatorname{Ext}(W_n, W_m)$ структуру правого модуля над A_n и левого модуля над A_m, причем эти структуры согласованы.

При $n=1$ группа W_1 сводится к G_a. Точные последовательности (22) показывают, что W_n — кратное расширение групп G_a и, значит, является унипотентной группой. Отождествляя W_i с подгруппой W_n при помощи V^{n-i}, имеем $W_i = p^{n-i}W_n$. Группы W_i являются единственными связными подгруппами в W_n.

9. Леммы

Лемма 3. *Всякий элемент $x \in \operatorname{Ext}(G_a, G_a)$ единственным образом записывается в виде $x = \varphi\alpha_1^1$ (соответственно $x = \alpha_1^1\psi$), где $\varphi, \psi \in A_1$.*

Элемент $\alpha_1^1 \in \operatorname{Ext}(G_a, G_a)$ соответствует системе факторов F, определяемой формулой (21). По предложению 8 элемент x соответствует системе факторов вида

$$f = \sum a_i F^{p^i}, \quad \text{где} \quad a_i \in k.$$

С другой стороны, всякий эндоморфизм φ группы G_a записывается единственным образом в виде

$$\varphi(t) = \sum b_i t^{p^i}.$$

Но $x = \varphi\alpha_1^1$ в том и только в том случае, когда $b_i = a_i$ для всех i, что и доказывает существование и единственность φ. Аналогично, если записать ψ в виде

$$\psi(t) = \sum c_i t^{p^i},$$

то c_i определяется уравнением $c_i^p = a_i$.

Лемма 4. $\mathrm{Ext}(W_n, G_a)$ *является левым свободным A_1-модулем с базисом* α_n^1.

Применим индукцию по n. Для $n=1$ имеем $W_1 = G_a$; применяем тогда часть леммы 3, относящуюся к φ. Для $n \geqslant 2$ используем точную последовательность (11) для Ext, соответствующую расширению $W_a/G_a = W_{n-1}$. Получим тогда точную последовательность

$$\mathrm{Ext}(W_{n-1}, G_a) \xrightarrow{\lambda} \mathrm{Ext}(W_n, G_a) \xrightarrow{\mu} \mathrm{Ext}(G_a, G_a). \quad (25)$$

Имеем $\lambda(x) = xR$ и $\mu(y) = yV^{n-1}$. Таким образом, λ и μ — гомоморфизмы относительно структуры левого A_1-модуля. Согласно (24), имеем $\lambda(\alpha_{n-1}^1) = \alpha_{n-1}^1 R = 0$. Так как α_{n-1}^1 порождает $\mathrm{Ext}(W_{n-1}, G_a)$ по предположению индукции, то $\lambda = 0$. Таким образом, гомоморфизм μ инъективен. Кроме того, согласно (24), имеем $\mu(\alpha_n^1) = \alpha_n^1 V^{n-1} = \alpha_1^1$, и в силу леммы 3 α_1^1 порождает $\mathrm{Ext}(G_a, G_a)$. Отсюда следует, что μ биективен и что α_n^1 порождает $\mathrm{Ext}(W_n, G_a)$ относительно его структуры левого A_1-модуля.

Лемма 4′. $\mathrm{Ext}(G_a, W_a)$ *является правым свободным A_1-модулем с базисом* α_1^n.

Доказательство леммы совпадает с доказательством леммы 4, следует только применить ту часть леммы 3, которая относится к ψ, и использовать точную последовательность (12), соответствующую расширению $W_n/W_{n-1} = G_a$:

$$\mathrm{Ext}(G_a, W_{n-1}) \xrightarrow{\lambda} \mathrm{Ext}(G_a, W_n) \xrightarrow{\mu} \mathrm{Ext}(G_a, G_a). \quad (26)$$

Снова доказываем, что $\lambda = 0$ и что μ — изоморфизм.

Лемма 5. *Пусть $n \geqslant 0$. Для всякого $\varphi \in A_1$ существуют Φ, $\Phi' \in A_{n+1}$, такие, что $\varphi R^n = R^n \Phi$ и $\Phi' V^n = V^n \varphi$.*

Можно ограничиться случаем, когда $\varphi(t) = \lambda t^{p^i}$, где $\lambda \in k$, так как $\varphi \in A_1$ является линейной комбинацией функций такого вида. Выберем $\vec{w} \in W_{n+1}$, такой, что $R^n \vec{w} = \lambda$, и определим Φ формулой

$$\Phi(\vec{x}) = \vec{w} \cdot F^i(\vec{x}), \quad (27)$$

где произведение берется в смысле *кольца* векторов Витта (см. Витт [1]). Тогда $R^n\Phi(\vec{x}) = \lambda \cdot R^n F^i(\vec{x}) = \lambda F^i R^n(\vec{x}) = \varphi R^n(\vec{x})$.

Аналогично Φ' определяем формулой

$$\Phi'(\vec{x}) = \vec{w}' F^i(\vec{x}), \quad \text{где} \quad R^n F^n \vec{w}' = \lambda. \tag{28}$$

Лемма 6. *Всякий элемент x группы* $\operatorname{Ext}(W_n, G_a)$ *может быть записан в виде $x = \alpha_n^1 t$, где $f \in A_n$. Кроме того, $\alpha_n^1 f = 0$ в том и только в том случае, когда f не является изогенией.*

Действительно, $xV^{n-1} \in \operatorname{Ext}(G_a, G_a)$. Это показывает (лемма 3), что

$$xV^{n-1} = \alpha_1^1\psi, \quad \text{где} \quad \psi \in A_1.$$

В силу леммы 5 существует $f \in A_n$, такой, что $fV^{n-1} = V^{n-1}\psi$. Таким образом,

$$xV^{n-1} = \alpha_1^1\psi = \alpha_n^1 V^{n-1}\psi = \alpha_n^1 f V^{n-1}.$$

Но, как мы видели при доказательстве леммы 4, гомоморфизм, отображающий x на xV^{n-1}, биективен. Соотношение $xV^{n-1} = \alpha_n^1 f V^{n-1}$ дает, таким образом, $x = \alpha_n^1 f$.

Далее, равенство $x = 0$ равносильно равенствам $xV^{n-1} = \alpha_1^1\psi = 0$, откуда $\psi = 0$ (лемма 3). В силу формулы $fV^{n-1} = V^{n-1}\psi$ это эквивалентно тому, что $fV^{n+1} = 0$, т. е. что $\operatorname{Ker} f \supset G_a$, или $\dim \operatorname{Ker} f \geqslant 1$. Лемма доказана.

[Через $\operatorname{Ker}(f)$ обозначается ядро f.]

Лемма 6'. *Всякий элемент $x \in \operatorname{Ext}(G_0, W_a)$ может быть записан в виде $x = g\alpha_1^n$, где $g \in A_n$. Кроме того, $g\alpha_1^n = 0$ в том и только в том случае, когда g не является изогенией.*

Доказательство аналогично доказательству леммы 6.

Лемма 7. *Если $m \geqslant n$, то всякий элемент $x \in \operatorname{Ext}(W_n, G_a)$ можно записать в виде $x = \alpha_n^1 f$, где $f \in \operatorname{Hom}(W_n, W_m)$.*

По лемме 6 имеем $x = \overset{1}{\alpha}_n f$, где $f_1 \in A_n$. Так как $\overset{1}{\alpha}_n = \overset{1}{\alpha}_m V^{m-n}$, то $x = \overset{1}{\alpha}_m V^{m-n} f_1$ и можно положить $f = V^{m-n} f_1$.

Лемма 7′. *Если $m \geqslant n$, то всякий элемент $x \in \operatorname{Ext}(G_a, W_n)$ можно записать в виде $x = g\alpha_1^n$, где $g \in \operatorname{Hom}(W_m, W_n)$.*

Доказательство аналогично доказательству леммы 7.

10. Изогения с произведением групп Витта

Пусть G — связная унипотентная группа. Поскольку G — кратное расширение групп G_a, существует целое $n \geqslant 0$, такое, что $p^n \cdot x = 0$ для всех $x \in G$. Наименьшая степень p, удовлетворяющая этому условию, называется *периодом* группы G; если $n = \dim G$, то период $G \leqslant p^n$. Обратно:

Предложение 9. *Пусть G — (коммутативная) связная унипотентная группа размерности n. Следующие три условия эквивалентны:*

(а) *период G равен p^n;*

(б) *существует изогения f: $W_n \to G$;*

(б′) *существует изогения f': $G \to W_n$.*

Поскольку период инвариантен при изогении, имеем импликации (б) $\Longrightarrow$ (а) и (б′) $\Longrightarrow$ (а). Покажем индукцией по n, что (а) $\Longrightarrow$ (б). Для $n = 1$ это тривиально. Если $n \geqslant 2$, то G можно рассматривать как расширение группы G_1 размерности $n - 1$ с помощью группы G_a. Период G_1 необходимо равен p^{n-1}, и по предложению индукции существует изогения g: $W_{n-1} \to G_1$. Имеем $\overset{*}{g}(G) \in \operatorname{Ext}(W_{n-1}, G_a)$. В силу леммы 4 существует $\varphi \in A_1$, такой, что $g^*(G) = \varphi_*(W_n)$, другими словами, согласно п. 1, существует гомоморфизм f: $W_n \to G$, приводящий к коммутативной диаграмме

$$\begin{array}{ccccccccc} 0 & \to & G_a & \to & W_n & \to & W_{n-1} & \to & 0 \\ & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \\ 0 & \to & G_a & \to & G & \to & G_1 & \to & 0 \end{array} \tag{26}$$

Отображение φ в этой диаграмме ненулевое, так как в противном случае гомоморфизм f определял бы при переходе к фактору гомоморфизм W_{n-1} в G и группа G была бы изогенна группе $G_a \times W_{n-1}$, а значит, имела бы период p^{n-1}. Так как, кроме того, g — изогения, то отображение f — также изогения, что доказывает импликацию (а)$\Rightarrow$(б).

Импликация (*a*)$\Rightarrow$(б′) проверяется аналогичным образом, следует лишь рассматривать G как расширение G_a с помощью G_1 размерности $n-1$ и применить лемму 4′ вместо леммы 4.

Предложение 10. *Пусть* $W = \prod W_{n_i}$ — *произведение групп Витта и* G — *унипотентная связная группа. Следующие условия эквивалентны*:

(а) *существует изогения* $f\colon W \to G$;

(а′) *существует изогения* $g\colon G \to W$.

Предположим, что выполняется (а), и пусть G'_i — прообразы в G множителей W_{n_i} группы W. Для всех i пусть G_i — связная компонента единицы группы G'_i. Отображение $f_i\colon G_i \to W_{n_i}$, определяемое f, является изогенией. По предложению 9 существует изогения $g_i\colon W_{n_i} \to G$; отображение $g\colon W \to G$, являющееся суммой g_i, очевидно, изогенно. Это доказывает импликацию (а)$\Rightarrow$(а′). Таким же рассуждением проверяется импликация (а′)$\Rightarrow$(а).

Говорят, что G *изогенна* W, если выполняются эквивалентные условия (а) и (а′). Если $G_1 \to G_2$ — изогения, то очевидно, что G_1 изогенно W тогда и только тогда, когда G_2 изогенна W.

Теорема 1. *Всякая связная (коммутативная) унипотентная группа изогенна произведению групп Витта.*

Пусть G — связная унипотентная группа размерности r. Применим индукцию по r (случай $r=1$ тривиален). Пусть G — расширение группы G_1 размерности $r-1$ с помощью группы G_a. По предположению индукции существует изогения

$$f\colon \prod_{i=1}^{k} W_{n_i} \to G_1.$$

Положим $W = \prod_{i=1}^{k} W_{n_i}$. Группа $f^*(G)$ является расширением W с помощью G_a и изогенна G. Таким образом, достаточно доказать, что группа $f^*(G)$ изогенна произведению групп Витта, другими словами, все сводится к случаю $W = G_1$.

В этом случае расширение G определяется семейством элементов $\gamma_i \in \operatorname{Ext}(W_{n_i}, G_a)$. Предположим, что $n_1 \geqslant n_i$ для всех i, и пусть W — произведение $(i \geqslant 2)$. Будем различать два случая.

1) $\gamma_1 = 0$. Группа G является в этом случае произведением W_{n_1} и расширения W' с помощью G_a, определяемого системой (γ_i), $i \geqslant 2$. Предположение индукции показывает, что a изогенна произведению групп Витта.

2) $\gamma_1 \neq 0$. Пусть $\beta = (\beta_i) \in \operatorname{Ext}(W, G_a)$ — элемент, определяемый соотношениями $\beta_1 = \alpha^1_n$, $\beta_i = 0$ при $i \geqslant 2$. Расширение G', соответствующее β, совпадает с произведением $W_{n_1+1} \times W'$. Мы докажем существование изогении φ: $W \to W'$, такой, что $\varphi^*(a')$ изоморфно G. Отсюда будет следовать, что G изогенна G', которая является произведением групп Витта.

По лемме 7 существует $f_i \in \operatorname{Hom}(W_{n_i}, W_{n_1})$, такой, что $\gamma_i = \alpha^1_{n_1} f_i$. Определим φ: $W \to W$ формулой

$$\varphi(w_1, w_2, \ldots, w_k) = (f_1(w_1) + \ldots + f_k(w_k), w_2, \ldots, w_k)$$

Непосредственное вычисление показывает, что $\varphi^*(\beta) = \gamma$, где через γ обозначен элемент группы $\operatorname{Ext}(W, G_a)$, определяемый группой G. Для доказательства же сюръективности φ достаточно убедиться в том, что f_1 сюръективно. Последнее следует из леммы 6, поскольку $\alpha^1_{n_1} f_1 \neq 0$.

Замечания. 1. В изогении между G и $\prod W_{n_i}$ имеет место *единственность* целых чисел n_i (с точностью до порядка). Действительно, обозначим через u_n число целых чисел, равных n. Немедленно проверяется формула

$$u_n = \dim(p^{n-1}G/p^nG) - \dim(p^nG/p^{n+1}G). \tag{27}$$

2. Теорема 1 аналогична теореме о структуре абелевых p-групп. Эту аналогию можно продолжить; например, можно показать, что подгруппа H унипотентной связной группы G является „квазипрямым множителем“ в G (прямым множителем с точностью до изогения) в том и только в том случае, когда эта подгруппа „квазичистая“, т. е. когда $\dim p^nH = \dim(H \cap p^nG)$ для всех n.

11. Структура связных унипотентных групп. Некоторые частные случаи

Теорема 1 определяет структуру связных унипотентных групп с точностью до изогении. В некоторых же случаях можно утверждать больше. Например:

Предложение 11. *Всякая связная (коммутативная) унипотентная группа периода p изоморфна произведению групп G_a.*

Применим индукцию по $r = \dim G$ (случай $r = 1$ тривиален). Будем считать, что группа G является расширением группы G_1 с помощью группы G_a. По предположению индукции имеем $G_1 = (G_a)^{r-1}$, и G определяется $r-1$ элементами $\gamma_i \in \operatorname{Ext}(G_a, G_a)$. Если один из γ_i, например γ_1, не равен нулю, то из доказательства теоремы 1 следует, что G изогенна $W_2 \times (G_a)^{r-2}$. Это противоречит тому, что период G равен p. Если все $\gamma_i = 0$, то $G = G_a \times G_1 = (G_a)^r$. Предложение доказано.

(Непосредственное доказательство см. у Розенлихта [6], предложение 2.)

Если размерность G равна 2, можно легко получить полную систему инвариантов. Исключая случай $G = (G_a)^2$, положим $G' = pG$ и обозначим через G'' подгруппу группы G, образованную элементами $x \in G$, такими, что $px = 0$. Группа G'' имеет размерность 1; ее связная компонента единицы равна G'. Факторгруппа G''/G' является конечной подгруппой G/G', которую можно отождествить с G_a. Таким образом, получаем *первый инвариант*, конечную подгруппу N группы G_a, определяемую с точностью до ненулевой гомотетии. С другой стороны, отображение $x \to px$ определяет при переходе к фактору биективный гомоморфизм $G/G'' \to G'$ с нулевым касательным отображением. Следовательно, этот гомоморфизм является радикальной изогенией степени p^h, где $h \geqslant 1$. Целое число h является *вторым инвариантом* группы G.

Используя лемму 3, нетрудно проверить, что инварианты N и h *характеризуют* G с точностью до изоморфизма и что их можно выбирать произвольными. Группа G *сепарабельно* (соответственно *радикально*) изогенна W_2 в том и только в том случае, когда $h = 1$ (соответственно $N = 0$).

12. Другие результаты

Теорема 2. *Всякая связная (коммутативная) унипотентная группа изоморфна подгруппе произведения групп Витта.*

Пусть G — такая группа и r — ее размерность. Применим индукцию по r (случай $r = 1$ тривиален) Группа G является расширением группы G_a с помощью G_1 размерности $r-1$. По предположению индукции G_1 погружается в произведение W групп Витта, а G погружается в соответствующее расширение G_a с помощью W. Следовательно, все сводится к случаю $G_1 = W$.

Пусть $W = \prod_{i=1}^{m} W_{n_i}$ — разложение W в произведение групп Витта. Элемент $G \in \mathrm{Ext}(G_a, W)$ определяется семейством элементов $\gamma_i \in \mathrm{Ext}(G_a, W_{n_i})$. По лемме 4′ существует $\varphi_i \in A_1$, такой, что $\gamma_i = \alpha_1^{n_i}\varphi_i$. Положим

$$L = \prod_{i=1}^{m} W_{n_i+1} \times G_a.$$

L можно рассматривать естественным образом как расширение $(G_a)^m \times G_a$ с помощью W; пусть $\beta \in \mathrm{Ext}((G_a)^m \times G_a, W)$ — соответствующий этому расширению элемент. Определим тогда гомоморфизм θ: $G_a \to (G_a)^m \times G_a$ формулой

$$\theta(x) = (\varphi_1(x), \ldots, \varphi_m(x), x).$$

Немедленно проверяется, что $\beta\theta = G$. Таким образом, существует гомоморфизм ψ: $G \to L$, приводящий к коммутативной диаграмме

$$\begin{tikzcd} 0 \arrow[r] & W \arrow[r] \arrow[d, "\mathrm{Id}"] & G \arrow[r] \arrow[d, "\psi"] & G_a \arrow[r] \arrow[d, "\theta"] & 0 \\ 0 \arrow[r] & W \arrow[r] & L \arrow[r] & (G_a)^m \times G_a \arrow[r] & 0 \end{tikzcd}$$

Кроме того, θ погружает G_a в $(G_a)^m \times G_a$, а следовательно, ψ погружает G в L, чем и заканчивается доказательство.

Теорема 3. *Всякая связная (коммутативная) унипотентная группа изоморфна фактору произведения групп Витта по связной подгруппе.*

Доказательство этой теоремы „двойственно“ предыдущему доказательству. Применяем индукцию по размерности группы G, рассматривая G как расширение G_a с помощью группы G_1. Используя предположение индукции, можем считать G_1 равным произведению $\prod_{i=1}^{m} W_{n_i}$ групп Витта. Используя лемму 4, показываем, как и прежде, что G_1 изоморфна фактору группы $\prod_{i=1}^{i=m} W_{n_{i+1}} \times G_a$ по связной подгруппе [изоморфной $(G_a)^m$].

13. Сравнение с обобщенными якобиевыми многообразиями

Пусть $J_{\mathfrak{m}}$ — обобщенное якобиево многообразие кривой X относительно модуля $\mathfrak{m} = \sum n_P P$ с носителем S. Мы видели в гл. V, что $J_{\mathfrak{m}}$ является расширением обыкновенного якобиева многообразия J кривой X с помощью линейной группы $L_{\mathfrak{m}}$, которая изоморфна произведению тора на унипотентную группу $V = \prod_{P \in S} V_{(n_P)}$. Мы убедились также с помощью экспоненты Артина — Хассе, что группа V *изоморфна* (а не только изогенна) произведению групп Витта. Этот факт можно использовать для нового доказательства теоремы 3. Докажем сначала следующий результат.

Теорема 4. *Всякая связная (коммутативная) группа изоморфна фактору произведения обобщенных якобиевых многообразий по связной подгруппе.*

Пусть G — такая группа, e — ее нейтральный элемент. Поскольку e — простая точка на G, существуют кривые X'_i на G, для которых e — простая точка и касательные к которым в этой точке порождают касательное пространство $\mathfrak{t}_a$. Если X_i обозначает нормальную модель X'_i, то рациональное отображение $X_i \to X'_i \to G$ представляется в виде $X_i \to J_i \to G$, где J_i — обобщенное якобиево многообразие кривой X_i.

Полагая $J = \prod J_i$, видим, что сумма гомоморфизмов $J_i \to G$ определяет гомоморфизм θ: $J \to G$. Образ $\mathfrak{t}_g$ при отображении θ содержит касательные $\mathfrak{t}_i$ кривых X_i'. Таким образом, $\theta(\mathfrak{t}_G) = \mathfrak{t}_G$. Это показывает одновременно, что θ *сюръективно* и *сепарабельно*. Следовательно, группу G можно отождествить с фактором J/N, где N обозначает ядро θ. Осталось установить, что N связно. Для этого нам придется ввести еще одно обобщенное якобиево многообразие.

Пусть N_0 — связная компонента единицы группы N и $G_0 = J/N_0$. Тогда $(J/N_0)/(N/N_0) = J/N = G$. Каноническая проекция $G_0 \to G$ является, следовательно, сепарабельной изогенией. Если $\dim G \geqslant 2$, то теорема Бертини (гл. VI, лемма 11) показывает, что обратный образ в G_0 подходящего гиперплоского сечения G неприводим. С помощью индукции получаем существование кривой X_1' на G, прообраз которой в G_0 неприводим (это верно лишь при $\dim G \geqslant 1$; но случай $\dim G = 0$ тривиален). Если X_1 обозначает нормальную модель X_1', то отображение $X_1 \to G$ определяет, как и выше, гомоморфизм

$$\theta_1\colon\ J_1 \to G,$$

где J_1 — обобщенное якобиево многообразие X_1. Пусть J_0 — обратный образ G_0 при отображении θ_1, т. е. подгруппа в $J_1 \times G_0$, образованная парами, имеющими одинаковый образ в G. Группа J_0 связна, так как в противном случае прообраз X_1' в G_0 не был бы неприводимым. Определим теперь гомоморфизм φ: $J \times J_1 \to G$, полагая $\varphi(j, j_1) = \theta(j) - \theta_1(j_1)$. Поскольку отображение $\mathfrak{t}_J \to \mathfrak{t}_G$ сюръективно, то таким же будет и отображение $\mathfrak{t}_{J \times J_1} \to \mathfrak{t}_G$. Это показывает, что φ *сюръективно* и *сепарабельно*. Далее, ядро M этого отображения является расширением группы J_0 с помощью N_0. Так как обе эти группы связны, то и M *связна*. Теорема доказана.

Следствие. *Всякое абелево многообразие изоморфно фактору произведения (обычных) якобиевых многообразий по связной подгруппе.*

Пусть G — абелево многообразие. По предыдущей теореме $G = \prod J_{\mathfrak{m}_i}/N$, где $J_{\mathfrak{m}_i}$ — обобщенные якобиевы многообразия, а N — связная группа. Пусть $L_{\mathfrak{m}_i}$ обозначает линейную часть J_{m_i}. Гомоморфизм $L_{m_i} \to G$ обязательно тривиален. Это означает, что N содержит все L_{m_i}. Полагая тогда $J_i = J_{m_i}/L_{m_i}$, видим, что G отождествляется с фактором $\prod J_i/N'$, где N' — образ N (а следовательно, связен). Так как J_i — обычные якобиевы многообразия, следствие доказано.

Вернемся теперь к случаю, когда G — *унипотентная* группа. Согласно следствию предложения 7, многообразие G изоморфно аффинному пространству k^n. В доказательстве теоремы 4 можно взять в этом случае в качестве кривых X_i' и X_i *прямые*; соответствующие якобиевы многообразия сводятся к их унипотентным частям, которые изоморфны произведению групп Витта, как упоминалось выше. Таким образом, теорема 3 доказана.

Отметим, что из теоремы 3 можно легко получить доказательство теоремы 1.

§ 3. Расширения абелевых многообразий

14. Классы примитивных когомологий

Пусть A — абелево многообразие, и B — связная линейная группа. По предложению 6 $\mathrm{Ext}(A, B) = H^2_{\mathrm{rat}}(A, B)_s$, а согласно п. 5, имеет место гомоморфизм

$$\pi\colon H^2_{\mathrm{rat}}(A, B)_s \to H^1(A, \mathscr{B}_A),$$

где $\mathscr{B}_A$ — пучок ростков регулярных отображений A в B. Соответствующий гомоморфизм $\mathrm{Ext}(A, B) \to H^1(A, \mathscr{B}_A)$ снова будем обозначать через π. Определим ядро и образ отображения π. Для этого нам потребуются некоторые предварительные определения гомологического характера.

Пусть q — целое число $\geqslant 1$. Для всякого алгебраического многообразия X положим $T(X) = H^q(X, \mathscr{B}_X)$. Таким образом определяется контрвариантный функтор на X, обращающийся в нуль, если X сводится к точке. Если $f\colon X \to Y$ — рациональное отображение, то гомоморфизм, соответствующий f, обозначим через $f^*\colon T(Y) \to T(X)$.

Пусть теперь X_1 и X_2 — два многообразия с „отмеченной" точкой на каждом из них, обозначаемой через e. Пусть $p_i\colon X_i \times X_2 \to X_i$ $(i = 1, 2)$ — проекция на i-й множитель, а m_i: $X_i \to X_1 \times X_2$ — вложение, определенное с помощью e. Этим отображениям соответствуют гомоморфизмы p_i^* и m_i^*. Так как $p_i \circ m_i$ — тождественное, а $p_i \circ m_j$ $(i \neq j)$ — постоянное отображение, имеем формулы

$$m_i^* \circ p_i^* = 1, \quad m_j^* \circ p_i^* = 0 \quad \text{при} \quad i \neq j. \tag{28}$$

Эти формулы означают, что гомоморфизм p^*: $T(X_1) \times \times T(X_2) \to T(X_1 \times X_2)$, определяемый (p_1^*, p_2^*), имеет в качестве левого обратного гомоморфизм, определяемый m_i^*. Таким образом, можно *отождествлять* $T(X_1) \times (X_2)$ *с прямым сомножителем* $T(X_1 \times X_2)$ (см. Картан и Эйленберг [1], стр. 18). Элемент группы $T(X_1 \times X_2)$, входящий в этот сомножитель, называется *разложимым*.

Применим все это к случаю $X_1 = X_2 = A$, где A — алгебраическая (коммутативная) группа. Группа $T(A \times A)$ содержит, таким образом, группу $T(A) \times T(A)$ в качестве прямого множителя. Пусть $x \in T(A)$ и s_A: $A \times A \to A$ — закон композиции A. Имеем $s_A^*(x) \in T(A \times A)$. Так как отображение $s_A \circ m_i$ тождественно ($i = 1, 2$), то компонента $s_A^*(x)$ в множителе $T(A) \times T(A)$ равна (x, x). Говорят, что x *примитивен*, если

$$s_A^*(x) = (x, x) \quad [\text{т. е. } p_1^*(x + p_2^*(x)], \tag{29}$$

другими словами, если $s_A^*(x)$ *разложим*.

Обозначим через $PT(A)$ подгруппу в $T(A)$, образованную примитивными элементами $T(A)$.

Лемма 8. *$PT(A)$ является аддитивным функтором A.*

Прежде всего надо показать, что если φ: $A \to C$ — гомоморфизм, то φ^* отображает $PT(C)$ в $PT(A)$. Это немедленно следует из рассмотрения соответствующей диаграммы. Кроме того, надо показать, что $PT(A)$ *аддитивен* по A, т. е. если φ, ψ, $\theta \in \operatorname{Hom}(A, C)$ таковы, что $\theta = \varphi + \psi$, то $\theta^*(x) = \varphi^*(x) + \psi^*(x)$ для всех $x \in PT(C)$. Но гомоморфизм θ представляется в виде

$$A \xrightarrow{\chi} C \times C \xrightarrow{s_C} C,$$

где гомоморфизм χ определяется парой (φ, ψ). Имеем тогда

$$\theta^*(x) = \chi^*(s_C^*(x)) = \chi^*(p_1^*(x) + p_2^*(x)) = \varphi^*(x) + \psi^*(x),$$

поскольку $p_1 \circ \chi = \varphi$ и $p_2 \circ \chi = \psi$.

Формула (29) показывает, между прочим, что $PT(A)$ является „наибольшей" подгруппой в $T(A)$, удовлетворяющей лемме 8.

15. Сравнение $\mathrm{Ext}(A, B)$ с $H^1(A, \mathscr{B}_A)$

Теорема 5. *Пусть A — абелево многообразие и B — линейная связная (коммутативная) группа. Канонический гомоморфизм*

$$\pi\colon \mathrm{Ext}(A, B) \to H^1(A, \mathscr{B}_A) \qquad \text{(см. п. 14)}$$

инъективен и имеет в качестве образа множество примитивных элементов из $H^1(A, \mathscr{B}_A)$.

Пусть C — расширение A с помощью B, входящее в ядро π. Как расслоенное пространство C тривиально, т. е. обладает регулярным сечением $s\colon A \to C$. Применив, если нужно, перенос на элемент из B, можем считать, что $s(e) = e$ (где e — нейтральный элемент рассматриваемой группы). Поскольку A — полное многообразие, $s(A)$ — полное подмногообразие в C. Пусть A' — подгруппа в C, порожденная группой $s(A)$ она тоже является полной группой. Группа $A' \cap B$ одновременно полна и линейна, а значит, конечна. Поскольку она является ядром проекции $A' \to A$, то $\dim A' = \dim A = \dim s(A)$, откуда $A' = s(A)$, так как A неприводима и содержит $s(A)$. Это означает, что $s(A)$ — подгруппа в C, т. е. что s — гомоморфизм и что расширение C тривиально. Следовательно, гомоморфизм π *инъективен.*

Пусть теперь $C \in \mathrm{Ext}(A, B)$. Проверим, что $x = \pi(C)$ — примитивный элемент группы $H^1(A, \mathscr{B}_A)$. Отметим сначала, что π имеет функториальный характер, т. е. коммутирует с гомоморфизмами φ^*, которые определяются элементами $\varphi \in \mathrm{Hom}(A, A')$. Имеем поэтому

$$\begin{aligned} s_A^*(x) &= s_A\pi^*(C) = \pi s_A^*(C) = \\ &= \pi\left(p_1^*(C) + p_2^*(C)\right) = \text{(см. предложение 1)} \\ &= p_1^*\pi(C) + p_2^*\pi(C) = p_1^*(x) + p_2^*(x). \end{aligned}$$

Это показывает, что x примитивен.

Обратно, пусть x — примитивный элемент из $H^1(A, \mathscr{B}_A)$ и C — главное расслоенное пространство с базой A и структурной группой B, соответствующее элементу x. Нам надо доказать, что на C существует структура алгебраической группы, получающаяся из расширения A с помощью B. Пусть C' — прообраз C при отображении s_A: $A \times A \to A$. Предположение о том, что x примитивен, означает, что C' изоморфно расслоенному пространству, получающемуся из $C \times C$ при гомоморфизме s_B: $B \times B \to B$. Взяв композицию отображений $C \times C \to C'$ и $C' \to C$, получим регулярное отображение g: $C \times C \to C$, приводящее к коммутативной диаграмме

$$\begin{array}{ccc} C \times C & \xrightarrow{g} & C \\ \downarrow & & \downarrow \\ A \times A & \xrightarrow{s_A} & A \end{array} \tag{30}$$

и удовлетворяющее тождеству

$$g(c+b,\ c'+b') = g(c,\ c') + b + b' \quad (c,\ c' \in c,\ b,\ b' \in B). \tag{31}$$

Выберем точку $e \in C$, которая проектируется в нейтральный элемент e группы A. Применяя, если нужно, перенос на элемент из B, можем считать, что $g(e,\ e) = e$. Остается доказать, что g наделяет C структурой коммутативной алгебраической группы с нейтральным элементом e. Формула (31) и диаграмма (30) показывают, что C — расширение B с помощью A. Необходимо проверить:

а) *что* $g(c,\ e) = g(e,\ c) = c$ *для всех* $c \in C$.

Согласно (30), имеем $g(c,\ e) = c + h(c)$, где h — регулярное отображение C в B. Кроме того, формула (31) показывает, что $h(c+b) = h(c)$ для всех $b \in B$, т. е. что h представляется в виде $C \to A \to B$. Так как A — полная и B — линейная группы, то отображение $\bar{h}$: $A \to C$, определенное таким образом, постоянно. Далее, формула $g(e,\ e) = e$ показывает, что $\bar{h}(e) = e$, откуда $h(c) = e$ для всех $c \in C$. Это доказывает формулу $g(c,\ e) = C$. Так же рассуждаем для доказательства формулы $g(e,\ c) = C$:

б) *что* $g(c,\ c') = g(c',\ c)$ *для всех* $c,\ c' \in C$.

Согласно (30), имеем $g(c,\ c') = g(c',\ c) + k(c,\ c')$, где k — регулярное отображение $C \times C$ в B. Формула (31) показывает, что k разлагается на $C\times C \to A\times A \to B$, где отображение $A\times A\to B$ необходимо постоянно и равно e, откуда и следует результат.

в) *что* $g(c, g(c', c''))=g(g(c, c'), c'')$ *для всех* $c, c', c''\in C$.

Доказательство то же, что для а) и б).

г) *что существует регулярное отображение* $i\colon C\to C$, *такое, что* $g(c, i(c))=e$ *для всех* $c\in C$.

Обозначим через i_A (соответственно i_B) отображение $a\to -a$ (соответственно $b\to -b$) группы A (соответственно B) в себя. Очевидно, что $i_B(x)=-x$. Аналогичная формула $i_A(x)=-x$ верна потому, что x — *примитивный* элемент (лемма 8). Поскольку $i_A(x)=i_B(x)$, существует регулярное отображение $i\colon C\to C$, приводящее к коммутативной диаграмме

$$\begin{array}{ccc} C & \xrightarrow{i} & C \\ \downarrow & & \downarrow \\ A & \xrightarrow{i_A} & A \end{array} \tag{32}$$

и удовлетворяющее тождеству

$$i(c+b)=i(c)-b \quad \text{для} \quad c\in C,\ b\in B. \tag{33}$$

Кроме того, можно считать, что $i(e)=e$. После этого при помощи рассуждений, аналогичных примененным в a), б) и в), показываем, что $g(c, i(c))=e$ для всех $c\in C$. Теорема доказана.

16. Случай $B=G_m$

В случае когда B есть мультипликативная группа G_m, пучок $\mathscr{B}_A$ совпадает с пучком $\mathcal{O}_A^*$ обратимых элементов пучка локальных колец $\mathcal{O}_A$ рассматриваемого абелевого многообразия. Группа $H^1(A, \mathcal{O}_A^*)$ есть группа $D(A)$ *классов дивизоров* в A (относительно линейной эквивалентности). Утверждение, что класс дивизоров X — примитивный элемент из $D(A)$, означает, что $s_k^{-1}(X)$ линейно эквивалентен на $A\times A$ „разложимому“ дивизору

$$X\times A+A\times X=p_1^{-1}(X)+p_2^{-1}(X),$$

что записывается также в виде $X \equiv 0$ (см. Ленг [5], стр. 90, теорема 2). Если обозначить через $P(A)$ подгруппу $D(A)$, образованную такими классами, то теорема 5 дает следующий результат.

Теорема 6. *Если A — абелево многообразие, то группа* $\mathrm{Ext}(A, G_m)$ *канонически изоморфна группе $P(A)$ классов дивизоров X на A, таких, что $X \equiv 0$.*

Известно (Барсотти [3]; см. также Серр [6]), что $X \equiv 0$ в том и только в том случае, когда X алгебраически *эквивалентно нулю*. Группа $P(A)$ является, следовательно, абелевой группой, *двойственной* к многообразию A.

Замечание. Согласно предложению 5, $\mathrm{Ext}(A, G_m) = H^2_{\mathrm{rat}}(A, G_m)_s$. Таким образом, всякий дивизор X, такой, что $X \equiv 0$, соответствует *классу систем рациональных факторов* на A со значениями в G_m. Систему факторов, входящую в этот класс, можно определить следующим образом.

Поскольку $s_A^{-1}(X) \sim p_1^{-1}(X) + p_2^{-1}(X)$ на $A \times A$, существует рациональная функция $f(x, y)$ на $A \times A$, такая, что

$$(f) = s_A^{-1}(X) - p_1^{-1}(X) - p_2^{-1}(X). \tag{34}$$

Функция f и будет искомой системой факторов.

17. Случай $B = G_a$

В случае когда B есть аддитивная группа G_a, пучок B_A совпадает с пучком локальных колец $\mathfrak{O}_A$ многообразия A, что приводит к необходимости изучать группу $H^1(A, \mathfrak{O}_A)$.

Вообще если X — произвольное алгебраическое многообразие, то мы пишем $H^q(X)$ вместо $H^q(X, \mathfrak{O}_X)$ и полагаем

$$H^*(X) = \sum_{q=0}^{\infty} H^q(X).$$

Операция $\cup$-произведения наделяет $H^*(X)$ структурой градуированной алгебры. Так как умножение в $\mathfrak{O}_X$ ассоциативно и коммутативно, то умножение в $H^*(X)$ ассоциативно и антикоммутативно. В $H^*(X)$ есть единичный элемент 1 степени 0 (свойства $\cup$-произведения см. в работе Годемана [1], гл. II, § 6).

Если X и Y — два многообразия, то проекции p_1 и p_2 произведения $X \times Y$ на X и на Y определяют гомоморфизмы

$$p_1^*\colon H^*(X) \to H^*(X \times Y) \text{ и } p_2^*\colon H^*(Y) \to H^*(X \times Y)$$

(см. п. 14). С помощью $\smile$-произведения получаем гомоморфизм

$$p_1^* \otimes p_2^*\colon H^*(X) \otimes H^*(Y) \to H^*(X \times Y),$$

где тензорное произведение берется над основным полем k. Имеет место „формула Кюннета":

Предложение 12. *Гомоморфизм $p_1^* \otimes p_2^*$, определенный выше, есть изоморфизм группы $H^*(X) \otimes H(Y)$ на $H^*(X \times Y)$.*

Доказательство то же, что и в классическом случае. Выберем конечное покрытие $\mathfrak{U}$ (соответственно $\mathfrak{V}$) многообразия X (соответственно Y) открытыми аффинными множествами U_i (соответственно V_j). Множества $W_{ij} = U_i \times V_j$ образуют тогда конечное покрытие $\mathfrak{W}$ многообразия $X \times Y$ аффинными открытыми множествами. Согласно АКП (стр. 239, теорема 4), группы когомологий X являются группами когомологий комплекса $C(\mathfrak{U}, \mathfrak{S}_X)$, „комплекса симплициальных цепей" по терминологии Годемана [1], гл. I, § 3.1. Аналогичный результат имеет место для Y и для $X \times Y$. Кроме того,

$$\Gamma\left(W_{i_0 j_0, \ldots, i_p j_p}, \mathfrak{S}_{X \times Y}\right) = \Gamma\left(U_{i_0 \ldots i_p}, \mathfrak{S}_X\right) \otimes \Gamma\left(V_{j_0 \ldots j_p}, \mathfrak{S}_Y\right),$$

поскольку координатное кольцо произведения аффинных многообразий является тензорным произведением координатных колец этих многообразий. Эта формула означает, что комплекс $C(\mathfrak{W}, \mathfrak{S}_{X \times Y})$ отождествляется с *декартовым произведением* $C(\mathfrak{U}, \mathfrak{S}_X) \times C(\mathfrak{V}, \mathfrak{S}_Y)$ комплексов $C(\mathfrak{U}, \mathfrak{S}_X)$ и $C(\mathfrak{V}, \mathfrak{S}_Y)$ (определение декартового произведения двух комплексов симплициальных цепей см. у Годемана [1], гл. I, § 3.6). По теореме Эйленберга — Зильбера (Годеман [1], теорема 3.10.1) комплекс $C(\mathfrak{W}, \mathfrak{S}_{X \times Y})$ гомотопно эквивалентен тензорному произведению

$$C(\mathfrak{U}, \mathfrak{S}_X) \otimes C(\mathfrak{V}, \mathfrak{S}_Y).$$

Применяя (обычную) формулу Кюннета к последнему комплексу, получаем, что $H^*(X \times Y)$ отождествляется с тензорным произведением $H^*(X)$ и $H^*(Y)$. Наконец, то, что это отождествление задается $\cup$-произведением p_1^* и p_2^*, проверяется либо при помощи явной формулы, задающей $\cup$-произведение и сравнением с доказательством теоремы Эйленберга — Зильбера, либо наконец при помощи диагонального отображения с использованием определения $\cup$-произведения (Годеман [1], гл. II, § 6).

Следствие. *Если X и Y — связные и полные многообразия, то $H^1(X \times Y)$ отождествляется с прямой суммой $H^1(X)$ и $H^1(Y)$.*

Действительно, предыдущее предложение показывает, что $H^1(X \times Y)$ есть прямая сумма $H^1(X) \otimes H^0(Y)$ и $H^0(X) \otimes \otimes H^1(Y)$, а предположения относительно X и Y дают

$$H^0(X) = H^0(Y) = k.$$

Замечание. Формула Кюннета имеет место для произвольных когерентных пучков, а не только для пучков локальных колец. Более точно, если $\mathcal{F}$ и $\mathcal{G}$ — когерентные пучки на X и Y соответственно, то определим когерентный пучок $\mathcal{F} \otimes \mathcal{G}$ на $X \times Y$, полагая

$$\mathcal{F} \otimes \mathcal{G} = \mathcal{F} \otimes \mathcal{O}_{X \times Y} \otimes \mathcal{G},$$

где тензорные произведения справа берутся над $\mathcal{O}_X$ и $\mathcal{O}_Y$ соответственно. Доказательство предложения 12 показывает тогда, что $H^*(X \times Y, \mathcal{F} \otimes \mathcal{G})$ отождествляется с

$$H^*(X, \mathcal{F}) \otimes H^*(Y, \mathcal{G}).$$

Теорема 7. *Если A — абелево многообразие, то группа $\mathrm{Ext}(A, G_a)$ канонически изоморфна $H^1(A, \mathcal{O}_A)$.*

Действительно, по следствию предложения 12 всякий элемент группы $H^1(A \times A, \mathcal{O}_{A \times A})$ разложим, а следовательно, всякий элемент $H^1(A, \mathcal{O}_A)$ примитивен. Применение теоремы 5 дает нужное утверждение.

Замечания. 1. Как будет показано в п. 21, размерность векторного пространства $H^1(A, \mathcal{O}_A)$ над полем k равна $\dim A$.

2. Если p — характеристика основного поля, то с помощью теоремы 7 можно определить $\mathrm{Ext}(A, \mathbf{Z}/p\mathbf{Z})$. Действи-

тельно, если обозначить через $\wp$; $G_a \to G_a$ изогению, определяемую формулой $\wp(\lambda) = \lambda^p - \lambda$ (см. гл. VI), то будет иметь место строго точная последовательность

$$0 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow G_a \xrightarrow{\wp} G_a \longrightarrow 0.$$

Применяя вторую точную последовательность для Ext (§ 1, предложение 3), видим что $\operatorname{Ext}(A, \mathbf{Z}/p\mathbf{Z})$ отождествляется с ядром изогении $\wp$, действующей на $H^1(A, \mathcal{O}_A)$. Но теорема Артина — Шрейера показывает, что элементы этого ядра соответствуют неразветвленным циклическим накрытиям степени p многообразия A (см. Серр [5], п. 16); таким образом, получается частный случай теоремы, по которой *всякое неразветвленное накрытие абелева многообразия является изогенией* (Ленг и Серр [1], теорема 2). В случае циклического накрытия степени, взаимно простой с p, можно проделать аналогичное рассуждение, использовав группу G_m вместо G_a и теорему 6 вместо теоремы 7 (см. Вейль [5], § XI).

18. Случай, когда B — унипотентная группа

Прежде всего обобщим следствие предложения 12.

Предложение 13. *Пусть B — связная (коммутативная) унипотентная группа. Если X и Y — полные и связные многообразия, то* $H^1(X \times Y, \mathcal{B}_{X \times Y})$ отождествляется с прямой суммой $H^1(X, \mathcal{B}_X)$ и $H^1(Y, \mathcal{B}_Y)$.

Применим индукцию по $n = \dim B$. Случай $n = 1$ является следствием предложения 12. Если $n > 1$, то выберем связную подгруппу B' группы B, такую, что $B/B' = G_a$. Точная последовательность пучков

$$0 \to \mathcal{B}'_X \to \mathcal{B}_X \to \mathcal{O}_X \to 0$$

порождает точную последовательность когомологий

$$\begin{aligned} H^0(X, \mathcal{B}_X) - H^0(X, \mathcal{O}_X) - H^1(X, \mathcal{B}'_X) \\ \to H^1(X, \mathcal{B}_X) \to H^1(X, \mathcal{O}_X). \end{aligned}$$

Но, поскольку X — полное и связное многообразие, всякое регулярное отображение X в группы B', B или G_a

постоянно. Таким образом, $H^0(X, \mathscr{B}_X) = B$ и $H^0(X, \mathfrak{G}_X) = G_a$. Предыдущая точная последовательность сводится к последовательности

$$0 \to H^1(X, \mathscr{B}'_X) \to H^1(X, \mathscr{B}_X) \to H^1(X, \mathfrak{G}_X). \qquad (35)$$

Аналогичные результаты имеем для Y и $X \times Y$. С другой стороны, если отметить „базисные" точки в X и Y, то соответствующие инъекции X и Y в $X \times Y$ определят гомоморфизм

$$m^*\colon H^1(X \times Y, \mathscr{B}_{X \times Y}) \to H^1(X, \mathscr{B}_X) \times H^1(Y, \mathscr{B}_Y).$$

Известно, что m^* сюръективен и имеет в качестве правого обратного гомоморфизм p^*, определенный проекциями $X \times Y \to X$ и $X \times Y \to Y$ (см. п. 14). Таким образом, все сводится к доказательству того, что m^* инъективен. Однако, согласно (35), имеем коммутативную диаграмму

$$\begin{array}{ccccccc}
0 \to & H^1(X \times Y, \mathscr{B}'_{X \times Y}) & \to & H^1(X \times Y, \mathscr{B}_{X \times Y}) & \to & H^1(X \times Y, \mathfrak{G}_{X \times Y}) \\
& \downarrow{\scriptstyle m^*} & & \downarrow{\scriptstyle m^*} & & \downarrow{\scriptstyle m^*} \\
0 \to & H^1(X, \mathscr{B}'_X) \times H^1(Y, \mathscr{B}'_Y) & \to & H^1(X, \mathscr{B}_X) \times H^1(Y, \mathscr{B}_Y) & \to & H^1(X, \mathfrak{G}_X) \times H^1(Y, \mathfrak{G}_Y).
\end{array}$$

По предположению индукции обе крайние вертикальные стрелки являются биекциями. Таким образом, средняя стрелка также является биекцией, что и завершает доказательство предложения.

Теорема 8. *Пусть A — абелево многообразие, а B — связная унипотентная (коммутативная) группа. Канонический гомоморфизм*

$$\pi\colon \operatorname{Ext}(A, B) \to H^1(A, \mathscr{B}_A),$$

определенный в п. 14, *биективен.*

Действительно, предложение 13 показывает, что всякий элемент группы $H^1(A \times A, \mathscr{B}_{A \times A})$ разложим, а следовательно, всякий элемент из $H^1(A, \mathscr{B}_A)$ примитивен. Воспользовавшись теоремой 5, получаем искомый результат.

§ 4. *Когомологии якобиевых многообразий*

19. Когомологии якобиевых многообразий

Пусть X — неприводимая проективная кривая без особенностей и φ: $X \to J$ — каноническое отображение X в ее якобиево многообразие. Это отображение определяет гомоморфизм φ^*: $H^1(J, \mathscr{O}_J) \to H^1(X, \mathscr{O}_X)$. Хотя φ определяется лишь с точностью до переноса, φ^* определяется единственным образом, поскольку, согласно формуле Кюннета, переносы на $H^*(J)$ действуют тривиально.

Теорема 9. *Гомоморфизм* φ^*: $H^1(J, \mathscr{O}_J) \to H^1(X, \mathscr{O}_X)$ *биективен.*

Заметим, что $H^1(J, \mathscr{O}_J) = \mathrm{Ext}(J, G_a)$ по теореме 7. Так как отображение φ максимально (в смысле гл. VI, п. 13), то *инъективность* φ^* будет следовать из более общего предложения:

Предложение 14. *Пусть* X — *полное многообразие,* A — *абелево многообразие, а* B — *связная линейная* (*коммутативная*) *группа. Если* φ: $X \to A$ — *максимальное всюду регулярное отображение, то композиция гомоморфизмов*;

$$\mathrm{Ext}(A, B) \xrightarrow{\pi} H^1(A, \mathscr{B}_A) \xrightarrow{\varphi} H^1(X, \mathscr{B}_X)$$

инъективна.

Пусть C — расширение A с помощью B. Утверждение, что C входит в ядро гомоморфизма $\mathrm{Ext}(A, B) \to H^1(X, \mathscr{B}_A)$, означает, что расслоенное пространство, являющееся прообразом C при отображении φ, тривиально, другими словами, что φ представляется в виде $X \xrightarrow{\psi} C \longrightarrow A$, где ψ — регулярное отображение. Применив, если нужно, к ψ перенос, можем считать, что $\psi(X)$ содержит нейтральный элемент e группы C. Пусть A' — подгруппа C, порожденная $\psi(X)$. Так как X — полное многообразие, таковым же будет и $\psi(X)$, а следовательно, и A'. Группа $A' \cap B$, являющаяся одновременно полной и линейной, необходимо конечна. Поскольку она является ядром проекции $A' \to A$, представимость φ в виде $X \to A' \to A$ показывает, что гомоморфизм

$A' \to A$ является изоморфизмом (это есть определение максимальных отображений). Расширение C, таким образом, тривиально, что и доказывает предложение.

Вернемся теперь к доказательству теоремы 9. Для доказательства *сюръективности* φ^* мы будем пользоваться обобщенными якобиевыми многообразиями, которые являются расширениями J.

Более точно, при $P \in X$ положим $\mathfrak{m} = 2P$. Обобщенное якобиево многообразие $J_{\mathfrak{m}}$ является расширением J с помощью локальной группы $L_{\mathfrak{m}}$. Если t — локальная униформизующая в P, то группа $L_{\mathfrak{m}} = U_P^{(1)}/U_P^{(2)}$ является группой функций вида $1 + at + \ldots$ по модулю функций вида $1 + bt^2 + \ldots$. Таким образом, $L_m = G_a$. Для $j_P \in \operatorname{Ext}(J, G_a) = H^1(J, \mathfrak{O}_J)$, соответствующего $J_{\mathfrak{m}}$, положим $j'_P = \varphi^*(j_P)$. Для нахождения j'_P отождествим $H^1(X, \mathfrak{O}_X)$ с пространством $R/(R(0) + k(X))$ классов распределений на X (см. гл. II, предложение 3). Имеем

Предложение 15. *Элемент j'_P, соответствующий $J_{\mathfrak{m}}$, равен классу распределения r, определенного следующим образом: $r_P = 1/t$ и $r_Q = 0$ при $Q \neq P$.*

Пусть U_i — открытое покрытие J, такое, что существуют регулярные сечения s_i многообразия $J_{\mathfrak{m}}$ над U_i. Предположим, что $\varphi(P) \in U_0$. Функции $f_{ij} = s_i - s_j$ образуют 1-коцикл со значениями в $\mathfrak{O}_J$ и класс этого коцикла равен j_P (см. п. 5). Функции $f_{ij} \circ \varphi = g_{ij}$ определяют поэтому на X 1-коцикл из класса j'_P. Пусть $\varphi_{\mathfrak{m}}$ — каноническое отображение X в $J_{\mathfrak{m}}$, нормализованное так, что композиция $X \to J_{\mathfrak{m}} \to J$ равна φ. Функции $h_i = \varphi_{\mathfrak{m}} - \varphi \circ s_i$ задают рациональные отображения X в G_a и $h_j - h_i = -g_{ij}$. Функции h_i определяют, таким образом, элемент $h \in R/R(0)$, принадлежащий классу $-j'_P$, и остается лишь доказать, что h и $-r$ принадлежат тому же классу. В каждой точке $Q \neq P$ имеем $h_Q = 0$, поскольку $\varphi_{\mathfrak{m}}$ регулярно в Q (гл. V, предложение 4). Надо, следовательно, доказать, что $h_P = -1/t$, т. е. что *нерегулярная составляющая h_0 в P равна* $-1/t$. Это можно было бы проверить, используя локальные символы и их явное определение в случае группы G_a (см. гл. III, п. 3). Следующий метод, предложенный Розенлихтом [6], имеет то преимущество, что применим к произвольным обобщенным якобиевым многообразиям (см. п. 20).

Для всякого элемента λ проективной прямой Λ положим $H_\lambda = t^{-1}(\lambda)$. Для $Q \in X$ положим

$$D_Q = H_{t(Q)} - H_\infty = (t - t(Q)) = (1 - t/t(Q)).$$

Дивизор $H_{t(Q)}$ может быть записан в виде $Q + H'_Q$, где H'_Q — положительный дивизор. Кроме того, отображение $Q \to H'_Q$ является регулярным отображением кривой X в ее симметрическое произведение, в чем легко убедиться, применяя лемму 14 из гл. V к накрытию ψ: $X \to \Lambda$. Определим рациональное отображение ψ: $X \to J_\mathfrak{m}$ формулой

$$\psi(Q) = \varphi_\mathfrak{m}(D_Q) = \varphi_\mathfrak{m}(Q) + \varphi_\mathfrak{m}(H'_Q) - \varphi_\mathfrak{m}(H_\infty). \qquad (36)$$

Это отображение регулярно вне дивизора нулей t. Так как D_Q — дивизор функции $1 - t/t(Q)$, то $\psi(Q)$ совпадает с каноническим образом этой функции в локальной группе $L_\mathfrak{m} = G_a$ и, таким образом, равно $-1/t(Q)$. С другой стороны, при $Q = P$ дивизор H'_Q равен нулю в P, поскольку t имеет простой нуль в P. Формула (36) показывает тогда, что $\psi(Q) - \varphi_\mathfrak{m}(Q)$ как функция от Q регулярна в P. Так как то же самое справедливо для функции $\varphi_\mathfrak{m} - h_0 = \varphi \circ s_0$ (см. выше), получаем, что $\psi - h_0$ регулярна в P, т. е. что h_0 имеет нерегулярную составляющую $-1/t$, что и завершает доказательство предложения.

Докажем теперь, что отображение φ^*: $H^1(J, \mathcal{O}_J) \to H^1(X, \mathcal{O}_X)$ сюръективно. Действительно, пусть ω — ортогональный к образу φ^* элемент двойственного пространства к пространству $H^1(X, \mathcal{O}_X)$. По теореме двойственности (гл. II, п. 8) ω отождествляется с *дифференциальной формой*, всюду регулярной на X. Если P — произвольная точка X и t — локальная униформизующая в P, то предложение 15 показывает, что образ φ^* содержит распределение r, равное $1/t$ в P и 0 в остальных точках X. Таким образом, $\langle \omega, r \rangle = 0$, или $\operatorname{Res}\left(\frac{1}{t}\,\omega\right) = 0$. Значит, $\omega = 0$ в P. Это имеет место для всех P, а поэтому $\omega = 0$, чем доказана сюръективность φ^*, а вместе с тем и теорема 9.

Замечание. Можно дать более изящную формулировку предложения 15 в терминах *касательных векторов*. Пусть $\vec{v}$ — ненулевой касательный вектор в точке P. Этому вектору можно двумя способами поставить в соответствие элемент из $H^1(X, \mathscr{O}_X)$:

а) Вектор $\vec{v}$ определяет линейную форму на $H^0(X, \Omega^1)$, а тем самым и элемент двойственного ему пространства $H^1(X, \mathscr{O}_X)$.

б) Вектор $\vec{v}$ определяет изоморфизм локальной группы $L_\mathfrak{m}$ (где $\mathfrak{m} = 2P$) на G_a, а якобиево многообразие $J_\mathfrak{m}$ определяет посредством этого изоморфизма элемент группы $H^1(J, \mathscr{O}_J)$. Образ этого элемента при отображении φ^* и дает нам элемент из $H^1(X, \mathscr{O}_X)$.

Предложение 15 сводится тогда к утверждению, что два определенных таким образом элемента из $H^1(X, \mathscr{O}_X)$ совпадают.

20. Нерегулярная часть отображений $\varphi_\mathfrak{m}$

Пусть $\mathfrak{m} = \sum n_P P$ — модуль на X с носителем S и $\varphi_\mathfrak{m}$: $X \to J_\mathfrak{m}$ — каноническое отображение X в соответствующее обобщенное якобиево многообразие. Группа $J_\mathfrak{m}$ является расширением обыкновенного якобиевого многообразия J с помощью локальной группы $L_\mathfrak{m}$; прообраз $J_\mathfrak{m}$ определяет главное расслоенное пространство $P_\mathfrak{m}$ с базой X и структурной группой $L_\mathfrak{m}$, а $\varphi_\mathfrak{m}$ — рациональное сечение $P_\mathfrak{m}$. Отсюда следует, как и в предыдущем пункте, что для определения расслоенного пространства $P_\mathfrak{m}$ необходимо определить „нерегулярную часть“ $\varphi_\mathfrak{m}$ в точке $P \in S$, т. е. построить регулярное отображение ψ: $X \to L_\mathfrak{m}$, такое, что $\varphi_\mathfrak{m} - \psi$ регулярно в P.

Так как $L_\mathfrak{m} = \left(\prod U_P/U_P^{n_P}\right)/G_\mathfrak{m}$, все сводится к построению рационального отображения ψ_P: $X \to U_P/U_P^{(n_P)}$ для данной точки $P \in X$. Это построение проводится следующим образом.

Пусть Δ — диагональ $X \times X$ и F — рациональная функция на $X \times X$, дивизор которой имеет вид

$$(F) = \Delta + R, \quad \text{где} \quad (P,\ P) \notin \operatorname{Supp}(R).$$

Такая функция существует: если t — локальная униформизующая в P, то можно положить $F(Q,\ Q') = t(Q) - t(Q')$. Для всех точек Q, принадлежащих открытому непустому подмножеству U многообразия X, функция $F_Q(Q') = F(Q,\ Q')$ рациональна по $Q' \in U_P$ и ее класс F_Q в локальной группе $U_P/U_P^{(n_P)}$ вполне определен. Легко проверяется, что $Q \to F_Q$ — регулярное отображение U в группу $U_P/U_P^{(n_P)}$, а рассуждения предложения 15 показывают, что *оно является искомым отображением* ψ_P. Это определение аналогично определению Вейля дифференциалов на кривой ([4], § II).

Отметим также, что, согласно предложению 10 из гл. V, локальный символ $(\psi_P,\ g)_P$, $g \in U_P$, равен обратному элементу к $\bar{g} \in U_P/U_P^{(n_P)}$.

21. Когомологии абелевых многообразий

Пусть A — абелево многообразие размерности g и

$$H^*(A) = \sum_{n=0}^{\infty} H^n(A,\ \mathcal{O}_A)$$

— его алгебра когомологий (см. п. 17). Закон композиции

$$s\colon\ A \times A \to A$$

определяет при переходе к когомологиям гомоморфизм

$$s^*\colon\ H^*(A) \to H^*(A \times A).$$

По формуле Кюннета (предложение 12) алгебра $H^*(A \times A)$ отождествляется с $H^*(A) \otimes H^*(A)$. Пользуясь тем, что A обладает нейтральным элементом, убеждаемся в том, что для всех $x \in H^n(A)$, $n > 0$, имеем

$$s^*(x) = x \otimes 1 + \sum y_i \otimes z_i + 1 \otimes x, \qquad \deg(y_i) > 0, \quad \deg(z_i) > 0. \tag{37}$$

Это тождество означает, **что алгебра** $H^*(A)$, снабженная отображением

$$s^*: H^*(A) \to H^*(A) \otimes H^*(A),$$

является *алгеброй Хопфа* в смысле Бореля [1], § 6. Заметим, что имеет место следующий результат.

Предложение 16. *Пусть H — ассоциативная, антикоммутативная и связная алгебра Хопфа (сводящаяся к скалярам в случае размерности нуль). Пусть g — целое число, такое, что $H^n = 0$ для $n > g$. Тогда $\dim H \leqslant g$, и если имеет место знак равенства, то H отождествляется с внешней алгеброй векторного пространства H^1.*

По теореме Хопфа — Бореля (Борель [1], теорема 6.1), алгебра H изоморфна тензорному произведению над основным полем k моногенных алгебр $k[x_i]$; положим $n_i = \deg(x_i)$.

Произведение всех x_i есть ненулевой элемент из H, степень которого равна $\sum n_i$. Отсюда следует неравенство $\sum n_i < g$. В частности, число элементов x_i степени 1 не больше g. Так как это число равно $\dim H^1$, то $\dim H^1 \leqslant g$. Если $\dim H^1 = g$, то все x_i необходимо имеют степень 1. Кроме того, их квадраты равны нулю, ибо если бы, например, $x_1^2 \neq 0$, то произведение $x_1^2 \otimes x_2 \otimes \ldots \otimes x_g$ было бы ненулевым элементом H степени $g+1$, что невозможно. Таким образом, алгебра H действительно отождествляется с внешней алгеброй H^1.

Возвратимся теперь к алгебре $H^*(A)$.

Теорема 10. *Если A — абелево многообразие размерности g, то $\dim H^1(A) = g$ и алгебра $H^*(A)$ отождествляется с внешней алгеброй пространства $H^1(A)$.*

Заметим прежде всего, что $H^*(A)$ удовлетворяет предположениям предложения 16: $H^0(A) = k$, поскольку A—связное и полное многообразие; $H^n(A) = 0$ для $n > g$, так как $\dim A = g$ (Серр [4], теорема 2, или Гротендик [1], теорема 3.6.5). Таким образом, $\dim H^1(A) \leqslant g$, и остается доказать неравенство в другую сторону $\dim H^1(A) \geqslant g$.

Согласно следствию теоремы 4 (п. 13), существует строго точная последовательность

$$0 \to B \to C \to A \to 0, \tag{38}$$

где C — произведение якобиевых многообразий, а B — абелево многообразие. Так как $\operatorname{Hom}(B, G_a) = 0$, то соответствующая (38) точная последовательность для Ext записывается в виде

$$0 \to \operatorname{Ext}(A, G_a) \to \operatorname{Ext}(C, G_a) \to \operatorname{Ext}(B, G_a).$$

Принимая во внимание теорему 7, получаем

$$0 \to H^1(A) \to H^1(C) \to H^1(B),$$

откуда следует неравенство

$$\dim H^1(A) \geqslant \dim H^1(C) - \dim H^1(B). \tag{39}$$

По теореме 9 $\dim H^1(J) = \dim J$ для всех якобиевых многообразий J. В силу формулы Кюннета это же справедливо для всех C, являющихся произведением якобиевых многообразий. С другой стороны, как мы видели, $\dim H^1(B) \leqslant \dim B$. Неравенство (39) переписывается теперь в виде

$$\dim H^1(A) \geqslant \dim C - \dim B = \dim A,$$

что и завершает доказательство.

Замечание. Пусть $\underline{\Omega}^r$ — пучок регулярных дифференциальных форм степени r на A. Положим $h^{r,s} = \dim H^s(A, \underline{\Omega}^r)$. Поскольку расслоенное пространство касательных векторов к многообразию группы A тривиально (гл. III, предложение 16), пучок $\underline{\Omega}^r$ изоморфен прямой сумме $\binom{g}{r}$ экземпляров пучка $\mathcal{O}_A$ и из теоремы 10 вытекает, что

$$h^{r,s} = \binom{g}{r}\binom{g}{s}.$$

В частности, получаем *формулу симметрии* $h^{r,s} = h^{s,r}$ для абелевых многообразий. Как известно, в случае характеристики $p > 0$ существуют неособые многообразия, не удовлетворяющие этой формуле (см. Серр [5]).

22. Отсутствие гомологий с кручением на абелевых многообразиях

Предположим, что характеристика основного поля $p > 0$. Известно (Серр [5], § 1), что каждому алгебраическому многообразию X можно сопоставить операции *Бокштейна*, действующие на $H^{\cdot}(X)$. Говорят, что X не имеет *гомологий с кручением*, если эти операции тождественно равны 0.

Теорема 11. *Абелево многообразие A не имеет гомологий с кручением.*

Пусть A — абелево многообразие, $\beta_1, \ldots, \beta_n$ — соответствующие ему операции Бокштейна. Будем считать доказанным, что $\beta_i = 0$ для $i < n$, и покажем, что $\beta_n = 0$. Так как β_n действует на алгебре когомологий $H^*(A)$ (Серр [5], п. 3), мы видим, что β_n действует на $H^*(A) \times H^*(A)$. Далее, для β_n верна следующая формула (Серр [5], формула (8)):

$$\beta_n(x, y) = \beta_n(x) \cdot F^n(y) + (-1)^{\deg(x)} F^n(x) \beta_n(y),$$
$$x, y \in H^*(A).$$

Здесь F обозначает эндоморфизм $H^*(A)$, определенный возведением в p-ю степень на $\mathcal{O}_A$.

Поскольку по теореме 10 $H^*(A)$ порождается этими элементами степени 1, достаточно показать, что $\beta_n(x) = 0$ для $x \in H^1$. В этом случае, очевидно, $s^*(x) = x \otimes 1 + 1 \otimes x$, т. е. x — примитивный элемент $H^1(A)$ (см. п. 17). Функториальный характер β_n показывает тогда, что $y = \beta_n(x)$ — примитивный элемент степени r. Но из того, что $H^*(A)$ — внешняя алгебра, следует, как легко видеть, что всякий ненулевой примитивный элемент из $H^*(A)$ имеет степень 1. Таким образом, $y = 0$, что и требовалось доказать.

Следствие 1. *Пусть φ: $X \to A$ — максимальное всюду регулярное отображение полного многообразия X в абелево многообразие A. Если Z^1_∞ обозначает пересечение ядер операций Бокштейна β_n, действующих на $H^1(X, \mathcal{O}_X)$* (см. Серр [5], п. 7), *то* $\dim A \leqslant \dim Z^1_\infty$.

Предложение 14 показывает, что φ^*: $H^1(A, \mathcal{O}_A) \to$ $\to H^1(X, \mathcal{O}_X)$ — инъективное отображение. Поскольку $\beta_n = 0$

на $H^1(A, \mathcal{O}_A)$, образ φ^* содержится в Z^1_∞. По теореме 10 $\dim A = \dim H^1(A, \mathcal{O}_A)$, что и дает искомое неравенство.

Замечание. Во всех известных до настоящего времени случаях это следствие давало *точную грань* для $\dim A$, т. е. размерность многообразия Альбанезе для X была равна $\dim Z^1_\infty$. Было бы очень интересно дать общее доказательство этого факта [1]) (или привести контрпример).

Следствие 2. *Пусть $\varphi: X \to J$ — каноническое отображение проективной неособой кривой X в ее якобиево многообразие. Для любой связной унипотентной группы B гомоморфизм*

$$\varphi^*: H^1(J, \mathcal{B}_J) \to H^1(X, \mathcal{B}_X)$$

биективен.

Нам уже известно, что φ^* инъективно (предложение 14) и что φ^* сюръективно, если $B = G_a$ (теорема 9). Докажем, исходя из отсюда, общий случай индукцией по $\dim B$. Если $\dim B \geqslant 2$, то существует строго точная последовательность

$$0 \to B' \to B \to B'' \to 0,$$

где B', B'' — связные унипотентные группы строго меньшей размерности, чем у B. Из этой последовательности получаем коммутативную диаграмму

$$\begin{array}{ccccccc} 0 \to & H^1(J, \mathcal{B}'_J) & \to & H^1(J, \mathcal{B}_J) & \to & H^1(J, \mathcal{B}''_J) \\ & \downarrow & & \downarrow & & \downarrow \\ 0 \to & H^1(X, \mathcal{B}'_X) & \to & H^1(X, \mathcal{B}_X) & \to & H^1(X, \mathcal{B}''_X), \end{array}$$

где обе крайние стрелки по предположению индукции представляют биекцию. Если бы гомоморфизм $H^1(J, \mathcal{B}_J) \to$ $\to H^1(J, \mathcal{B}''_J)$ был сюръективным, то отсюда следовало бы, что средняя вертикальная стрелка также представляет сюръекцию, что и доказывало бы следствие. Так как J не имеет гомологий с кручением, то все сводится к доказательству следующей леммы.

---

[1]) Как сообщил автор, Мамфордом показано (Мамфорд Д., Лекции о кривых на алгебраической поверхности, „Мир“, 1968, лекция 28) что утверждение, о котором идет речь, справедливо Это легко следует из представимости функтора Пикара, которая доказана Гротендиком. — *Прим. ред.*

Лемма 8. *Пусть* $0 \to B' \to B \to B''$ - *строго точная последовательность унипотентных групп, причем B связна. Если проективное многообразие X не имеет гомологий с кручением размерности q, то гомоморфизм $H^q(X, \mathscr{B}_X) \to$ $\to H^q(X, \mathscr{B}''_X)$ сюръективен.*

Группа B'' связна. Применим индукцию по ее размерности. При $\dim B'' = 0$ доказывать нечего. Если $\dim B'' = 1$, то $B'' = G_a$. По теореме 3 группа B является факторгруппой произведения W групп Витта, и достаточно показать, что гомоморфизм $H^q(X, \mathscr{W}_X) \to H^q(X, \mathscr{O}_X)$ сюръективен. Положим $W = \prod W_{n_i}$. По крайней мере один из гомоморфизмов $W_{n_i} \to G_a$ имеет нетривиальное касательное отображение, что позволяет нам ограничиться случаем сепарабельного сюръективного гомоморфизма f: $W_n \to G_a$. Такой гомоморфизм представляется в виде $W_n \xrightarrow{\varphi} G_a \xrightarrow{g} G_a$, где $\varphi = R^{n-1}$ (см. п. 8), и гомоморфизм g сепарабелен. Это означает, что

$$g(t) = a_0 t + a_1 t^p + \ldots + a_n t^{p^k}, \quad \text{где} \quad a_0 \neq 0.$$

Если обозначить через F эндоморфизм группы $V = H^q(X, \mathscr{O}_X)$, задаваемый возведением в p-ю степень, то эндоморфизм g_* группы V, определяемый g, будет равен

$$a_0 + a_1 F + \ldots + a_k F^k.$$

Из того, что V — конечномерное векторное пространство, а F — p-линейное отображение, следует, что g_* сюръективен (его дифференциал сюръективен; см. гл. VI, п. 4). С другой стороны, φ_* сюръективен, поскольку X не имеет гомологий с кручением размерности q (см. Серр [5], п. 3). Следовательно, гомоморфизм $f_* = g_* \circ \varphi_*$ также сюръективен, что доказывает лемму для случая $\dim B'' = 1$.

Пусть теперь $\dim B'' \geqslant 2$ и

$$0 \to C'' \to B'' \to D'' \to 0$$

— строго точная последовательность групп, где C'' и D'' — связные группы размерности $< \dim B''$. Пусть C - прообраз C'' в B, а C_0 — связная компонента единицы группы C. Для сокращения записи положим $T(B) = H^q(X, \mathscr{B}_X)$ и аналогично для B'', C'', D'', C_0. Если $b'' \in T(B'')$, то предположение индукции, примененное к отображению $B \to D''$, показывает, что существует элемент $b \in T(B)$, имеющий тот же образ, в $T(D'')$, что и b''. Отнимая его от b'', видим, что можно ограничиться случаем, когда элемент $b'' \in T(B'')$ имеет нулевой образ в $T(D'')$. Точная последовательность

$$T(C'') \to T(B'') \to T(D'')$$

показывает тогда, что существует элемент $c'' \in T(C'')$, имеющий своим образом b''. Предположение индукции, примененное к отображению $C_0 \to C''$, позволяет поднять C'' до $C_0 \in T(C_0)$. Так как $T(C_0)$ отображается в $T(B)$, то мы находим, наконец, элемент из $T(B)$, имеющий образ b'', что и требовалось доказать.

23. Приложение к функтору Ext(A, B)

Теорема 12. *Если A — абелево многообразие, то функтор* Ext(A, B) *точен на категории линейных (коммутативных) групп.*

Положим $T(B) = \text{Ext}(A, B)$. Нам надо доказать, что функтор $T(B)$ переводит строго точную последовательность линейных групп

$$0 \to B' \to B \to B'' \to 0$$

в точную последовательность групп

$$0 \to T(B') \to T(B) \to T(B'') \to 0.$$

В силу предложения 3 достаточно доказать, что $T(B) \to T(B'')$ — сюръективное отображение.

Рассмотрим сначала несколько частных случаев.

a) *B — конечная группа.* Известно (Вейль [5], стр. 128), что для любого целого n отображение $x \to nx$ является изогенией A на себя. Если n выбрать делящимся на порядок группы B, то легко получим, что $T(B) = \text{Ext}(A, B)$ отождествляется с $\text{Hom}({}_nA, B)$, где через ${}_nA$ обозначена подгруппа в A, образованная элементами $x \in A$, такими, что $nx = 0$. Разлагая B в прямую сумму, можем, кроме того, считать, что n равно степени простого числа. Группа ${}_nA$ является в этом случае прямой суммой некоторого числа циклических групп порядка n (Вейль [5]), а гомоморфизм $\text{Hom}({}_nA, B) \to \text{Hom}({}_nA, B'')$ будет сюръективным.

б) *B'' — конечная группа.* Пусть B'_0 — связная компонента единицы группы B'. Если характеристика поля k равна 0, то группа B равна произведению B'_0 на конечную группу B/B'_0 и все сводится к случаю а). Если характеристика поля k отлична от 0, то начнем с того, что выбросим из гр ппы B'_0 ее множители типа G_m (являющиеся прямыми множителями в B). После чего период B будет конечен, и поднимая в B образующие группы B'', получим, что существует конечная подгруппа C группы B, проектирующаяся на B''. Остается применить а) к отображению $C \to B''$.

в) *B — тор.* В этом случае группа B'' будет также тором; таким образом, $B = (G_m)^r$, $B'' = (G_m)^s$. Гомоморфизм $\varphi\colon B \to B''$ определяется с помощью целочисленной матрицы Φ. Так как φ сюръективно, существует целочисленная матрица Ψ, такая, что $\Phi \cdot \Psi = N$, где N — целое число, не равное нулю. Имеем $T(B) = \operatorname{Ext}(A, G_m)^r = P(A)^r$, где через $P(A)$ обозначено двойственное к A пространство (см. п. 16). Аналогично $T(B'') = P(A)^s$. Матрицы Φ и Ψ определяют гомоморфизмы $P(\Phi)$ и $P(\Psi)$, удовлетворяющие соотношению $P(\Phi) \cdot P(\Psi) = N$. Поскольку $P(A)$ — абелево многообразие, умножение на N сюръективно, а значит, сюръективно и $P(\Phi)$, что и доказывает требуемый результат.

г) *B — унипотентная и связная группа.* По теореме 8 $H^1(A, \mathscr{B}_A) = T(B)$ и лемма 8 показывает, что $T(B) \to T(B'')$ сюръективно.

д) *B — связная группа.* Разлагая B и B'' в произведение тора на унипотентную группу, применяем в) и г).

Перейдем теперь к общему случаю. Пусть B''_0 — связная компонента единицы B'', а B_0 — ее прообраз в B. Пусть $b'' \in T(B'')$ и x''_0 — образ b'' в $T(B''/B''_0) = T(B/B_0)$. Применяя б) к отображению $B \to B/B_0$, получаем, что x''_0 является образом элемента из $T(B)$. После вычитания можем считать, что $x''_0 = 0$. Элемент b'' превращается тогда в $b''_0 \in T(B''_0)$. Если B_1 — связная компонента единицы группы B, то можно применить д) к отображению $B_1 \to B''_0$, т. е. существует $b_1 \in T(B_1)$, имеющий своим образом b''_0. Так как $T(B_1)$ отображается в $T(B)$, получаем наконец элемент из $T(B)$, имеющий своим образом b'', что и завершает доказательство.

Можно было бы указать другие случаи, когда функтор $\mathrm{Ext}(A, B)$ точен. Ограничимся следующим.

Теорема 13. *Пусть C — расширение абелевого многообразия A с помощью связной (коммутативной) линейной группы L. Если G — конечная группа, то имеет место точная последовательность*

$$0 \to \mathrm{Ext}(A, G) \to \mathrm{Ext}(C, G) \to \mathrm{Ext}(L, G) \to 0.$$

В силу предложения 2 достаточно доказать, что $\mathrm{Ext}(C, G) \to \mathrm{Ext}(L, G)$ является сюръективным отображением, т. е. что всякая изогения L „продолжается“ до C. Итак, пусть $L' \in \mathrm{Ext}(C, G)$. По теореме 12 гомоморфизм $\mathrm{Ext}(A, L') \to \mathrm{Ext}(A, L)$ сюръективен. Следовательно, существует $C' \in \mathrm{Ext}(A, L')$, имеющий своим образом элемент $C \in \mathrm{Ext}(A, L)$. Группа C' содержит L' в качестве подгруппы, которая в свою очередь содержит G. Группа C'/G отождествляется с C. Поэтому C' можно рассматривать как элемент группы $\mathrm{Ext}(C, G)$. Очевидно, что этот элемент имеет своим образом в группе $\mathrm{Ext}(L, G)$ расширение L', что и требовалось доказать.

Пример. Возьмем в качестве C *обобщенное якобиево многообразие* $J_{\mathfrak{m}}$. Абелевым многообразием A будет тогда обычное якобиево многообразие J, а группой L — локальная группа $L_{\mathfrak{m}}$ (гл. V, § 3). Известно (гл. VI, п. 12), что группа $\mathrm{Ext}(J_{\mathfrak{m}}, G)$ отождествляется с группой классов накрытий кривой, группой Галуа которой служит группа G и ведущий модуль которой $\leqslant \mathfrak{m}$. Аналогично группа $\mathrm{Ext}(J, G)$ отождествляется с подгруппой классов неразветвленных накрытий. Теорема 13 показывает тогда, что факторгруппа отождествляется с группой $\mathrm{Ext}(L_{\mathfrak{m}}, G)$, определение которой чисто локально.

Библиографические замечания

Расширения абелевого многообразия A с помощью групп G_a или G_m впервые рассмотрены в короткой заметке Вейля [6], содержащей результат о том, что $\mathrm{Ext}(A, G_m)$ изоморфна группе классов дивизоров X на A, таких, что $X \equiv 0$.

Этот результат был заново доказан Барсотти [2], который систиматически использует „системы факторов“. Барсотти определяет, кроме того, размерность группы $\mathrm{Ext}(A, G_a)$ при помощи классификации радикальных изогений.

Соотношение $H^1(A, \mathfrak{S}_A) = \mathrm{Ext}(A, G_a)$ доказано Розенлихтом [6] (см. также Барсотти [4] и Серр [6]), который получил размерность $H^1(A, \mathfrak{S}_A)$ с помощью обобщенных якобиевых многообразий; именно его доказательство с некоторыми изменениями и приводится в этой книге.

Картье получил недавно более точный результат, чем простое вычисление размерности. Он установил „функториальный" изоморфизм между $H^1(A, \mathfrak{S}_A)$ и касательным пространством $\mathfrak{t}_{A^*}$ к двойственному многообразию A^* многообразия A, что позволило ему вывести „теорему бидвойственности": $A^{**} = A$ (см. Картье [2]).

Наконец, тот факт, что всякая коммутативная связная унипотентная группа изогенна произведению групп Витта, доказан Шевалле и Чжоу (не опубликовано), а также Барсотти [5]. Как показал Дьёдонне [2], аналогичный результат имеет место в „формальной" геометрии.

ЛИТЕРАТУРА

Артин (Artin E.) и Хассе (Hasse H.)

1. Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln. *Hamb. Abh.*, **6** (1928), 146—162.

Барсотти (Barsotti I.)

1. A note on abelian varieties, *Rend. Cir. Palermo*, **2** (1954), 1—22.
2. Structure theorems for group varieties, *Annali di Math.*, **38** (1955), 77—119.
3. Abelian varieties over fields of positive characteristic, *Rend. Cir. Palermo*, **5** (1956), 1—25.
4. Repartitions on abelian varieties, *Illinois J. Math.*, **2** (1958), 43—70.
5. On Witt vectors and periodic group-varieties, *Illinois J. Math.*, **2** (1958), 99—110, 608—610.

Борель (Borel A.)

1. Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts, *Ann Math.*, **57** (1953), 115—207. (Русский перевод: сб. Расслоенные пространства и их приложения, ИЛ, М., 1958, стр. 372—451.)
2. Groupes linéaires algébriques, *Ann. Math.*, **64** (1956), 20—82.

Бэр (Baer R.)

1. Erweiterungen von Gruppen und ihren Isomorphismen, *Math. Zeit.*, **38** (1934), 375—416.

Вейль А. (Weil A.)

1. Zur algebraischen Theorie der algebraischen Funktionen, *J. Crelle*, **179** (1938), 129—133.
2. Sur les fonctions algébriques à corps de constantes finis, *C. R.*, **210** (1940), 592—594.
3. Foundations of algebraic geometry, Coll. № 29, New-York, 1946.
4. Sur les courbes algébriques et les variétés qui s'en déduisent, Hermann, Paris, 1948.
5. Variétés abéliennes et courbes algébriques, Hermann, Paris, 1948.

6. Variétés abéliennes, Colloque d'algèbre et théorie des nombres. Paris, 1949, 125—128.
7. Sur la théorie du corps de classes, *J. Math. Soc. Japan*, **3** (1951), 1—35.
8. Abstract versus classical algebraic geometry, Cong. Int. Amsterdam, 1954, v. III, 550—558. (Русский перевод сб. *Математика*, 2 : 4 (1958), 59—65.)
9. On algebraic groups of transformations, *Amer. J. Math.*, 77 (1955), 355—391.
10. On algebraic groups and homogeneous spaces, *Amer. J. Math.*, **77** (1955), 493—512.
11. The field of definition of a variety, *Amer. J. Math.*, **78** (1956), 569—574.
12. Introduction à l'étude des variétés kählériennes, Hermann, Paris, 1958. (Русский перевод: А. Вейль, Введение в теорию кэлеровых многообразий, ИЛ, М., 1961.)

Вейль Г. (Weyl H.)
1. Die Idee der Riemannschen Fläche, Teubner, 1923.

Витт (Witt E.)
1. Zyklische Körper und Algebren der Charakteristic p vom Grade p^n, *J. Crelle*, **176** (1936), 176—140.

Годеман (Godement R.)
1. Topologie algébrique et théorie des faisceaux, Paris, Hermann, 1958. (Русский перевод: Р. Годеман, Алгебраическая топология и теория пучков. ИЛ, М., 1961.)

Горенштейн (Gorenstein D.)
1. An arithmetic theory of adjoint plane curves, *Trans. Amer. Math Soc.*, 72 (1952), 414—436.

Гротендик (Grothendieck A.)
1. Sur quelques points d'algèbre homologique, *Tohoku Math. J.*, **9** (1957), 119—221. (Русский перевод: Гротендик А., О некоторых вопросах гомологической алгебры, ИЛ, М., 1961.)
2. Théorèmes de dualité pour les faisceaux algébriques cohérents, *Séminaire Bourbaki*, Mai 1957.
3. Le théorème de Riemann-Roch (redigé par A. Borel et J-P. Serre. (Русский перевод: Борель А., Серр Ж.-П., Теорема Римана — Роха, сб. *Математика*, **5 : 5** (1961), 17—54.)

Дёйринг (Deuring M.)
1. Die Zetafunktion einer algebraischen Kurve vom Geschlechte eins (vierte Mitteilung), Gött. Nach., 1957, № 3.

Дьёдонне (Dieudonné J.)
1. La géometrie des groupes classiques, *Ergeb. Math.*, № **5**, Springer, 1955.
2. Groupes de Lie et hyperalgèbres de Lie sur un corps de caracteristique p (VII), *Math. Ann.*, **134** (1957), 114—133.

3. On the Artin — Hasse exponential series, *Proc. Amer. Math. Soc.*, **72** (1957), 210—214.

Зарисский (Zariski O.)
1. Pencils on an algebraic variety and a new proof of a theorem of Bertini, *Trans. Amer. Math. Soc.*, **50** (1941), 48—70.
2. Complete linear systems on normal varieties and a generalization of a lemma of Enriques — Severi, *Ann Math.*, **55** (1952), 552—592.
3. Scientific report on the second summer institute, Part III, Algebraic sheaf theory, *Bull. Amer. Math. Soc.*, **62** (1956), 117—141. (Русский перевод: Зарисский О., Теория алгебраических пучков, сб. *Математика*, **4** : 2 (1960), 3—24.)

Игуза (Igusa J.)
1. On some problems in abstract algebraic geometry, *Proc. Nat. Acad. Sci.*, **41** (1955), 964—967.
2. Fibre systems of Jacobian varieties, *Amer. J. Math.*, **78** (1956), 171—199.
3. Fibre systems of Jacobian varieties, II, *Amer. J. Math.*, **78** (1956), 745—760.

Ионеда (Yoneda N.)
1. On the homology theory of modules, *J. Fac. Sci. Tokyo*, **7** (1954), 193—227.

Кавада (Kawada Y.)
1. Class formations, I. *Duke Math. J.*, **22** (1955), 165—178.
2. Class formations, III, *J. Math. Soc. Japan*, **7** (1955), 453—496.
3. Class formations, IV, *J. Math. Soc. Japan*, **9** (1957), 395—405.

Кавада (Kawada Y.) и Сатаке (Satake I.)
1. Class formations, II, *J. Fac. Sci. Tokyo*, **7** (1955), 353—389.

Картан (Cartan H.) и Эйленберг (Eilenberg S.)
1. Homological algebra, Princeton Math. Ser., № 19. (Русский перевод: Картан А., Эйленберг С., Гомологическая алгебра, ИЛ, М., 1961.)

Картан (Cartan H.) и Шевалле (Chevalley C.)
1. Géométrie algébreque, *Séminaire E. N. S.*, 1955—1956.

Картье (Cartier P.)
1. Une nouvelle opération sur les formes différentielles, *C. R.*, **244** (1957), 476—478.
2. Dualité des variétés abéliennes, *Séminaire Bourbaki*, Mai 1958.

Клебш (Clebsch A.) и Гордан (Gordan P.)
1. Theorie der abelschen Funktionen, Teubner, Leipzig, 1866.

Кодаира (Kodaira K.)
1. On compact complex analytic surfaces, I (notes polycopiées), Princeton, 1955 (Русский перевод: Кодаира К., О компактных комплексных аналитических поверхностях, сб. *Математика*, **6** : **6** (1962), 19—57.)
2. The theorem of Riemann — Roch on compact analytic surfaces, *Amer. J. Math.*, **73** (1951), 813—875.

Колчин (Kolchin E.)
1. On certain concepts in the theory of algebraic matric groups, *Ann. Maths*, **49** (1948), 774—875.

Крацер (Krazer A.) и Виртингер (Wirtinger W.)
1. Abelsche Funktionen und allgemeine Thetafunktionen, Enc. Math. Wiss., II B-7, 1920.

Лазар (Lasard M.)
1. Sur les groupes de Lie formels à un paramètre, *Bull. Soc. Math. France*, **83** (1955), 251—274.

Ленг (Lang S.)
1. Algebraic groups over finite fields, *Amer. J. Math.*, **78** (1956), 555—563.
2. Unramified class field theory over function fields in several variables, *Ann. Math.*, **64** (1956), 285—325.
3. Sur les séries L d'une variété algébrique, *Bull. Soc. Math. France*, **84** (1956), 385—407.
4. Introduction to algebraic geometry, Interscience Tracts, № 5, New-York, 1958.
5. Abelian varieties, Interscience Tracts, № 7, New-York, 1959.

Ленг (Lang S.) и Серр (Serre J.-P.)
1. Sur les revêtements non ramifiés des variétés algébriques, *Amer. J. Math.*, **79** (1957), 319—330.

Ленг (Lang S.) и Тейт (Tate J.)
1. Galois cohomology and principal homogeneous spaces, *Amer. J. Math.*, **80** (1958), 659—684

Мацусака (Matsusaka T.)
1. The theorem of Bertini on linear systems in modular fields, *Kyoto Math. Mem.*, **26** (1960), 51—62.

Морикава (Morikawa H.)
1. Generalized Jacobian varieties and separable abelian extensions of function fields, *Nagoya Math. J.*, **12** (1957), 231—254.

Нагата (Nagata M.)
1. On the embedding problem of abstract varieties in projective varieties, *Mem. Kyoto*, **30** (1956), 71—82.

Норткотт (Northcott D.)
1. The neighbourhoods of a local ring, *J. London Math. Soc.*, **30** (1955), 360—375,

2. A note on the genus formula for plane curves, *J. London Math. Soc.*, **30** (1955), 376—382.
3. A general theory of one-dimensional local rings, *Proc. Glasgow Math. Ass.*, **2** (1956), 159—169.

Рейнер (Reiner I.)
1. Integral representations of cyclic groups of prime orders, *Proc. Amer. Math. Soc.*, 8 (1957), 142—146.

Розенлихт (Rosenlicht M.)
1. Equivalence relations on algebraic curves, *Ann. Math.*, **56** (1952), 169—191. (Русский перевод: Розенлихт М., Отношения эквивалентности на алгебраических кривых, сб. *Математика*, **5 : 1** (1961), 3—31.)
2. Generalized Jacobian varieties, *Ann Math.*, **59** (1954), 505—530. (Русский перевод: Розенлихт М., Обобщенные якобиевы многообразия, сб. *Математика*, **6 : 2** (1962). 40—75.)
3. A universal mapping property of generalized Jacobian varieties, *Ann. Math.*, **66** (1957), 80—88.
4. Some basic theorems on algebraic groups, *Amer. J. Math.*, **78** (1956), 401—443.
5. A note on derivations and differentials on algebraic varieties, *Port. Math.*, **16** (1957), 43—55.
6. Extensions of vector groups by abelian varieties, *Amer. J. Math.*, **80** (1958) 685—714.

Самюэль (Samuel P.)
1. Singularités des variétés algébriques, *Bull. Soc. Math. France*, **79** (1951), 121—129.
2. Algèbre locale, Mém. Sci. Math., № **123**, Paris, 1953.
3. Méthodes d'algèbre abstraite en géométrie algébrique, Ergeb. Math., № **4**, Springer, 1955.

Севери (Severi F.)
1. Vorlesungen über algebraische Geometrie, Teubner, Leipzig, 1921.
2. Serie, sistemi d'equivalenza e corrispondenze algebriche sulle varietà algebriche, Rome, 1942.
3. Funzioni quasi abeliane, Vatican, 1947.

Серр (Serre J.-P.)
1. Faisceaux algébriques cohérents, *Ann. Math.*, **61** (1955), 197—278. (Русский перевод: Серр Ж.-П., Алгебраические когерентные пучки, сб. Расслоенные пространства и их приложения, ИЛ, М., 1958, 372—451.)
2. Cohomologie et géométrie algébriques, Cong. Int. Amsterdam, 1954, III, 515—520.
3. Géométrie algébriques et géométrie analytique, *Annales Inst. Fourier*, **6** (1955—1956), 1—42.
4. Sur la cohomologie des variétés algébriques, *J. Math. pures et Appl.*, **36** (1957), 1—42.
5. Sur la topologie des variétés algébriques en caracteristique *p*. Symposium de topologie algébrique, Mexico, 1956.

6. Quelques propriétés de variétés abéliennes en caractéristique *p*, *Amer. J. Math.*, **80** (1958), 715—739.

Тейт (Tate J.).
1. The higher dimensional cohomology groups of class field theory, *Ann. Math.*, **56** (1952), 294—297.
2. *WC*-groups over *p*-adic fields, *Séminaire Bourbaki*, Déc. 1957.

Уэплс (Whaples G.)
1. Local theory of residues, *Duke. Math. J.*, **18** (1951), 683—688.

Хассе (Hasse H.)
1. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, *Jahr. D. Math. Ver.*, **35** (1926), 1—55; **36** (1927), 255—311; **39** (1930), 1—204.
2. Theorie der relativ-zyklischen algebraischen Funktionkörper insbesondere bei endlichem Konstantenkörper, *J. Crelle*, **172** (1934), 37—54.
3. Theorie der Differentiale in algebraischen Funktionenkörpern mit vollkommenem Konstantenkörper, *J. Crelle*, **172** (1934), 55—64.

Хербранд (Herbrand J.)
1. Le développement moderne de la théorie des corps algébriques—corps de classes et lois de réciprocité, Mém. Sc. Math., № **75**, Paris, 1936.

Хиронака (Hironaka H.)
1. On the arithmetic genera and the effective genera of algebraic curves. *Mem. Kyoto*, **30** (1957), 177—195.

Хирцебрух (Hirzebruch F.)
1. Neue topologische Methoden in der algebraischen Geometrie, Ergeb. Math., № **9**, Springer, 1956.

Хохшильд (Hochschild G.) и Накаяма (Nakayama T.)
1. Cohomology in class field theory, *Ann. Math.*, **55** (1952), 348—366.

Цассенхауз (Zassenhaus H.)
1. The theory of groups, New-York, Chelsea, 1949.

Чжоу (Chow W. L.)
1. The Jacobian variety of an algebraic curve. *Amer. J. Math.*, **76** (1954), 453—476.
2. On the projective embedding of homogeneous varieties, Symp. in honor of S. Lefschetz, Princeton, 1957, 122—128.

Шателе (Châtelet F.)
1. Variations sur un thème de H. Poincaré, *Annales E. N. S.*, **61** (1944), 249—300.

Шевалле (Chevalley C.)
1. Introduction to the theory of algebraic functions of one va-

riable, Math. Surv., VI. New-York, 1951. (Русский перевод: Шевалле К., Введение в теорию алгебраических функций одной переменной, Физматгиз, М., 1959.)
2. Class field theory, Nagoya, 1954.
3. Classification des groupes de Lie algébriques, *Séminaire E. N. S.* (1956—1957).

Шимура (Shimura G.) и Танияма (Taniyama Y.)
1. Complex multiplication of abelian varieties and its applications to number theory, *J. Math. Soc. Japan*, **10** (1958).

Шмид (Schmid H. L.)
1. Ueber das Reziprozitätsgesetz in relativ-zyklischen algebraischen Funktionenkörpern mit endlichem Konstantenkörper, *Math. Zeit.*, **40** (1936), 94—109.

УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ

Ж. Серр

АЛГЕБРАИЧЕСКИЕ ГРУППЫ И ПОЛЯ КЛАССОВ

Редактор *В. И. Авербух* Художник *В. М. Новоселова*
Художественный редактор *В. И. Шаповалов*
Технический редактор *Л. М. Харьковская* Корректор *В. И. Киселева*

Сдано в производство 20/II 1968 г. Подписано к печати 29/VIII 1968 г.
Бумага глуб. печ. $84 \times 108^1/_{32} = 4{,}5$ бум. л. 15,12 усл. печ. л. Уч.-изд. л. 13,43.
Изд. № 1/4599. Цена 1 р. 15 к. Зак. 1117

Темплан изд-ва «Мир» 1968 года, пор № 17

ИЗДАТЕЛЬСТВО „МИР"
Москва, 1-й Рижский пер., 2

Ленинградская типография № 2 имени Евгении Соколовой Главполиграфпрома Комитета по печати при Совете Министров СССР. Измайловский проспект. 29.

Ж. СЕРР

АЛГЕБРАИЧЕСКИЕ ГРУППЫ И ПОЛЯ КЛАССОВ

Перевод с французского
И. В. ДОЛГАЧЕВА

Под редакцией
С. П. ДЕМУШКИНА

ИЗДАТЕЛЬСТВО
„МИР"
МОСКВА 1968